

Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x

First Published: 2026-02-24

Last Modified: 2026-07-09

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

Full Cisco Trademarks with Software License ?

CHAPTER 1

Authentication 1

- Authentication 2
- Authentication order 2
- Authentication fallback mechanism 3
- Configure authentication order 4
- Duo Multi-factor authentication 4
  - Duo Multi-factor authentication 4
  - Configure Duo multifactor authentication 4
- RADIUS authentication 6
  - Radius authentication 6
  - Configure RADIUS authentication using CLI commands 6
- SSH authentication 7
  - SSH authentication 7
  - Restrictions for SSH authentication 8
  - Supported methods for configuring SSH authentication using CLI commands 8
  - Configure SSH Authentication using templates 8
- IEEE 802.1X authentication 9
  - IEEE 802.1X authentication 9
  - Restrictions for configuring IEEE 802.1X authentication 9
  - Prerequisites for configuring IEEE 802.1X authentication 10
  - Configure IEEE 802.1X Authentication using templates 10
    - Create a Switch Port template using templates 12
  - IEEE 802.1X Open Authentication using CLI commands 14
  - Configure IEEE 802.1X Authentication using CLI commands 14

Configure Switch Port using a configuration group 15
Authentication, Authorization, and Accounting 18
Restrictions to configure authorization and accounting 18
Configure AAA using a configuration group 18
Methods of configuring AAA using templates 22
Create a template 22
Configure local access for users and user groups 23
Configure RADIUS authentication 25
Configure TACACS+ authentication 26
Configure authentication order 27
Configure authorization 27
Configure accounting 28
Posture assessment support 29
Posture assessment support 29
Restrictions for Posture Assessment 30
Configure posture assessment using CLI commands 30

CHAPTER 2 RADIUS and TACACS 33
Feature history for RADIUS and TACACS 33
RADIUS 34
TACACS 34
Restrictions for cloud multitenant with on-prem per-tenant AAA and provider AAA 35
Prerequisites for cloud multitenant with on-prem per-tenant AAA and provider AAA 35
Configuring remote AAA 36
Enable multitenancy 36
Configure a tenant 36
Configure remote AAA 37
Configure RADIUS 38
Configure TACACS 39
Configure RADIUS and TACACS for multitenancy using CLI 40
Verify RADIUS and TACACS 41

CHAPTER 3 Users and Access 43
Users and access 43

Users and access 43
Users and user groups 44
User group permissions 46
Configure users using CLI commands 46
Configure password for admin users using CLI commands 47
Create user groups 48
Create user groups using CLI commands 48
Delete a user group 49
Edit user group privileges 49
Account lockout 50
Account Lockout 50
Configure Account Lockout 50
Configure unsuccessful login attempts lockout 52
User sessions 53
User sessions 53
Restrictions for configuring user sessions 53
Configure a client session timeout in SD-WAN Manager 54
Configure a session lifetime in SD-WAN Manager 54
Configure the Server Session Timeout in SD-WAN Manager 55
Set the maximum sessions per user role 55
Ciscotac user access 56
Ciscotac user access 56
Limitations for Ciscotac user access 56

CHAPTER 4 **Password Management** 57
Hardened passwords 58
Restrictions for passwords 58
Password requirements 58
Enable Password Policy 59
Reset a locked user using SD-WAN Manager 60
Reset a locked user using CLI commands 60
Type 6 passwords 61
Type 6 passwords 61
Supported platforms and templates 61

Restrictions for Type 6 passwords 62
Upgrade existing templates to Type 6 passwords 62
Type 6 encryption for CLI commands 63
Methods for verifying Type 6 passwords 63

CHAPTER 5 **Role-Based Access Control** 65
Role-Based Access Control 68
Restrictions for configuring RBAC 70
RBAC by VPN 70
RBAC with AAA 71
User authorization rules for operational and configuration commands 73
RBAC by scope 80
RBAC by scope 80
Multitenancy support 82
Granular RBAC 83
Granular RBAC for templates 83
Benefits of granular RBAC 83
RBAC for policies 84
RBAC for policies 84
Configure RBAC for policies 84
Modify policy configurations 84
Configure RBAC for CFlowd policy 85
Create a CFlowd user group 85
Create a CFlowd policy user 85
Modify a CFlowd policy 86
Assigning roles to users defined by identity providers 86
Configure RBAC 87
Configure scope 87
Configure roles 88
Copy custom role 88
Edit custom role 89
Delete a role 89
Prerequisites for Application Catalog features 89
Manage user group permissions 90

User group permissions for Cisco IOS XE Catalyst SD-WAN devices 90
User group permissions for Cisco Catalyst Wireless Gateway devices 109
Configure Users 111
Add user 111
Edit user 112
Copy user 113
Delete user 113
Change user password 114
Reset locked user 114
Apply administrative lock 114
View users logged in to a device using SSH sessions 114
View users with active HTTP sessions 115
Configure user sessions 115
Configure VPN segments 115
Configure VPN groups 116
Verify granular RBAC permissions 116
Monitor devices for VPN groups 116

CHAPTER 6 **System Logging** 119
Feature history: System logging 119
System logging 119
System log files 120
System log formats 121
System log message levels 122
Sending system log messages to a server, using TLS 123
Restrictions for system logging 124
Configure system logging 125
Configure system logging using a configuration group 125
Configure system logging using a template 129
Create a System Logging feature template 130
Configure a device to save system log messages locally 130
Configure a device to save system log messages to a server, using TLS 131
Configure a device to save system log messages to a server 132
Configure system logging using CLI commands 134

Configure system logging, saved locally, using CLI commands 134
Configure system logging, saved remotely, using CLI commands 135
Install a root certificate on a device for mutual authentication 135
Install a root certificate authority on a syslog server for server authentication 136
Install a root certificate authority on a device for server authentication, using CLI commands 137
Create a certificate signing request and install feature certificates 139
Viewing system log information 139
View system logs using SD-WAN Manager 139
Viewing system log information using CLI commands 140
Verifying the trustpoint configuration on a device 140
Remote logging over TCP and TLS 141
Benefits of remote logging over TCP and TLS 141
Configure remote logging over TCP using CLI commands 142
Configure remote logging over TLS using CLI commands 142
Verifying remote logging over TCP and TLS 143

CHAPTER 7 **Device Tagging** 145
Feature history: Device tagging 145
Device tagging 145
Restrictions for device tagging 146
Add device tags 146
Delete device tags 147

CHAPTER 8 **Configure Devices** 149
Feature history for configure devices 149
Configure devices in Cisco Catalyst SD-WAN 150
Types of templates 150
Template variables 151
Use variable values in configuration templates 152
Use a file for variable parameters 152
CSV file format 153
Generate a skeleton CSV file 153
Import a CSV file 154
Manually enter values for device-specific variables and for optional rows 155

Configure and manage device templates 156
Create a device template 156
Create a device template from feature templates 156
Create a device template after building custom feature templates 158
Create a device CLI template 159
Default device templates 160
Change variable values for a device 160
Change the device rollback timer 161
Edit a device template when a push fails 162
Retrieve last edited configuration 162
Determine why a device rejects a template 162
Preview device configuration and view configuration differences 163
Export a variables-spreadsheet in CSV format for a template 163
Edit a device template 164
Delete a template 164
Copy a template 165
Edit a CLI device template 165
View a template 165
View device templates attached to a feature template 166
View devices attached to a device template 166
Attach templates to devices 167
Attach and detach a device template 167
Attach a device template to devices 167
Configuration prerequisites 169
Device configuration workflow 169
Configure and manage devices using SD-WAN Manager 170
Change configuration modes 171
Upload WAN edge router authorized serial number file 171
Upload WAN edge router serial numbers from Cisco Smart Account 172
Export device data in CSV format 173
View a device's running configuration 174
View a device's local configuration 174
Copy router configuration 174
Delete a WAN edge router 175

Decommission a cloud router 176
View log of template activities 176
View status of device bring up 177
Add a Cisco SD-WAN Validator 177
Configure Cisco SD-WAN Controllers 178
Add an SD-WAN Controller 178
Edit SD-WAN Controller details 178
Delete an SD-WAN Controller 179
Configure reverse proxy on SD-WAN Controllers 179
Configure UCSE using a configuration group 179
Create a UCS-E Template 181

CHAPTER 9 **Basic Settings for Cisco SD-WAN Manager** 185
Basic system settings 185
Device and SD-WAN Control Component properties 186
Time and NTP 186
User authentication and access with AAA, RADIUS, and TACACS+ 186
Authentication for WANs and WLANs 187
Network segmentation 188
Network interface properties 188
Management and monitoring options 189
IPFIX 190
REST API 190
SNMP 190
System log messages 191
Cisco SD-WAN Manager 191
Enforce a software version on devices 192
Configuring a login page banner 193
Configure a login page banner using a configuration group 193
Configure a login page banner, using templates 194
Configure a login page banner, using CLI commands 195
Create a custom banner 195
Configuring device basic settings 195
Configure device basic settings using a configuration group 195

Configure device basic system settings using templates 198
Configuring global system settings 202
Configure global system settings using a configuration group 202
Configure global system settings using templates 204
Configure global system settings using CLI commands 207
Configuring NTP servers 209
Configure NTP servers using a configuration group 209
Configure NTP servers and parameters using templates 211
Configure NTP servers using CLI commands 213
Configuring a router as an NTP primary 214
Configure a router as an NTP primary using templates 214
Configure a router as an NTP primary using CLI commands 215
Configure device time using CLI commands 216
Configuring GPS 217
Configure GPS using a configuration group 217
Configure GPS using templates 218
Configuring automatic bandwidth detection 219
Configure automatic bandwidth detection using templates 219
Configure automatic bandwidth detection using CLI commands 221
Proxy server for SD-WAN Manager HTTP and HTTPS traffic with external servers 222
Restrictions for a proxy server for HTTP and HTTPS traffic 223
Configure a proxy server for HTTP and HTTPS traffic 223
Rate limit for bulk API requests 224
Configure the rate limit for bulk API requests, using CLI commands 224
Configure device statistics collection 226
Configure the time interval for collecting device statistics 226
Configure the SD-WAN Manager server maintenance window 227
Configure system logging using CLI commands 228
Connect to a device by SSH terminal 228
View the rate limit for bulk API requests 229
Monitor NAT DIA endpoint trackers 229

CHAPTER 10 VPN 231
VPN 231

Interfaces in the WAN Transport VPN 231
Interfaces in the Management 232
Configure VPN 233
Configure VPN using configuration groups 233
Configure transport VPN using a configuration group 233
Configure management VPN using a configuration group 236
Configure service VPN using a configuration group 238
Configure VPN using templates 248
Configure VPN parameters using CLI commands 250
Configure load-balancing algorithm using CLI commands 250
Map host names to IP addresses using CLI commands 251
Verify the VPN configuration 252

CHAPTER 11 TLOC 255
TLOC 255
System IP address 256
Color 257
Encapsulation 257

CHAPTER 12 TLOC Extension 259
Feature history for TLOC extension 259
TLOC extension 259
TLOC extension over IPv6 260
Limitations for TLOC extension over IPv6 260
How TLOC extension over IPv6 works 261
Configure TLOC extension using CLI commands 262
Verify TLOC extension 263

CHAPTER 13 Network Hierarchy Management 265
Feature history for network hierarchy management 265
Network hierarchy management 266
Benefits of network hierarchy 267
Supported devices for network hierarchy 267
Restrictions for network hierarchy 267

Manage a network hierarchy 268
Create a region in a network hierarchy 268
Create a subregion in a network hierarchy 269
Create a secondary region in a network hierarchy 270
Create a group in a network hierarchy 271
Create a site in a network hierarchy 271
Edit a WAN region 272
Delete a WAN region 273
Edit a group 273
Delete a group 273
Edit a site 273
Delete a site 274
Create a system IP pool 274
Edit a system IP pool 275
Create a remote access pool 275
Edit a remote access pool 276
Create an IP pool for ThousandEyes 276
Delete a pool 276

CHAPTER 14 **Resource Management and Collectors in a Network Hierarchy** 279
Feature history of resource management and collectors 279
Resource management and collectors 280
Assign resource IDs to devices 281
Assign a site ID to a device using the quick connect workflow 281
Assign a site ID to a device using a template 281
Assign a site ID to a device using a configuration group 282
Assign a region ID to a device 282
Assign a system IP to a device 283
Assign a hostname to a device 283
Configure cflowd 284
Configure security logging 285

CHAPTER 15 **Wireless Management** 289
Feature history for wireless management 289

Wireless management on ISR 1000 series routers 290
Supported devices for wireless management 290
Prerequisites for wireless management on Cisco ISR 1000 series routers 291
Restrictions for wireless management on Cisco ISR 1000 series routers 292
Configuring wireless management 292
Configure wireless management on Cisco ISR 1000 series routers using a configuration group 292
Configure wireless management on ISR 1000 series routers 294
Configure wireless management on Cisco ISR 1000 series routers using CLI commands 296
Configuration example for wireless configuration on Cisco ISR 1000 series routers 300
Monitor wireless configuration on Cisco ISR 1000 series routers 300
Troubleshooting wireless configuration on Cisco ISR 1000 series routers 301

CHAPTER 16 **Cellular Gateway** 303
Feature history for Cellular Gateway configuration 303
Cellular gateways 303
Supported Cellular Gateway devices 304
Configuring cellular gateways 304
Configure a cellular gateway using a configuration group 304
Configure a cellular gateway with a feature template 309

CHAPTER 17 **Cisco Unified Communications Voice Services** 313
Feature history for Cisco Unified Communications Voice Services 313
Cisco Unified Communications Voice Services 314
Configure Unified Communications Voice Services 315
Add a voice card feature template 316
Voice card analog interface configuration options 317
Voice card digital interface configuration options 319
Add call routing feature template 326
Global call routing options 327
Dial peer options 328
Add an SRST feature template 331
Global Cisco Unified SRST Options 332
SRST Phone profile options 333
Add a DSPFarm feature template 333

Media resource options 335
DSPFarm service options 335
SCCP options 339
Add a voice policy 345
Configure voice ports for a voice policy 345
Configure POTS dial peers for a voice policy 361
Configure SIP Dial Peers for a voice policy 370
Configure SRST phones for a voice policy 383
Provision a device template for unified communications 385
Generated CLI commands for subpolicies to endpoints mapping 387
Dial peer CSV file 388
Translation rules CSV file 390
Monitor UC operations 391
Voice calls monitoring information 392
Voice VoIP calls monitoring information 392
Voice phone info monitoring information 393
Voice controller T1 E1 current 15 Mins stats monitoring information 394
Voice controller T1 E1 total stats monitoring information 395
Voice ISDN status information 396
Voice DSPFarm SCCP CUCM groups monitoring information 396
Voice DSPFarm profile monitoring information 397
Voice DSPFarm SCCP connections monitoring information 398
Voice DSPFarm active monitoring information 398

CHAPTER 18 **Cisco Unified Border Element** 401
Feature history for Cisco Unified Border Element 401
Cisco unified border elements (CUBE) 403
Supported devices for CUBE configuration 403
Restrictions for CUBE configuration 404
Use cases for CUBE 404
Configure CUBE 404
CUBE commands 405
SRST commands 414

CHAPTER 19 **Onboarding ThousandEyes Agent and Onboarding Tests** 415

Feature History for Simplified Onboarding of Cisco ThousandEyes Agent 415

Simplified workflow for onboarding Cisco ThousandEyes agents and configuring tests 415

Create an IP Pool for the Cisco ThousandEyes Agents 416

Prerequisites for simplified workflow 416

Restrictions for simplified workflow 417

Configure Cisco ThousandEyes agent and tests using simplified workflow 418

Monitor onboarded Cisco ThousandEyes agents and configured tests 419

Troubleshoot Cisco ThousandEyes agent on edge device 419

CHAPTER 20 **Monitoring with Cisco ThousandEyes** 421

Feature history for extended visibility with Cisco Catalyst SD-WAN and ThousandEyes 421

Extending visibility for Cisco Catalyst SD-WAN and Cisco ThousandEyes 422

Supported devices for running Cisco SD-WAN and Cisco ThousandEyes 423

ThousandEyes Enterprise Agent supported versions and system requirements 425

Prerequisites for extending visibility with SD-WAN Manager and Cisco ThousandEyes 426

Restrictions for Extending Visibility with SD-WAN Manager and Cisco ThousandEyes 427

Configure a Cisco ThousandEyes Enterprise Agent using a Configuration Group 427

Upload the Cisco ThousandEyes Enterprise Agent software to SD-WAN Manager 429

Provision Cisco ThousandEyes Enterprise Agent in a Service VPN or Transport VPN (VPN0) 430

Provision a Cisco ThousandEyes Enterprise Agent in a Service VPN Using CLI 433

Uninstall the Cisco ThousandEyes Enterprise Agent software 434

Upgrade the Cisco ThousandEyes Enterprise Agent software 434

Troubleshoot the Cisco ThousandEyes Enterprise Agent on Cisco IOS XE Catalyst SD-WAN devices 435

CHAPTER 21 **EtherChannels** 437

Feature history for EtherChannels 437

EtherChannels on the service side 438

Supported devices for service side EtherChannel 438

Prerequisites for EtherChannels on the service side 439

Restrictions for EtherChannels on the service side 439

Load balancing for service side EtherChannels using CLI commands 440

Enable load balancing on an individual port channel 440
Enable hash algorithms for flow-based load balancing on a global level 442
Enable hash algorithms flow-based load balancing on an individual port channel interface 442
Enable VLAN load balancing per port channel on the service side 443
Configure load balancing for EtherChannels on the service side using CLI commands 444
Configure a service-side port channel and member link interface using configuration groups 445
EtherChannels on the transport side 446
Supported devices for transport side EtherChannel 446
Prerequisites for EtherChannels on the transport side 447
Restrictions for EtherChannels on the transport side 447
Configure a transport side EtherChannels using a CLI template 448
Configure load balancing for EtherChannels on the Transport Side using CLI Commands 450
Enable load balancing on individual portchannel interface on the transport side 451
Enable load balancing globally for EtherChannels on the transport side 452
Enable hash algorithms globally for EtherChannels on the transport side 453
Monitor configured EtherChannel using CLI 454
Aggregate EtherChannel Quality of Service 455
Prerequisites for Aggregate EtherChannel Quality of Service 455
Restrictions for Aggregate EtherChannel Quality of Service 456
Configure Aggregate EtherChannel Quality of Service using CLI Template 456
Verify Aggregate EtherChannel Quality of Service 459

CHAPTER 22 **Network Interfaces** 461
Network Interfaces 461

CHAPTER 23 **Bandwidth Utilization Reference Values** 463
Feature history for bandwidth utilization Reference Values 463
Bandwidth Utilization Reference Values 463
Generating Notifications 464
Monitoring Bandwidth Utilization with Interface Charts 464
Restrictions for bandwidth utilization reference values 465
Configure bandwidth utilization reference values 465
Configure bandwidth utilization reference values using a configuration group 465
Configure bandwidth utilization reference values using CLI commands 465

Configure bandwidth utilization reference values using templates 466
Monitor bandwidth utilization events 467
Monitor bandwidth utilization reference values 467
Verify bandwidth utilization reference values 467

CHAPTER 24 **Loopback Interfaces** 469
Feature history for loopback interfaces 469
Loopback interfaces 470
Implicit ACLs on loopback interfaces 470
Loopback TLOC interface bound to a physical WAN interface 470
Loopback TLOC interface not bound to a physical WAN interface 471
Bind mode and unbind mode 471
Configure implicit ACL on loopback interfaces using CLI commands 472
Examples of implicit ACL configurations on loopback interfaces 473
Verify implicit ACL configurations on loopback interfaces 474

CHAPTER 25 **Subinterfaces** 477
Subinterfaces 477
Configuration examples for subinterfaces 478
Verify configurations on subinterfaces 479

CHAPTER 26 **Dynamic Interfaces** 481
Feature history for dynamic interfaces 481
Configure dynamic interfaces 481

CHAPTER 27 **VPN Ethernet Interface** 485
Configure VPN ethernet interface 485
Configure VPN ethernet interface using a configuration group 485
Configure prefix list for VRRP using a configuration group 495
Configure VPN ethernet interface using templates 495
Configure a prefix list for VRRP 502
Configure a prefix list for VRRP in the device template 503

CHAPTER 28 **Cellular Interfaces** 505

Feature history for cellular interfaces 505
Cellular interfaces 506
Supported devices 507
Guidelines 508
Configure cellular interface 508
Configure cellular interfaces using a configuration group 508
Configure cellular interfaces using CLI 519
Configure cellular interfaces using templates 519
Reset the profile configuration of a cellular modem 527
Troubleshoot LTE modem crash 528

CHAPTER 29 **VRRP Interface Tracking** 531

Feature history for VRRP interface tracking 531
VRRP 532
Restrictions for VRRP interface tracking 533
VRRP tracking use cases 533
Configure VRRP 534
Configuring VRRP using Cisco Catalyst SD-WAN Manager 534
Configure a prefix list for VRRP using Configuration Groups 535
Configure a prefix list for VRRP using a feature template 536
Configure a prefix list for VRRP using a device template 536
Configure VRRP using CLI commands 537
Configure VRRP tracking using CLI templates 542
VRRP object tracking using CLI 542
SIG container tracking 543
Configure VRRP tracking 544
Configure an object tracker using a feature template 544
Configure VRRP for a VPN interface template and associate interface object tracker 545
Monitor VRRP configuration 546
Verify VRRP tracking 547

CHAPTER 30 **VPN Interface Bridge** 549

Configure VPN interface bridge 549

CHAPTER 31 DSL IPoE 555

Configure DSL IPoE 555

Configure DSL IPoE using a configuration group 555

Configure DSL IPoE using templates 562

CHAPTER 32 DSL PPPoA 573

Configure DSL PPPoA 573

Configure DSL PPPoA using a configuration group 573

Configure DSL PPPoA using templates 581

CHAPTER 33 DSL PPPoE 591

Feature history for DSL PPPoe 591

Configure DSL PPPoE 591

Configure DSL PPPoE using a configuration group 592

Configure DSL PPPoE using templates 599

CHAPTER 34 VPN Interface Ethernet PPPoE 609

Configure VPN interface ethernet PPPoE 609

Configure VPN interface ethernet PPPoE using a configuration group 609

Configure VPN interface ethernet PPPoE using templates 616

CHAPTER 35 VPN Interface GRE 625

Configure VPN interface GRE 625

Configure VPN interface GRE on transport VPN using a configuration group 625

Configure GRE on service VPN using a configuration group 629

Configure VPN Interface GRE using templates 633

CHAPTER 36 VPN Interface IPsec 637

Feature history for VPN interface IPsec 637

Configure VPN interface IPsec 637

Configure IPsec on the transport VPN using a configuration group 637

Configure IPsec on the service VPN using a configuration group 642
Configure VPN interface IPsec using templates 646
Change the IKE version from IKEv1 to IKEv2 651
CLI configuration examples for VPN interface IPsec 652

CHAPTER 37 VPN Interface Multilink 655
Configure VPN interface multilink 655
Configure VPN interface multilink using a configuration group 655
Configure VPN interface multilink using templates 661

CHAPTER 38 VPN Interface SVI 669
Feature history for VPN interface SVI 669
Configure VPN interface SVI 669
Configure SVI interface using a configuration group 669
Configure SVI interface using templates 675

CHAPTER 39 VPN Interface T1/E1 679
Configure VPN interface T1/E1 679
Configure VPN interface T1/E1 using a configuration group 679
Configure T1 or E1 controller using a configuration group 686
Configure VPN interface T1/E1 using templates 688
Configure T1 or E1 controller using templates 693

CHAPTER 40 IP Directed Broadcast 697
IP directed broadcast 697
Configure IP directed broadcast using CLI commands 697

CHAPTER 41 Layer 2 VPN 699
Feature history for L2VPN 699
Layer 2 VPNs within the SD-WAN overlay network 700
Supported platforms for Layer 2 VPN 703
Restrictions for Layer 2 VPN 703
Methods to configure Layer 2 VPN using CLI template 704

Configure a Layer 2 VPN on a Cisco IOS XE Catalyst SD-WAN device using CLI template 704
Configure a point-to-point Layer 2 VPN using CLI template 705
Configure an edge router at Site A for point-to-point Layer 2 VPN using CLI template 706
Configure an edge router at Site B for point-to-point Layer 2 VPN using CLI temple 707
Configure a point-to-multipoint Layer 2 VPN using CLI template 708
Configure an edge router at sites A, B and C 708
Configure an edge router at Site B for point-to-point Layer 2 VPN using CLI temple 709
Configure an edge router at Site C for point-to-point Layer 2 VPN using CLI template 711
Configure a Layer 2 VPN Switchport using CLI template 712
Methods to verify Layer 2 VPN using CLI 714
View a Layer 2 VPN status 714
View L2VPN information learned through OMP route on a Cisco SD-WAN Controller 714
View Bridge-domain information 715
View Cisco Catalyst SD-WAN Flood List Information and Packet Counters in Data Plane 716
View packet counters in data plane 716
Monitor configured layer 2 VPN using CLI 718

CHAPTER 42 **VFR and Underlay Fragmentation** 721
Feature history for VFR and underlay fragmentation 722
Virtual Fragmentation Reassembly 722
Underlay fragmentation 723
Benefits of VFR and underlay fragmentation 723
Prerequisites for configuring VFR and underlay fragmentation 723
Restrictions for configuring VFR and underlay fragmentation 724
Use cases for VFR and underlay fragmentation 724
Boost mode 724
Configure VFR and underlay fragmentation 725
Configure underlay fragmentation using a configuration group 725
Configure VFR using CLI commands 725
Configure underlay fragmentation using CLI commands 727
Enable boost mode using CLI commands 728
Verify VFR and underlay fragments 728

CHAPTER 43 **PPPoE** 735

Feature history for PPPoE 735
PPPoE 735
PPPoE over ATM 736
Supported platforms for PPPoE over ATM 736
Configure PPPoE using templates 736
Configure PPPoE over ATM using templates 739
Configuration examples for PPPoE 741

CHAPTER 44 GRE-in-UDP 743
Feature history for GRE-in-UDP 743
GRE-in-UDP 743
Configure GRE-in-UDP using CLI commands 743

CHAPTER 45 Track Static Routes for Service VPNs 745
Feature history of track static routes for service VPNs 745
Track static routes for service VPNs 746
Supported platforms 746
Restrictions for IPv4 static route tracking 747
Configure tracker group using a configuration group 747
Create a static route tracker 748
Configure a next hop static route with tracker 750
Monitor static route tracker configuration 751
Configure static routes using CLI 751
Configuration examples static route tracking 753
Verify static route tracking configuration 754

CHAPTER 46 VDSL and GSHDSL 757
VDSL and GSHDSL 757
VDSL configuration guidelines 758
GSHDSL configuration guidelines 759
GSHDSL EFM-ATM NIM 761
Cisco VDSL examples 761
Cisco GSHDSL examples 763

CHAPTER 47 **Network Slicing** 767

Feature history of network slicing 767

Network slicing 767

Configure network slicing 768

Configure network slicing using CLI 770

Verify network slicing using CLI 771

CHAPTER 48 **Carrier Supporting Carrier** 773

Feature history for carrier supporting carrier 773

Carrier supporting carrier 774

Traffic flow configuration between CSC-CE and CSC-PE devices 774

Edge device functioning as a CSC-CE device 775

Use cases for carrier supporting carrier 776

Configure carrier supporting carrier 776

Configure carrier supporting carrier using a feature template 776

Configure carrier supporting carrier using CLI 777

Verify device configuration for carrier supporting carrier 779

CHAPTER 49 **TCP MSS and Clear Dont Fragment** 781

Feature history for TCP MSS and clear dont fragment 781

TCP MSS 781

Restrictions for TCP MSS and clear dont fragment 782

Configure TCP MSS and clear dont fragment 782

Configure TCP MSS and clear dont fragment using CLI commands 782

Configure TCP MSS and clear dont fragment using templates 783

Verify TCP MSS and dont clear fragment configurations 784

CHAPTER 50 **Hot Standby Router Protocol** 787

Feature history table for hot standby router protocol 787

Hot standby router protocol 787

How HSRP topologies work 788

HSRP benefits 789

Supported devices 790

Configure HSRP using the CLI 790
Verify hot standby router protocol 793

CHAPTER 51 IP DHCP Smart-Relay 797
Feature history for IP DHCP smart-relay 797
IP DHCP smart-relay 797
Benefits of IP DHCP smart-relay 798
Configure IP DHCP smart-relay agent using a CLI template 798

CHAPTER 52 DHCP Vendor Option Support 801
Feature history for DHCP vendor option support 801
DHCP vendor option support 801
Configure a DHCP vendor option using CLI command 803
Configure a DHCPv6 client option option using a CLI template 804
Configure DHCP server using templates 805

CHAPTER 53 Geofencing 809
Feature history for geofencing 809
Geofencing 810
Platforms supported for geofencing 812
Prerequisites for geofencing 812
Restrictions for geofencing 812
Configure geofencing 813
Configure geofencing using templates 813
Configure geofencing using CLI commands 814
Configuration example using CLI commands 816
Methods for verifying the geofencing configuration 817
Geofencing alarms 819

CHAPTER 54 Multitenancy 821
Feature history for Cisco Catalyst SD-WAN multitenancy 821
Cisco Catalyst SD-WAN multitenancy 821
Multitenant SD-WAN Manager 823
Multitenant SD-WAN Validator 824

Multitenant SD-WAN Controllers 824
Tenant-specific WAN edge devices 825
Feature availability 825
User roles in multitenant environment 826
Provider role 826
SD-WAN Manager views for providers 827
Tenant role 827
Provider and tenant remote servers and images 828
Supported devices, hypervisor and persona for multitenancy 828
Supported hardware specifications for multitenancy 830
Restrictions for multitenancy 830
Initial setup for multitenancy 831
Prerequisites for Cisco Catalyst SD-WAN multitenancy 831
Initial setup for Cisco Catalyst SD-WAN multitenancy 832
Create a 3-Node SD-WAN Manager multitenant cluster 833
Create a 6-node SD-WAN Manager multitenant cluster 835
Enable multitenancy on SD-WAN Manager 837
Add SD-WAN Controller 838
Expand a multitenant deployment to support more tenants and tenant devices 839
Prerequisites to expand a multitenant deployment 839
Restrictions for expanding a 3-node cluster to a 6-node cluster 840
Expand a 3-node cluster to a 6-node cluster 840
Upgrade SD-WAN Controller and Edge Device Software 841

CHAPTER 55 **Multitenancy Tenant Management** 843
Feature history for tenant management 843
Tenant management 843
Restrictions for tenant management 844
Prerequisites for adding a tenant 844
Add a new tenant 845
View tenant information 847
Delete a tenant 847
Add a tenant in a Cisco-hosted multitenant environment 848
Manage tenant WAN edge devices 849

Add a WAN edge device to a tenant network 850
Delete a WAN edge device from a tenant network 850
Manage tenant data 851
Back up tenant data 851
Backup and restore guidelines for tenant data 852
Create data backup file 853
Restore tenant data backup file 854
Monitor backup data restore 855
Delete a tenant 855
View tenants associated with a Cisco SD-WAN Controller 855
View OMP statistics per tenant on a Cisco SD-WAN Controller 856

CHAPTER 56 **Multitenant WAN Edge Devices** 857
Feature history for multitenant WAN edge devices 857
Multitenant WAN edge devices 858
Benefits of multitenant WAN edge devices 860
Device resource tiers 860
Device resource tiers 860
Supported devices for multitenant WAN edge devices 861
Restrictions for multitenant WAN edge devices 862
Enable multitenant WAN edge device deployment 863
Onboard WAN edge devices at the provider level using a template 864
Enable multitenancy on provider-level WAN edge devices using a template 864
Create a resource profile (tier) 865
Onboard tenants to a multitenant WAN edge device using a template 867
Create a tenant VPN for onboarded tenants using a template 868
Remove a tenant from a multitenant WAN edge device using a template 870
Delete a resource profile (tier) 870

CHAPTER 57 **Multitenancy Migration** 873
Feature history for multitenancy migration 873
Tenant migration in a multitenant deployment 874
Restrictions for migration of a tenant from a multitenant overlay to a single-tenant deployment 874

Migrate single-tenant Cisco Catalyst SD-WAN overlay to multitenant Cisco Catalyst SD-WAN deployment 875

Prerequisites to migrate single-tenant SD-WAN overlay to multitenant SD-WAN deployment 875

Migrate single-tenant SD-WAN overlay to multitenant SD-WAN deployment 876

Migrate a tenant from a multitenant Cisco Catalyst SD-WAN overlay to single-tenant Cisco Catalyst SD-WAN deployment 879

Prerequisites to migrate a tenant from a multitenant SD-WAN overlay to single-tenant SD-WAN deployment 879

Migrate a tenant from a multitenant SD-WAN overlay to single-tenant SD-WAN deployment 880

Migrate multitenant Cisco Catalyst SD-WAN overlay 883

Restrictions for migrating multitenant Cisco Catalyst SD-WAN overlay 883

Migrate multitenant Cisco Catalyst SD-WAN overlay 883

Verify the migration 885

CHAPTER 58 **Multitenancy Disaster Recovery** 887

Disaster recovery for a multitenant Cisco SD-WAN Manager cluster 887

Prerequisites for a multitenant disaster recovery 888

Restrictions for a multitenant disaster recovery 888

Configure a standby SD-WAN Manager cluster 888

Back up the active SD-WAN Manager cluster configuration 889

Restore SD-WAN Manager cluster using the configuration database backup 889

Verify the valid SD-WAN Manager nodes 892

Disaster recovery in an overlay network with virtual routers 892

Restore SD-WAN Manager cluster using the configuration database backup 893

Disaster recovery after a failed data center becomes operational 896

Replace faulty SD-WAN Controller 897

CHAPTER 59 **Multitenancy Dashboard** 899

Cisco SD-WAN Manager dashboard for multitenancy 899

View Cisco SD-WAN Validator health dashlet 900

View Cisco SD-WAN Manager health dashlet 900

View Cisco SD-WAN Controller health dashlet 900

View multitenant WAN edge health dashlet 900

View tenant activity, device, and network information 901

View detailed information of a tenant setup 901
View all network connections in the tenant overlay network 902
View information about device reboots 902
View state of data connections for a site 902
View interface usage for WAN edge interfaces 903
View WAN edge device counts 903
View aggregated state of WAN edge devices 903
View WAN edge device loss, latency, and jitter 904
View SAIE flow information of WAN edge devices 904
View tunnels data 904
View tenant alarms in provider dashboard 905
View tenant events in provider dashboard 905
View OMP statistics per tenant on a Cisco SD-WAN Controller 905
View tenants associated with a SD-WAN Controller 906

CHAPTER 60 **Assigning SD-WAN Controllers to Tenants in a Multitenancy Environment** 907
Feature history for assigning Cisco SD-WAN Controllers to tenants 907
Multitenancy 907
Manual tenant placement 908
Automatic tenant placement 908
Benefits of automatic tenant placement on multitenant SD-WAN Controllers 909
Restrictions for automatic tenant placement on multitenant SD-WAN Controllers 909
Prerequisites for automatic tenant placement on multitenant SD-WAN Controllers 910
Assign SD-WAN Controllers to tenants during onboarding 911
Update SD-WAN Controller placement for a tenant 913

CHAPTER 61 **Dynamic On-Demand Tunnels** 915
Feature history for dynamic on-demand tunnels 915
Dynamic on-demand tunnels 916
How on-demand tunnels work 916
How on-demand tunnels work with a transport gateway 918
Prerequisites for on-demand tunnels 918
Prerequisites: OMP settings 919
Prerequisites: Hub device traffic engineering service 920

Prerequisites: Spoke Device ECMP Limit 921
Restrictions for on-demand tunnels 922
Configure on-demand tunnels 922
Configure on-demand tunnels using control policy 922
Configure a centralized control policy for on-demand tunnels 923
Configure centralized control policy for on-demand tunnels using a CLI policy 924
Configure on-demand tunnels using a transport gateway 925
Enable on-demand tunnels on a spoke device using a configuration group 925
Enable on-demand tunnels on a spoke device using a template 926
Enable on-demand tunnels using a CLI template 926
Monitor the status of on-demand tunnels 927
View the current status of on-demand tunnels using Cisco SD-WAN Manager 927
View a chart of the on-demand tunnel status over time in Cisco SD-WAN Manager 928
View the route to a destination device 928
View OMP routes 929

CHAPTER 62 **IPv6 Functionality** 931
Configure IPv6 functionality 931
Configure IPv6 functionality for an Interface or Subinterface using templates 931
Configure IPv6 functionality for an interface or subinterface using CLI commands 932
Configure IPv6 functionality for OMP using templates 932
Configure IPv6 functionality for OMP using CLI commands 933
Configure IPv6 functionality for BGP using templates 933
Configure IPv6 functionality for BGP using CLI commands 935
Configure IPv6 functionality for VRRP using templates 935
Configure IPv6 functionality for VRRP using CLI commands 936
Configure IPv6 functionality for SNMP using templates 937
Configure IPv6 functionality for SNMP using CLI commands 938
Configure IPv6 functionality for a DHCP relay agent using templates 938
Configure IPv6 functionality for a DHCP relay agent using CLI commands 939
Configure IPv6 functionality for ACL and QoS using templates 939
Configure IPv6 functionality for ACL and QoS using CLI commands 940
Configure IPv6 functionality for a logging host using templates 941
Configure IPv6 functionality for a logging host using CLI commands 942

Configure IPv6 functionality for a prefix list using templates 942
Configure IPv6 functionality for a prefix list using CLI commands 943
Configure IPv6 functionality for a data prefix using templates 943
Configure IPv6 functionality for a data prefix using CLI commands 944
Configure IPv6 functionality for a centralized policy using templates 944
Configure IPv6 functionality for a centralized policy using CLI commands 944
Configure IPv6 functionality for a localized policy using templates 945
Configure IPv6 functionality for a localized policy using CLI commands 945

CHAPTER 63 **IPv6 in a Dual Stack Environment** 947
Dual stack environment with IPv6 as the preferred address family 947
Dual stack environment with IPv6 as the preferred address family 948
Methods for configuring a dual stack environment with IPv6 as the preferred address family 949
Configure IPv6 as the preferred address family for devices, using a configuration group 949
Configure IPv6 as the preferred address family for devices, using the Quick Connect workflow 950
Configure IPv6 as the preferred address family for devices, using CLI commands 951
Configure IPv6 as the preferred address family for SD-WAN Manager and SD-WAN Controller, using CLI commands 951
Configure IPv6 as the preferred address family for SD-WAN Manager and SD-WAN Controller, using templates 952
Monitor the use of IPv6 as the preferred address family in a dual stack environment, in SD-WAN Manager 953
Monitoring IPv6 as the preferred address family in a dual stack environment 953

CHAPTER 64 **CLI Templates for Cisco IOS XE Catalyst SD-WAN Devices** 955
Feature history: CLI templates 955
CLI templates for Cisco IOS XE Catalyst SD-WAN devices 956
Benefits of CLI templates 956
Restrictions of CLI templates 956
Using CLI templates in Cisco SD-WAN Manager 957
Device configuration-based CLI templates for Cisco IOS XE Catalyst SD-WAN devices 957
Create a CLI template using the device configuration option 957
Intent-based CLI templates for Cisco IOS XE Catalyst SD-WAN devices 958
Create a CLI template using the intent option 958

Sample configurations for CLI templates 960

CHAPTER 65 CLI Add-On Feature Templates 981

Feature history for CLI add-on feature templates 981

CLI add-on feature templates 982

Restrictions for CLI add-on feature templates 983

Create a CLI add-on feature template 983

Qualified CLI commands for CLI add-on feature templates 984

CHAPTER 66 Configuring and Monitoring P-LTE-450 MHz Modules 985

Configuring and monitoring P-LTE-450 modules 985

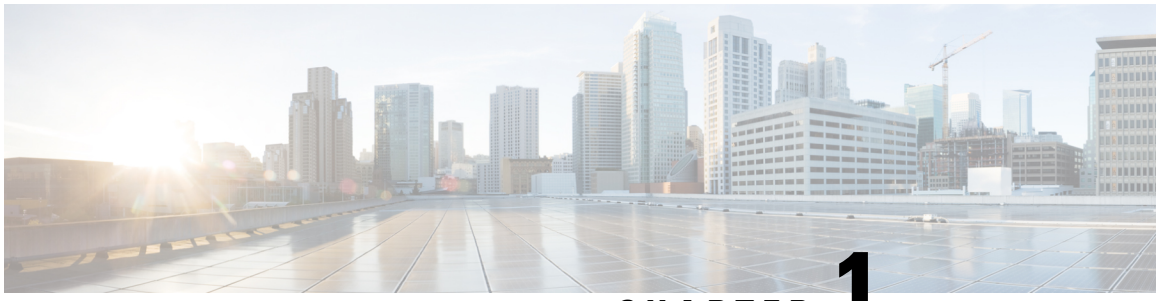
Prerequisite for configuring P-LTE-450 MHz modules 986

Restrictions for configuring P-LTE-450 modules 986

Configure a P-LTE-450 module using Configuration Group and CLI Add-on Profile 987

Monitor the P-LTE-450 module using Cisco Catalyst SD-WAN Manager 988

Monitor a P-LTE-450 module using CLI 989



CHAPTER 1

Authentication

This table describes the developments of this feature, by release.

Table 1: Feature History

Feature Name	Release Information	Description
Duo Multifactor Authentication Support	Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature lets you configure Cisco SD-WAN Manager to require Duo multifactor authentication (MFA) to verify the identity of users before they can log in to Cisco SD-WAN ManagerCisco SD-WAN Manager.
Secure Shell Authentication Using RSA Keys	Cisco IOS XE Catalyst SD-WAN Release 16.12.1b	This feature helps configure RSA keys by securing communication between a client and a Cisco Catalyst SD-WAN server.
Authorization and Accounting	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature allows you to configure authorization, which verifies and permits the commands a user enters on a device before execution, and accounting, which generates a record of the commands a user executes on the device
Posture Assessment Support	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature enables you to utilize Posture Assessment capabilites to validate the compliance of endpoints according to security policies of your enterprise. Identity Services Engine (ISE) Posture functions are integrated into Cisco 1100 Integrated Services Routers. This feature can only be configured using the Add-On feature template in Cisco SD-WAN Manager.

- Authentication, on page 2
- Authentication order, on page 2
- Authentication fallback mechanism, on page 3
- Configure authentication order, on page 4
- Duo Multi-factor authentication, on page 4
- RADIUS authentication, on page 6
- SSH authentication, on page 7
- IEEE 802.1X authentication, on page 9
- Authentication, Authorization, and Accounting, on page 18
- Posture assessment support, on page 29

Authentication

Authentication in Cisco SD-WAN Manager is a security mechanism that

- ensures only authorized devices and users can access the network, and
- integrates with AAA, RADIUS, and TACACS+ to authenticate users and control device access and operations.

Authentication order

The authentication order is a configuration setting that

- dictates the order in which authentication methods are tried when verifying user access to a Cisco IOS XE Catalyst SD-WAN device through an SSH session or a console port, and
- provides a way to proceed with authentication if the current authentication method is unavailable.

Default authentication order

The default authentication order is local, followed by radius, and then tacacs. The default authentication order works as follows:

- local: The authentication process checks for a username and passwords in the running configuration of the device.
- radius: The authentication process uses a RADIUS server to validate credentials.
- tacacs: The authentication process uses a TACACS+ server to validate credentials. For this method to work, you must configure one or more TACACS+ servers with the **system tacacs server** command. If a TACACS+ server is reachable, you are authenticated or denied access based on that server's TACACS+ database. If you have configured multiple TACACS+ servers, then the authentication process contacts one server, and if that server is not available, the process continues in sequence to the other servers. You are then authenticated or denied access based on one of the reachable TACACS+ servers.

  If none of the authentication processes succeed, access to the device is denied.

Modifying the default authentication order

You can use the **auth-order** command to modify the default authentication order. Specify one, two, or three authentication methods in the preferred order, starting with the one to be tried first. If you configure only one authentication method, it must be local.

To modify the authentication order for admin users, include the keyword **admin** in the preceding command, for e.g., **admin-auth-order** and then specify the authentication method(s).

If you do not include this command, the admin user is always authenticated locally.

Authentication fallback mechanism

You can configure authentication to fall back to a secondary or tertiary authentication mechanism when the higher-priority authentication method fails to authenticate a user, either because the user has entered invalid credentials or because the authentication server is unreachable (or all the servers are unreachable).

If the authentication order is configured as

- radius local: With radius as the default authentication, local authentication is used only when all RADIUS servers are unreachable. If an authentication attempt via a RADIUS server fails, the user is not allowed to log in even if they have provided the correct credentials for local authentication.
- local radius: With local as the default authentication, RADIUS authentication is tried when a username and matching password are not present in the running configuration on the local device.
- radius tacacs local: With radius as the default authentication, TACACS+ is tried only when all RADIUS servers are unreachable, and local authentication is tried only when all TACACS+ servers are unreachable. If an authentication attempt via a RADIUS server fails, the user is not allowed to log in even if they have provided the correct credentials for the TACACS+ server. Similarly, if a TACACS+ server denies access, the user cannot log via local authentication.

User group assignment after authentication

After the remote server authenticates a user, it assigns the user to a user group:

- If a remote server validates the authentication but does not specify a user group, it places the user in the *basic* user group.
- If a remote server validates the authentication and specifies a user group (say, X), it assigns the user to that group only. However, if that user is also configured locally and belongs to a user group (for example, group Y), the user is assigned to both groups (X and Y).
- If a remote server validates the authentication and the user is not configured locally, the system logs the user into the vshell as the *basic* user, with a home directory of /home/basic.
- If a remote server validates the authentication and the user is configured locally, the system logs the user into the vshell under their local username (for example, "eve") with a home directory of /home/*username* (for example, /home/eve).

Configure authentication order

The authentication order determines the order in which the system authenticates users, and helps users proceed with authentication if the current authentication method is unavailable.

Configure the authentication order for devices using these steps.

Procedure

Step 1 To configure AAA authentication order on a Cisco IOS XE Catalyst SD-WAN device, select the **Authentication** tab and configure the **Server Group Order** parameter.

Using AAA server groups allows you to group existing server hosts. By grouping these hosts, you can select a specific subset of configured servers to use for a particular service.

Step 2 Change the default order of authentication methods that the software uses to verify user's access to a Cisco IOS XE Catalyst SD-WAN device:

a) Click the **ServerGroups priority order** field to display the drop-down list of server groups.

The list displays groups from local, RADIUS, and TACACS authentication methods.

b) Select the groups in the order the software should use to verify users accessing the device.

Note
Select at least one group from the list.

Duo Multi-factor authentication

Duo Multi-factor authentication

Duo multi-factor authentication is a security feature that

- integrates with Cisco SD-WAN Manager and controllers to enhance user login security
- requires users to verify their identity using a second factor after entering their username and password, and
- helps prevent unauthorized access by adding a second authentication factor aligned with zero-trust principles.

Configure Duo multifactor authentication

From Cisco Catalyst SD-WAN Manager Release 20.12.1, you can configure Cisco SD-WAN Manager to require Duo multifactor authentication (MFA) to verify the identity of users before they can log in to SD-WAN Manager and other controllers.

Before you begin

Create local users in your Duo account before proceeding.

By default, Duo MFA does not apply to the admin user. To enable Duo MFA for the admin user, enable the **DUO MFA Configuration** option, and enter the admin-auth-order command in the CLI.

Once Duo authentication is set up, users are prompted to authenticate with their Duo credentials on their mobile devices and thereafter log in to SD-WAN Manager.

SD-WAN Manager does not display any message that an MFA request has been sent to the user's mobile device.

Follow these steps to set up Duo authentication.

Procedure

Step 1 Log in to the Duo Admin Panel.

Step 2 Create an Auth API application.

This step gives you the Duo integration key, secret key, and API hostname information required to complete Duo MFA configuration. See Duo Auth API for more information.

Step 3 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Step 4 Click **DUO MFA Configuration**.

If you are using Cisco Catalyst SD-WAN Manager Release 20.12.x or earlier, click **Edit**.

Step 5 Click **Enabled**.

Step 6 Configure the following options:

Field	Description
Integration Key	Enter the integration key (Ikey) for your Duo account.
Secret Key	Enter the secret key (Skey) for your Duo account.
API Hostname	Enter the API hostname (api-hostname) for your Duo account.
Server proxy	(Read only) Displays the server proxy used to access the Duo server if SD-WAN Manager is behind a firewall. Set this server proxy with the **system http proxy** or the **system https proxy** command. **Note** If SD-WAN Manager is deployed on a cloud that can be reached by an external network, a server proxy should not be set.

Step 7 Click **Save**.

Step 8 If a Cisco SD-WAN Validator or a Cisco SD-WAN Controller does not have internet access, enter the following commands in the CLI or the device template to provide access to the Duo MFA feature.

These commands configure the device with proxy information about the device on which Duo MFA is enabled.

```
vm# config
vm(config)# system aaa
vm(config-aaa)# multi-factor-auth
vm(config-multi-factor-auth)# duo
vm(config-duo)# api-hostname name
vm(config-duo)# secret-key key
vm(config-duo)# integration-key key
vm(config-duo)# proxy proxy_url
vm(config-duo)# commit
```

RADIUS authentication

Radius authentication

The Remote Authentication Dial-In User Service (RADIUS) is a distributed client/server system that

- secures networks against unauthorized access
- enables RADIUS clients on Cisco devices to send authentication requests to a central RADIUS server, and
- stores all user authentication and network service access information on the central server.

Configure RADIUS authentication using CLI commands

Authenticate a Cisco IOS XE Catalyst SD-WAN device with up to 8 RADIUS servers by configuring each server's parameters as explained here.

Procedure

Step 1 For each RADIUS server, configure the IP address and a password, or key at a minimum.

Example:

```
Device# config-transaction
Device(config)# radius server test address ipv4 10.1.1.55 acct-port 110
Device(config-radius-server)# key 33
Device(config-radius-server)# exit
Device(config)# radius server test address ipv4 10.1.1.55 auth-port 330
Device(config-radius-server)# key 55
Device(config-radius-server)#
```

Specify the key as a clear text string up to 31 characters, or provide it as an AES 128-bit encrypted key. The local device passes the key to the RADIUS server. The password must match the one used on the server.

Step 2 To add additional RADIUS servers, include the **server** and **secret-key** commands for each server.

Step 3 Optionally, configure these RADIUS parameters:

a) Set the priority of a RADIUS server that you want to use.

Priority is a means of choosing or load balancing among multiple RADIUS servers. The priority value can range from 0 to 7. The server with the lower priority number will be prioritized over those with higher numbers.

b) To change the default port numbers, use the **auth-port** and **acct-port** commands.

By default, the Cisco IOS XE Catalyst SD-WAN device uses port 1812 for authentication connections to the RADIUS server and port 1813 for accounting connections.

c) If the RADIUS server is reachable through specific interface, set that interface with the **source-interface** command.

d) Define a tag for the RADIUS server and then associate the tag with the **radius-servers** command.

A tag can be a string with 4 to 16 characters. You can tag RADIUS servers so that a specific server or servers can be used for AAA, IEEE 802.1X, and IEEE 802.11i authentication and accounting.

Note
Tags are used for grouping, describing, or finding devices. You can tag RADIUS and TACAC servers for authentication and accounting. You can add more than one tag to a device. Starting from Cisco vManage Release 20.9.1, following new tags are used in authentication:

- Viptela-User-Group: for user group definitions instead of Viptela-Group-Name.
- Viptela-Resource-Group: for resource group definitions.

e) Configure a VPN number for the server so that the device can locate it.

This is required if the RADIUS server is located in a different VPN from the Cisco IOS XE Catalyst SD-WAN device. If you configure multiple RADIUS servers, they must all be in the same VPN.

f) Change the time interval using the **timeout** command, and set a value from 1 to 1000 seconds.

When waiting for a reply from the RADIUS server, a Cisco IOS XE Catalyst SD-WAN device by default waits three seconds before retransmitting its request.

```
Device# config-transaction
 Device(config)# aaa group server radius server-10.99.144.201
 Device(config-sg-radius)# server-private 10.99.144.201 auth-port 1812 timeout 5 retransmit 3
```

SSH authentication

SSH authentication

The Secure Shell (SSH) protocol is a network protocol that

- provides secure remote access connection to network devices
- supports user authentication using public and private keys, and
- enables encrypted communication between clients and network devices.

Enabling SSH authentication

To enable SSH authentication, store your public key in your home directory of in the following location:

```
~<user>/.ssh/authorized_keys
```

A new key is generated on the client machine which owns the private key. The client decrypts any message encrypted with the SSH server's public key using the client's private key.

Restrictions for SSH authentication

SSH RSA key size

- The range of SSH RSA key sizes supported by Cisco IOS XE Catalyst SD-WAN device is from 2048 to 4096. SSH RSA key sizes of 1024 and 8192 are not supported.
- A maximum of two keys per user are allowed on Cisco IOS XE Catalyst SD-WAN devices.

Supported methods for configuring SSH authentication using CLI commands

Use these supported SSH RSA key-based authentication methods when configuring SSH authetnciation using the CLI.

SSH key based login is supported on IOS. Per user a maximum of 2 keys can be supported. Also, IOS only supports RSA based keys.

Traditional IOS CLI, allow support for:

- Key-string
- Key-hash – The key-string is base64 decoded and MD5 hash is run on it.

The transaction yang model has provision to only copy the key-hash instead of the entire key-string. SD-WAN Manager does this conversion and pushes the configuration to the device.

Configure SSH Authentication using templates

Configure SSH authentication on Cisco IOS XE Catalyst SD-WAN devices using these steps.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**, and click **Add Template**.

Note
In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

Step 3 From **Select Devices**, select the type of device for which you are creating the template.

Step 4 From **Basic Information**, choose **CISCO AAA** template.

Step 5 From **Local**, click **New User** and enter the details.

Step 6 Enter **SSH RSA Key**.

Note

You must enter the complete public key from the id_rsa.pub file in **SSH RSA Key**.

IEEE 802.1X authentication

IEEE 802.1X authentication

IEEE 802.1X is a port-based network access control (PNAC) protocol that

- prevents unauthorized network devices from gaining access to wired networks, and
- provides authentication for devices that want to connect to a wired network.

IEEE 802.1X open authentication and host modes

Any of the four host modes (single-host mode, multiple-host mode, multi-domain authentication mode, and multiauthentication mode) may be configured to allow a device to gain network access before authentication.

You can enable open authentication by entering the **authentication open** command after host mode configuration. This acts as an extension to the configured host mode. For example, if open authentication is enabled with single-host mode, then the port will allow only one MAC address. When preauthentication open access is enabled, initial traffic on the port is restricted and independent of 802.1X is configured on the port. If you don't configure any access restriction other than 802.1X on the port, then a client device will have a full access on the configured VLAN.

Note You can configure open authentication using CLI template only. You cannot configure open authentication using dot1x feature template on SD-WAN Manager.

Note From Cisco IOS XE Catalyst SD-WAN Release 17.2.1r, IEEE 802.1X is supported based on Identity-Based Networking Services (IBNS) 1.0 IOS-XE CLIs. This feature is supported on both LAN and WAN interfaces.

Restrictions for configuring IEEE 802.1X authentication

Authentication, Authorization, and Accounting

IEEE 802.1X Authentication, Authorization, and Accounting (AAA) is not supported on multiple groups.

Authentication order

Authentication order IEEE 802.1X MAB CLI cannot be disabled through SD-WAN Manager. The presence of this authentication order CLI results in a 60 second delay in MAB authentication when MAB client is online.

Open authentication

Authentication open is not supported in feature templates but can be deployed with a CLI add on template.

Prerequisites for configuring IEEE 802.1X authentication

Enable or configure these prerequisites before you configure IEEE 802.1X authentication with templates, CLI commands or configuration groups.

RADIUS

Enable RADIUS authentication servers to authenticate IEEE 802.1x services.

Configure RADIUS Accounting attributes.

Switch port

Enable IEEE 802.1X configuration on the switch port interface.

VLAN configurations

Enable these VLAN configurations to manage authenticated and unauthenticated clients:

- Restricted VLAN (or authentication rejected VLAN)
- Guest VLAN
- Critical VLAN (or authentication failed VLAN)
- Critical Voice VLAN

Enable IEEE 802.1X authentication event by VLAN ID in the Add-on template, if required.

Host-mode authentication

Enable one of these host-mode authentications:

- Single-host mode
- Multiple-host mode
- Multiple-authentication mode
- Multi-domain mode

Configure IEEE 802.1X Authentication using templates

IEEE 802.1X is a port-based network access control (PNAC) protocol that prevents unauthorized devices from accessing wired networks by authenticating devices that want to connect. Before any client can use network services, a RADIUS authentication server must authenticate each connected client. Use a Cisco AAA feature template to configure IEEE 802.1X authentication on the interface.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**. Then, click **Add Template**.

Note
In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

Step 3 Select your device from the list on the left panel.

Step 4 Select the **Cisco AAA** template and enter the **Template Name** and **Description**.

Step 5 Select the **RADIUS** tab.

a) Under **RADIUS SERVER** click **New RADIUS Server** and configure these parameters:

Parameter Name	Description
Mark as Optional Row	Check the **Mark as Optional Row** check box to mark your configuration as device-specific.
Address	Enter IP Address of the RADIUS server.
Authentication Port	Click **Authentication**, then click **Add New Authentication Entry** to configure RADIUS authentication attribute–value (AV) pairs to send to the RADIUS server during an IEEE 802.1X session. To save the entry, click **Add**.
Accounting Port	Click **Accounting**, then click **Add New Accounting Entry** to configure RADIUS accounting attribute–value (AV) pairs to send to the RADIUS server during an IEEE 802.1X session. To save the entry, click **Add**.
Timeout	Configure how long to wait for replies from the RADIUS server.
Retransmit Count	Configure how many times the system contacts this RADIUS server.
Key	Enter the RADIUS server shared key.

b) Click **Add**.

Step 6 Select the **RADIUS GROUP** tab.

a) Under **New RADIUS Group** configure these parameters:

Parameter Name	Description
VPN-ID	Enter the VPN through which the RADIUS or other authentication server is reachable.
Source Interface	Enter the interface that will be used to reach the RADIUS server.
Radius Server	Configure the Radius server.

b) Click **Add**.

Step 7 Select the **802.1X** tab and enter these parameters:

Parameter Name	Description
Authentication Param	Click **On** to enable authentication parameters.
Accounting Param	Click **On** to enable accounting parameters.

Step 8 To save this feature template, click **Save**.

Step 9 To enable this feature on your device, ensure to add these feature templates to your device template.

Note
You need to recreate the AAA feature templates as the templates created prior to Cisco vManage Release 20.5.1 fails when attached to the device.

What to do next

Create a **Switch Port** template that can be used for the Switch Port device.

Create a Switch Port template using templates

Create a **Switch Port** template for the Switch Port device.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**, and then click **Add Template**.

Note
In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

Step 3 Select your device from the list.

Step 4 Select the **Switch Port** template and enter the **Template Name** and **Description**.

Step 5 Select the **Interface** tab and click **New Interface**.

a) Configure these parameters:

Parameter Name	Description
Interface name	Enter the interface name.
Speed	Enter the interface speed.
VLAN Name	Enter the VLAN name.
VLAN ID	Enter the VLAN identifier associated with the bridging domain.
802.1X	Enable IEEE 802.1X authentication on this interface. Select "On". This will provide a further set of parameters listed below.

Parameter Name	Description
Interface PAE Type	Enter the IEEE 802.1x Interface PAE type.
Control Direction	Enter unidirectional or bidirectional authorization mode.
Host Mode	Select whether an IEEE 802.1X interface grants access to a single host (client) or to multiple hosts (clients): • Multi Auth—Grant access to one host on a voice VLAN and multiple hosts on data VLANs. • Multi Host—Grant access to multiple hosts • Single Host—Grant access only to the first authenticated host. This is the default. • Multi-Domain—Grant access to both a host and a voice device, such as an IP phone on the same switch port. **Note** These options are available only in the 'Global' Host Mode settings.
Periodic Reauthentication	Enter how often to reauthenticate IEEE 802.1X clients. By default, no reauthentication attempts are made after the initial LAN access request. Range: 0 to 1440 minutes

b) Click **Advanced Options** and configure these parameters:

Parameter Name	Description
Authentication Order	Enter the order of authentication methods to use when authenticating devices for connection to the IEEE 802.1X interface. The default authentication order is RADIUS, then MAC authentication bypass (MAB).
MAC Authentication Bypass	Select to enable MAC authentication bypass (MAB) on the RADIUS server and to authenticate non-IEEE 802.1X–compliant clients using a RADIUS server.
Port Control Mode	Enter the port control mode to enable IEEE 802.1X port-based authentication on the interface. Auto- Configure this to enable IEEE 802.1X authentication and start the port in unauthorized state. This allows only EAPOL frames to be sent and received through the port.
Voice VLAN ID	Configure the Voice VLAN ID.
Critical VLAN	Enter the critical VLAN (or authentication failed VLAN) for IEEE 802.1x-compliant clients. Configure network access when RADIUS authentication or the RADIUS server fails.
Critical Voice VLAN	Enable the critical voice VLAN.
Guest VLAN	Configure guest VLAN to drop non-IEEE 802.1X enabled clients, if the client is not in the MAB list.

Parameter Name	Description
Restricted VLAN	Enter the restricted VLAN (or authentication failed VLAN) for IEEE 802.1x-compliant clients. Configure limited services to IEEE 802.1X–compliant clients that failed RADIUS authentication.

c) Click **Add**.

Step 6 To save this feature template, click **Save**.

Step 7 To enable this feature on your device, ensure to add these feature templates to your device template.

IEEE 802.1X Open Authentication using CLI commands

You can configure IEEE 802.1X Open Authentication using the CLI add-on template:

```
Device# config-transaction
Device(config)# interface GigabitEthernet2
Device(config-if)# authentication open
```

Configure IEEE 802.1X Authentication using CLI commands

For configuring IEEE 802.1x using CLI commands, two sets of configuration are required:

- Global AAA commands
- Interface level commands

Procedure

Step 1 Configure the Global AAA commands.

a) Enable or disable IEEE 802.1X globally:

```
Device(config)# aaa authentication dot1x default group radius-0
Device(config)# aaa authorization network default group radius-0
Device(config)# dot1x system-auth-control
Device(config)# radius-server dead-criteria time 10 tries 3
Device(config)# radius-server deadtime 15
```

b) Enable accounting:

```
Device(config)# aaa accounting dot1x default start-stop group radius-0
```

Step 2 Configure the interface level commands.

a) Enable or disable IEEE 802.1X on port-basis:

```
Device(config-if)# dot1x pae authenticator
Device(config-if)# authentication port-control auto
```

b) Enable or disable MAB on port-basis and then select host-mode:

```
Device(config-if)# mab
Device(config-if)# authentication host-mode  <multi-auth | multi-domain | multi-host | single-host>
```

c) Configure voice VLAN:

```
Device(config-if)# switchport voice vlan <vlan-id>
```

d) Select IEEE 802.1X control direction:

```
Device(config-if)# authentication control-direction <both | in>
```

e) Enable periodic re-authentication and corresponding re-authentication interval and inactivity timeout time:

```
Device(config-if)# authentication periodic
Device(config-if)# authentication timer reauthenticate <internal-in-sec>
Device(config-if)# authentication timer inactivity <timeout-in-sec>
```

f) Configure authentication orders on per-port basis:

```
Device(config-if)# authentication order dot1x mab
```

g) Specify the restricted VLAN and then specify the guest VLAN:

```
Device(config-if)#  authentication event fail action authorize vlan <vlan-id>
Device(config-if)# authentication event no-response action authorize vlan <vlan-id>
```

h) Specify the critical VLAN:

```
Device(config-if)# authentication event server dead action authorize vlan <vlan-id>
```

i) Enable the critical voice VLAN feature:

```
Device(config-if)# authentication event server dead action authorize voice
```

Configure Switch Port using a configuration group

Configure Switch Port settings using these steps.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure a Switch Port feature in a Service profile.

Table 2: Switch Port

Field	Description
Age Out Time	Enter how long an entry is in the MAC table before it ages out. Set the value to 0 to prevent entries from timing out. Range: 0, 10 through 1000000 seconds Default: 300 seconds
Configure Interface	

Field	Description
Interface Name	Enter the name of the interface to associate with the bridging domain, in the format `geslot/port`.
Mode	Choose the switch port mode. • **access**: Configure the interface as an access port. You can configure only one VLAN on an access port, and the port can carry traffic only for one VLAN. When you choose **access**, the following field appears: **Switchport Access Vlan**: Enter the VLAN number, which can be a value from 1 through 4094. • **trunk**: Configure the interface as a trunk port. You can configure one or more VLANs on a trunk port, and the port can carry traffic for multiple VLANs. When you choose **trunk**, the following fields appear: • **Allowed Vlans**: Enter the number of the VLANs for which the trunk can carry traffic and a description for the VLAN. • **Switchport Trunk Native Vlan**: Enter the number of the VLAN allowed to carry untagged traffic.
Shutdown	Enable the interface. By default, an interface is disabled.
Speed	Enter the speed of the interface.
Duplex	Choose **full** or **half** to specify whether the interface runs in full-duplex or half-duplex mode.
Port Control	Choose the port control mode to enable IEEE 802.1X port-based authentication on the interface. • **auto**: Enables IEEE 802.1X authentication and starts the port in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port changes from down to up or when an EAPOL-start frame is received. The device requests the identity of the supplicant and starts relaying authentication messages between the supplicant and the authentication server. Each supplicant attempting to access the network is uniquely identified by the device by using the supplicant MAC address. • **force-unauthorized**: Causes the port to remain in the unauthorized state, ignoring all attempts by the supplicant to authenticate. The device cannot provide authentication services to the supplicant through the port. • **force-authorized**: Disables IEEE 802.1X authentication and causes the port to change to the authorized state without any authentication exchange required. The port sends and receives normal traffic without IEEE 802.1X-based authentication of the client.
Voice VLAN	Enter the Voice VLAN ID.

Field	Description
Pae Enable	The Cisco Catalyst SD-WAN device acts as a port access entity (PAE), allowing authorized network traffic and preventing unauthorized network traffic ingressing to and egressing from the controlled port.
MAC Authentication Bypass	Enable this option to allow MAC authentication bypass (MAB) on the RADIUS server and to authenticate non-IEEE 802.1X–compliant clients using a RADIUS server.
Host Mode	Choose whether an IEEE 802.1X interface grants access to a single host (client) or to multiple hosts (clients). • **single-host**: Grant access only to the first authenticated host. This is the default. • **multi-auth**: Grant access to one host on a voice VLAN and multiple hosts on data VLANs. • **multi-host**: Grant access to multiple hosts. • **multi-domain**: Grant access to both a host and a voice device, such as an IP phone on the same switch port.
Enable Periodic Reauth	Enable periodic re-authentication. By default, this option is enabled.
Inactivity	Enter the inactivity timeout time in seconds. Default: 60 seconds
Reauthentication	Enter the re-authentication interval in seconds.
Control Direction	Choose **both** (bidirectional) or **in** (unidirectional) authorization mode.
Restricted VLAN	Enter the restricted VLAN (or authentication-failed VLAN) for IEEE 802.1x-compliant clients. Configure limited services to IEEE 802.1X-compliant clients that failed RADIUS authentication.
Guest VLAN	Enter the guest VLAN to drop non-IEEE 802.1X enabled clients, if the client is not in the MAB list.
Critical VLAN	Enter the critical VLAN (or authentication-failed VLAN) for IEEE 802.1x-compliant clients. Configure network access when RADIUS authentication or the RADIUS server fails.
Enable Voice	Enable the critical voice VLAN.
Configure Static Mac Address	
MAC Address	Enter the static MAC address to map to the switch port interface.
Interface Name	Enter the name of the switch port interface.
VLAN ID	Enter the number of the VLAN for the switch port.

What to do next

Also see Deploy a configuration group.

Authentication, Authorization, and Accounting

Restrictions to configure authorization and accounting

If you enter a configuration and press enter before you choose a value from an enumeration, the CLI shows a choice sub-menu. In this scenario, the system does not send the final value for authorization.

You cannot use the **load merge** and **load override** commands when authorization is configured.

Commands that you configure using load or rollback are not authorized or accounted.

Configure AAA using a configuration group

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure a AAA feature in a System profile.

a) Configure users.

Table 3: Local

Field	Description
Enable AAA Authentication	Enable authentication parameters.
Accounting Group	Enable accounting parameters.
Add AAA User	
Name	Enter a name for the user. It can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any uppercase letters. The following usernames are reserved, so you cannot configure them: backup, basic, bin, daemon, games, gnats, irc, list, lp, mail, man, news, nobody, proxy, quagga, root, sshd, sync, sys, uucp, and www-data. Also, names that start with viptela-reserved are reserved.

Field	Description
Password	Enter a password for the user. The password is an MD5 digest string, and it can contain any characters, including tabs, carriage returns, and linefeeds. For more information, see Section 9.4 in RFC 7950, The YANG 1.1 Data Modeling Language. Each username must have a password. Users are allowed to change their own passwords. The default password for the admin user is admin. We strongly recommended that you change this password.
Confirm Password	Re-enter the password for the user.
Privilege	Select between privilege level 1 or 15. • Level 1: User EXEC mode. Read-only, and access to limited commands, such as the ping command. • Level 15: Privileged EXEC mode. Full access to all commands, such as the reload command, and the ability to make configuration changes. By default, the EXEC commands at privilege level 15 are a superset of those available at privilege level 1.
Add Public Key Chain	
Key String*	Enter the authentication string for a key.
Key Type	Choose **ssh-rsa**.

b) Configure RADIUS servers.

Table 4: RADIUS

Field	Description
Address*	Enter the IP address of the RADIUS server host.
Acct Port	Enter the UDP port to use to send 802.1X and 802.11i accounting information to the RADIUS server. Range: 1 - 65534. Default: 1813
Auth Port	Enter the UDP destination port to use for authentication requests to the RADIUS server. Default: 1812 Range: 1 - 65534
Retransmit	Enter the number of times the device transmits each RADIUS request to the server before giving up. Default: 3 Range: 0 - 100

Field	Description
Timeout	Enter the number of seconds a device waits for a reply to a RADIUS request before retransmitting the request. Default: 5 seconds Range: 1 through 1000
Key*	Enter the key the Cisco IOS XE Catalyst SD-WAN device passes to the RADIUS server for authentication and encryption.
Key Type	Choose Protected Access Credential (PAC) key.

c) Configure TACACS servers.

Table 5: TACACS Server

Field	Description
Address*	Enter the IP address of the TACACS+ server host.
Port	Enter the UDP destination port to use for authentication requests to the TACACS+ server. If the server is not used for authentication, configure the port number to be 0. Default: 49
Timeout	Enter the number of seconds a device waits for a reply to a TACACS+ request before retransmitting the request. Default: 5 seconds Range: 1 through 1000
Key*	Enter the key the Cisco IOS XE Catalyst SD-WAN device passes to the TACACS+ server for authentication and encryption. You can type the key as a text string from 1 to 31 characters long, and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the AES encryption key used on the TACACS+ server.

d) Configure accounting rules.

Table 6: Accounting

Field	Description
Rule Id*	Enter the accounting rule ID.

Field	Description
Method*	Specifies the accounting method list. Choose one of the following: • **commands**: Provides accounting information about specific, individual EXEC commands associated with a specific privilege level. • **exec**: Provides accounting records about user EXEC terminal sessions on the network access server, including username, date, and start and stop times. • **network**: Runs accounting for all network-related service requests. • **system**: Performs accounting for all system-level events not associated with users, such as reloads. **Note** When system accounting is used and the accounting server is unreachable at system startup time, the system will not be accessible for approximately two minutes.
Level	Choose the privilege level (1 or 15). Accounting records are generated only for commands entered by users with this privilege level.
Start Stop	Enable this option to if you want the system to send a start accounting notice at the beginning of an event and a stop record notice at the end of the event.
Use Server-group*	Choose a previously configured TACACS group. The parameters that this accounting rule defines are used by the TACACS servers that are associated with this group.

e) Configure authorization parameters.

Table 7: Authorization

Field	Description
Server Auth Order*	Choose the authentication order. It dictates the order in which authentication methods are tried when verifying user access to a Cisco IOS XE Catalyst SD-WAN device through an SSH session or a console port.
Authorization Console	Enable this option to perform authorization for console access commands.
Authorization Config Commands	Enable this option to perform authorization for configuration commands.
Add Authorization Rule	
Rule Id*	Enter the authorization rule ID.
Method*	Choose **Commands**, which causes commands that a user enters to be authorized.
Level	Choose the privilege level (1 or 15) for commands to be authorized. Authorization is provided for commands entered by users with this privilege level.
If Authenticated	Enable this option to apply the authorization rule parameters only to the authenticated users. If you do not enable this option, the rule is applied to all users.

Field	Description
Use Server-group*	Choose a previously configured TACACS group. The parameters that this authorization rule defines are used by the TACACS servers that are associated with this group.

f) Configure 802.1x parameters.

What to do next

Also see Deploy a configuration group.

Methods of configuring AAA using templates

You can configure authentication, authorization, and accounting (AAA) using Cisco SD-WAN Manager template and push these settings to selected devices of the same type. This helps you to conveniently configure several devices of the same type at once.

You can use the AAA template for Cisco Catalyst SD-WAN Validators, Cisco SD-WAN Manager instances, Cisco Catalyst SD-WAN Controllers, Cisco IOS XE Catalyst SD-WAN devices.

Cisco IOS XE Catalyst SD-WAN devices support configuration of AAA in combination with RADIUS and TACACS+ servers.



Note You must configure a local user with a secret key via the template if you are using PPP or using MLPPP with CHAP.

Create a template

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Device Templates**, and click **Create Template**.

Note
In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

Step 3 From the **Create Template** drop-down list, select **From Feature Template**.

Step 4 From the **Device Model** drop-down list, select the type of device for which you are creating the template.

Step 5 Select **Basic Information**.

Step 6 To create a custom template for AAA, select **Factory_Default_AAA_CISCO_Template** and click **Create Template**.

The AAA template form appears. The top of the form has fields where you name the template, and the bottom has fields where you define AAA parameters.

Step 7 In the **Template Name** field, enter a name for the template.

The name can include up to 128 alphanumeric characters.

Step 8 In the **Template Description** field, enter a description of the template.

The description can include up to 2048 alphanumeric characters.

Step 9 When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the **Scope** drop-down list to the left of the parameter field and select one of these:

Parameter Scope	Scope description
Device Specific (indicated by a host icon)	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Cisco IOS XE Catalyst SD-WAN device to a device template. When you click **Device Specific**, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each subsequent row corresponds to a device and defines the values of the keys for that device. Upload the CSV file when you attach a Cisco IOS XE Catalyst SD-WAN device to a device template. For more information, see Create a Template Variables Spreadsheet. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.
Global (indicated by a globe icon)	Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

Configure local access for users and user groups

You can configure local access to a device for users and user groups. Local access provides access to a device if RADIUS or TACACS+ authentication fails.

Procedure

Step 1 To configure local access for individual users, select **Local**.

Step 2 To add a new user, click **+ New User**, and configure the following parameters:

Parameter Name	Description
Name	Enter a name for the user. The name must start with a letter and be between 1 and 128 characters. Use only lowercase letters, numbers 0 through 9, hyphens (-), underscores (_), or periods (.). The name should not contain any uppercase letters. These usernames are reserved, so you cannot configure them: backup, basic, bin, daemon, games, gnats, irc, list, lp, mail, man, news, nobody, proxy, quagga, root, sshd, sync, sys, uucp, and www-data. In addition to these, names starting with viptela-reserved are reserved. **Note** From Cisco Catalyst SD-WAN Manager Release 20.18.1, the character limit for local user accounts remains restricted to 32 characters. However, for TACACS users, usernames extend up to 128 characters.
Password	Enter a password for the user. Each username must have a password. Users are allowed to change their own passwords. The default password for the admin user is admin. We strongly recommended changing this password. **Note** When configuring local users using a Cisco SD-WAN Manager AAA template, SD-WAN Manager uses a Cisco type 9 password type that uses the scrypt algorithm for hashing the passwords of local users. If you configure local users using a device CLI template or a CLI add-on template, you can choose other Cisco password types for hashing of local user passwords. For more information about type 6 encryption, refer to the *Cisco Catalyst SD-WAN Configuration Groups Reference Guide*.
Privilege Level 1 OR 15	Select between privilege level 1 or 15. • **Level 1**: User EXEC mode. Read-only, and access to limited commands, such as the **ping** command. • **Level 15**: Privileged EXEC mode. Full access to all commands, such as the **reload** command, and the ability to make configuration changes. By default, the EXEC commands at privilege level 15 are a superset of those available at privilege level 1.
SSH RSA Key(s)	Click **+ Add** to add SSH RSA keys. Paste your SSH RSA key in the field. To remove a key, click **-**. Devices support a maximum of 2 SSH RSA keys.

Step 3 Click **Add** to add the new user. Click **+ New User** again to add additional users.

To configure local access for user groups, first place the user into either the basic or operator group. The admin is automatically placed in the netadmin group. Then you configure user groups.

Step 4 From **Local**, select **User Group**.

Step 5 Click **+ New User Group**, and configure the following parameters:

Parameter Name	Description
Name	Name of an authentication group. The name must start with a letter and be between 1 and 128 characters. Use only lowercase letters, numbers 0 through 9, hyphens (-), underscores (_), or periods (.). The name should not contain any uppercase letters. SD-WAN Manager provides three standard user groups, basic, netadmin, and operator. The user admin is automatically placed in the group netadmin and is the only user in this group. All users learned from a RADIUS or TACACS+ server are placed in the basic group. Users in the basic group have the same permissions to perform tasks, as in the operator group. You cannot configure these groups as they are reserved: adm, audio, backup, bin, cdrom, dialout, dip, disk, fax, floppy, games, gnats, input, irc, kmem, list, lp, mail, man, news, nogroup, plugdev, proxy, quagga, quaggavty, root, sasl, shadow, src, sshd, staff, sudo, sync, sys, tape, tty, uucp, users, utmp, video, voice, and www-data. Also, group names starting with the string viptela-reserved are reserved.
Feature Type	Click **Preset** to display a list of preset roles for the user group. Click **Custom** to display a list of authorization tasks that have been configured.
Feature	The feature table lists the roles for the user group. These roles are Interface, Policy, Routing, Security, and System. Each role allows the user group to read or write specific portions of the device's configuration and to execute specific types of operational commands. Click the appropriate boxes for **Read**, **Write**, or **None** to assign privileges to the group for each role.

Step 6 Click **Add** to add the new user group.

Step 7 To add another user group, click **+ New User Group** again.

Step 8 To delete a user group, click the trash icon. You cannot delete the three standard user groups, basic, netadmin, and operator.

Configure RADIUS authentication

Configure RADIUS authentication if you are using RADIUS in your deployment.

Procedure

Step 1 To configure a connection to a RADIUS server, from **RADIUS**, click **+ New Radius Server**, and configure the following parameters:

Table 8:

Parameter Name	Description
Address	Enter the IP address of the RADIUS server host.

Parameter Name	Description
Authentication Port	Enter the UDP destination port to use for authentication requests to the RADIUS server. If you do not use the server for authentication, set the port number to 0. Default: Port 1812
Accounting Port	Enter the UDP port to send 802.1X and 802.11i accounting information to the RADIUS server. Range: 0 to 65535. Default: 1813.
Timeout	Enter the number of seconds a device should wait for a reply to a RADIUS request before retransmitting the request. Default: 5 seconds. Range: 1 to 1000
Retransmit Count	Enter the number of times the device transmits each RADIUS request to the server before giving up. Default: 5 seconds.
Key (Deprecated)	Enter the Cisco IOS XE Catalyst SD-WAN devicekey the passes to the RADIUS server for authentication and encryption. Type the key as a text string from 1 to 31 characters. The system encrypts it immediately. Alternatively, type an AES 128-bit encrypted key. Use the same AES encryption key as on the RADIUS server.

Step 2 Click **Add** to add a new RADIUS server.

Step 3 To add another RADIUS server, click **+ New RADIUS Server** again.

Step 4 To remove a server, click the trash icon.

CLI equivalent:

```
Device(config)# radius server 10.99.144.201
Device1(config-radius-server)# retransmit 5
Device(config-radius-server)# timeout 10
```

Configure TACACS+ authentication

Configure TACACS+ authentication if you are using TACACS+ in your deployment.

Procedure

Step 1 To configure a connection to a TACACS+ server, from **TACACS**, click **+ New TACACS Server**.

Step 2 Configure these parameters:

Parameter Name	Description
Address	Enter the IP address of the TACACS+ server host.
Port	Enter the UDP destination port to use for authentication requests to the TACACS+ server. If the server is not used for authentication, configure the port number to be 0. Default: Port 49
Key	Enter the key the Cisco IOS XE Catalyst SD-WAN device passes to the TACACS+ server for authentication and encryption. You can type the key as a text string from 1 to 31 characters long, and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the AES encryption key used on the TACACS+ server.

Configure authentication order

The authentication order determines the order in which the system authenticates users, and helps users proceed with authentication if the current authentication method is unavailable.

Configure the authentication order for devices using these steps.

Procedure

Step 1 To configure AAA authentication order on a Cisco IOS XE Catalyst SD-WAN device, select the **Authentication** tab and configure the **Server Group Order** parameter.

Using AAA server groups allows you to group existing server hosts. By grouping these hosts, you can select a specific subset of configured servers to use for a particular service.

Step 2 Change the default order of authentication methods that the software uses to verify user's access to a Cisco IOS XE Catalyst SD-WAN device:

a) Click the **ServerGroups priority order** field to display the drop-down list of server groups.

The list displays groups from local, RADIUS, and TACACS authentication methods.

b) Select the groups in the order the software should use to verify users accessing the device.

Note
Select at least one group from the list.

Configure authorization

You can configure authorization, that causes a TACACS+ server to authorize commands that the user enters on a device before the commands can be executed. Authorization is based on the policies that are configured in the TACACS+ server and on the parameters that you configure on the **Authorization** tab.

Before you begin

The TACACS+ server and the local server must be configured first in the authentication order on the **Authentication** tab.

Procedure

Step 1 To configure authorization, choose the **Authorization** tab, click **+ New Authorization Rule**.

Step 2 Configure the following parameters:

Parameter Name	Description
Console	Enable this option to perform authorization for console access commands.
Config Commands	Enable this option to perform authorization for configuration commands.
Method	Choose **Command** to authorize the commands entered by the user.
Privilege Level 1 OR 15	Choose the privilege level (1 or 15) for commands to be authorized. Authorization is provided for commands entered by users with this privilege level.
Groups	Choose a previously configured TACACS group. TACACS servers associated with this group use the parameters defined by this authorization rule.
Authenticated	Enable this option to apply the parameters defined by this authorization rule only to authenticated users. If you do not enable this option, the rule is applied to all users.

Step 3 Click **Add** to add the new authorization rule.

Step 4 To add another authorization rule, click **+ New Accounting Rule** again.

Step 5 To remove an authorization rule, click the trash icon on the right side of the line.

CLI commands for configuring authorization:

```
system
   aaa
     aaa authorization console
     aaa authorization config-commands
     aaa authorization exec default list-name method
     aaa authorization commands level default list-name method
```

Configure accounting

Configure accounting so that the TACACS+ server generates a record of commands executed by the user on a device.

Before you begin

Ensure to configure the TACACS+ server as the first option and local server as the second option in the authentication order on the **Authentication** tab. Refer to Authentication order, on page 2 for details.

Procedure

Step 1 To configure accounting, choose the **Accounting** tab and click **+ New Accounting Rule**.

Step 2 Configure these parameters:

Table 9: Accounting

Parameter Name	Description
Method	Choose **Command** to log commands executed by a user.
Privilege Level 1 OR 15	Choose the privilege level (1 or 15). Accounting records are generated only for commands entered by users with this privilege level.
Enable Start-Stop	Click **On** to have the system send a start accounting notice at the beginning of an event and a stop record notice at the end of the event.
Groups	Choose a previously configured TACACS group. TACACS servers associated with this group use the parameters defined by this accounting rule.

Step 3 Click **Add** to add the new accounting rule.

Step 4 To add another accounting rule, click **+ New Accounting Rule** again.

Step 5 To remove an accounting rule, click the trash icon on the right side of the line.

CLI commands for configuring authorization:

```
system
  aaa
    aaa accounting exec default start-stop group group-name
    aaa accounting commands level default start-stop group group-name
    aaa accounting network default start-stop group group-name
    aaa accounting system default start-stop group group-name
```

Posture assessment support

Posture assessment support

Cisco AnyConnect Posture Assessment is a posture assessment solution that

- installs on endpoints to enforce security policies downloaded from an ISE server,
- checks endpoint conditions such as anti-malware, anti-spyware, anti-virus, application, and USB compliance, and
- reports compliance status to the ISE server to control network access based on posture evaluation.

Network endpoint validation and posture assessment workflow

Endpoint validation plays a critical role in network security by ensuring that devices connecting to a company's network comply with established security policies. The posture module enforces these policies on endpoints that are connected to the network. When Cisco 1100 Integrated Services Routers communicate with Cisco Identity Services Engine (ISE), they require authentication interaction. Use IEEE 802.1X as the recommended standard for posture assessment authentication. If required, MAC Authentication Bypass (MAB) can also be used.

After successful authentication and authorization using redirect Access Control Lists (ACLs), the posture assessment process begins. Once the system completes posture assessment and authentication, the ISE policy set triggers the RADIUS Change of Authorization (CoA) process to re-authenticate or re-authorize endpoints and enforce new or updated policies.

Following successful posture assessment and CoA re-authentication, endpoints and the Cisco ISR 1100 router receive full access to the network, ensuring that only compliant devices interact with network resources.

Restrictions for Posture Assessment

- Only 8 port Cisco 1100 Integrated Services Routers support ACL functions such as dACL and redirect ACL.
- ACL and Access Control Entry (ACE) rules do not support compare operations, such as >, <, >=, <=
- Up to 120 dACL ACEs are supported, and 64 Redirect ACL ACEs are supported.
- Port ACL and IPv6 ACL are not supported.
- IP option and IP fragment ACL are not supported.
- Per-VLAN device-tracking is not supported.
- Only limited per-port device tracking policy options such as glean and address tracking are allowed.

Configure posture assessment using CLI commands

Use the CLI Add-on template to configure AAA, IEEE 802.1x, posture assessment and redirect ACL and device-tracking.

Before you begin

Ensure these requirements are met before proceeding to configure posture assessment support:

- Basic IEEE 802.1x authentication process should be functional.
- Change of Authorization (CoA) should be supported.
- Redirect ACL, downloadable ACL (dACL) and critical ACL should be available.
- Device tracking policy (for identity) should be supported.
- URL redirect should be supported.

Refer instructions to create a CLI Add-on template and then add the configuration explained next.

Procedure

Step 1 Configure AAA.

Example:

```
aaa new-model
radius server ISE1

address ipv4 198.51.100.255 auth-port 1812 acct-port 1813
key cisco

aaa group server radius ISE
 server name ISE1
!
aaa authentication dot1x default group ISE
aaa authorization network default group ISE
aaa accounting dot1x default start-stop group ISE

interface vlan 15
 ip address 198.51.100.1 198.51.100.254

interface GigabitEthernet0/1/0
 switchport mode access
 switchport access vlan 15

ip radius source-interface vlan 15
```

Note
`aaa new-model` is enabled by default on Cisco Catalyst SD-WAN and you cannot configure it. However, you can configure it on a non SD-WAN image.

Step 2 Configure IEEE 802.1x authentication and authorization.

Example:

```
policy-map type control subscriber simple_dot1x
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x
!
interface GigabitEthernet0/1/7
 switchport access vlan 22
 switchport mode access
 access-session closed
 access-session port-control auto
 dot1x pae authenticaton
 service-policy type control subscriber simple_dot1x
!
interface Vlan22
 ip address 198.51.100.1 198.51.100.254
```

Note
The IEEE 802.1x endpoint is connected to GigabitEthernet0/1/7.

Step 3 Configure posture assessment and redirect ACL.

Example:

```
ip http server
ip http secure-server
```

```
ip access-list extended ACL-POSTAUTH-REDIRECT
10 deny tcp any host 192.0.2.255
20 deny tcp any any eq domain
30 deny udp any any eq domain
40 deny udp any any eq bootpc
50 deny udp any any eq bootps
60 permit tcp any any eq www
70 permit tcp any any eq 443
```

Step 4 Configure device tracking.

Example:

```
!
device-tracking policy tracking_test
 security-level glean
 no protocol ndp
 no protocol dhcp6
 tracking enable
!
interface GigabitEthernet0/1/7
 device-tracking attach-policy tracking_test
```

Note
The IP address mentioned belongs to ISE.

Step 5 Configure CoA reauthentication and dACL on ISE.

a) Create a downloadable ACL and define the ACEs in it.

ACL name: TEST_IP_PERMIT_ALL

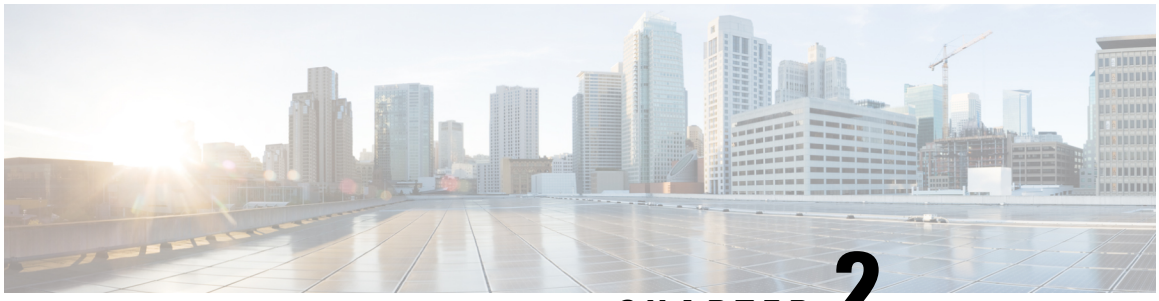
ACEs: permit ip any any

b) Create an authorization result and choose the downloadable ACL as dACL.

c) Navigate to **Administration** > **System** > **Settings** > **Policy Settings**, and in **Policy Sets** configuration, select the authorization result as authorization policy.

Step 6 After creating the CLI Add-On template, attach it to a device template.

SD-WAN Manager pushes all the configuration in the device template onto your device.



CHAPTER 2

RADIUS and TACACS

- Feature history for RADIUS and TACACS, on page 33
- RADIUS, on page 34
- TACACS, on page 34
- Restrictions for cloud multitenant with on-prem per-tenant AAA and provider AAA, on page 35
- Prerequisites for cloud multitenant with on-prem per-tenant AAA and provider AAA, on page 35
- Configuring remote AAA , on page 36
- Configure RADIUS and TACACS for multitenancy using CLI, on page 40
- Verify RADIUS and TACACS, on page 41

Feature history for RADIUS and TACACS

Table 10: Feature history table

Feature name	Release information	Description
RADIUS and TACACS Support for Multitenancy	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature enables support for Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System (TACACS) authentication in a multitenant deployment on WAN edge devices.
Configure RADIUS and TACACS Servers to Receive Authentication Requests Over Management VPN 512	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	This feature provides increased security by allowing you to configure tenants to send and receive AAA traffic over WAN transport VPN 0 or management VPN 512.

Note Some configurations and protocols are identified as insecure and is a security risk for Cisco devices. Existing deployments continue to function, but new installations require intentional enablement. For more information on remediation, refer to Resilient Infrastructure: Cisco Catalyst SD-WAN and Routing

RADIUS

A RADIUS is a distributed client and server system that

- secures networks with authorized access,
- runs on supported Cisco devices, and
- sends authentication requests to a central RADIUS server.

The RADIUS server stores user authentication and network service access information.

TACACS

A TACACS is a security application that

- provides centralized validation of users accessing an access point,
- delivers separate and modular authentication, authorization, and accounting, and
- integrates each service with separate databases.

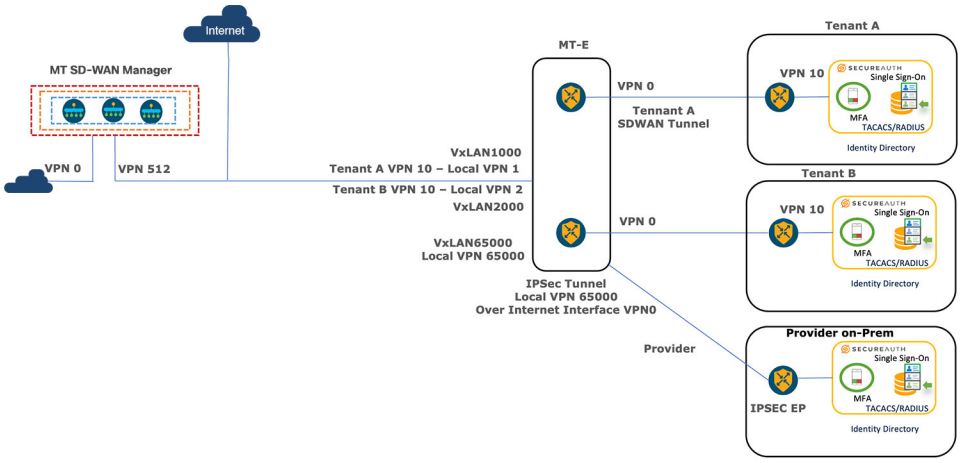
TACACS within AAA

TACACS administered through AAA security services provides these functions:

- Authentication: Complete control through login/password dialog, challenge-response, and messaging support.
- Authorization: Fine-grained privilege control, including access, session limits, protocol support, and command restrictions.
- Accounting: Collects and reports administrator activity (identities, times, executed commands, packets, bytes) for billing, auditing, and reporting.

Cloud multitenancy with on-prem tenant and provider AAA

This illustration shows the architecture of the cloud multitenancy with on-prem per tenant and provider AAA.



Restrictions for cloud multitenant with on-prem per-tenant AAA and provider AAA

Lists restrictions for multitenant deployment in Cisco SD-WAN Manager

- A provider's RADIUS and TACACS server cannot be shared with the tenant.
- VxLAN tunnels must use the VPN 512 interface as the underlay.
- A provider can have tenant configurations only through a device or feature template.

Prerequisites for cloud multitenant with on-prem per-tenant AAA and provider AAA

- Ensure that a multitenant edge connector is onboarded in Cisco SD-WAN Manager, and it is located on the same premises as the controllers.
- Ensure that the edge connector is on the same premises as the controllers.
- Ensure that Cisco SD-WAN Manager is configured with VPN 512 interface.
- Ensure that in a Cisco SD-WAN Manager cluster, there is a VxLAN tunnel created between each Cisco SD-WAN Manager node and the edge connector.
- Ensure that RADIUS and TACACS server authentication is within the tenant network.
- Ensure that multiple RADIUS and TACACS servers are used for the same tenant.
- Ensure that a tenant's RADIUS and TACACS server is on-prem or cloud-hosted.
- Ensure that you configure an external AAA server and provide mapping between the user and the Viptela groups to authentication. For example, Viptela-Group-Name as basic, tenantadmin, or operator.

Configuring remote AAA

Use these steps to configure remote AAA:

- Enable multitenancy, on page 36
- Configure a tenant, on page 36
- Configure remote AAA
- Configure RADIUS
- Configure TACACS

Enable multitenancy

Cisco SD-WAN Manager reboots in multitenant mode, and when a provider user logs in to Cisco SD-WAN Manager, the provider dashboard appears.

For information about configuring AAA using feature templates for a single tenant, see Configuring AAA using Cisco SD-WAN Manager Template.

Use these steps to enable multitenancy.

Procedure

Step 1 From Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Step 2 Click **Edit** adjacent to the **Tenancy Mode**.

If you are using Cisco Catalyst SD-WAN Manager Release 20.12.x or earlier, click **Edit**.

Step 3 Click **Multitenant**.

Step 4 In the **Domain** field, enter the domain name of the service provider (for example, managed-sp.com).

Step 5 Enter a **Cluster Id** (for example, cluster-1 or 123456).

Step 6 Click **Save**.

If you are using Cisco Catalyst SD-WAN Manager Release 20.12.x or earlier, click **Proceed** to confirm that you want to change the tenancy mode.

Configure a tenant

To onboard the edge connector in a Cisco SD-WAN Manager provider, perform these steps:

Procedure

Step 1 From the Cisco SD-WAN Manager, choose **Administration** > **Tenant Management**.

Step 2 Click **Edit** adjacent to the tenant.

The **Edit Tenant** window is displayed

Step 3 Enter the description in the **Description** field.

Step 4 Enter the edge number in the **Forecasted Edge** field.

Step 5 Enter the sub-domain URL in the **URL Subdomain** field.

Step 6 Enable the **Edge Connector** option.

Step 7 Choose the **Edge Connector IP** from the drop-down list.

Step 8 Choose the VXLAN tunnel endpoint from the **Edge Connector VTEP Interface Name** drop-down list.

For a cloud deployment, it is essential to provision the Cloud-hosted SD-WAN Control Components and gateway with the third interface GigabitEthernet3 for AAA.

When selecting the VXLAN tunnel endpoint from the Edge Connector VTEP Interface Name drop-down list, choose **GigabitEthernet3**. Selecting any other interface, such as VPN 0 or VPN 512, might result in misconfiguration.

Step 9 Click **Save**.

Configure remote AAA

Cisco SD-WAN Manager reboots in multitenant mode, and when a provider user logs in to Cisco SD-WAN Manager, the provider dashboard appears.

Use these steps to configure Remote AAA:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**.

Step 2 Click **Remote AAA**.

Expand the **Remote AAA** tab to configure remote AAA.

Step 3 Enter the order in which to attempt different authentication methods in the **Authentication Order** field.

Step 4 Choose the option in **Authentication Fallback** to fallback if higher-priority authentication fails.

Step 5 Choose the **Admin Authentication Order** to authenticate a tenantadmin user according to the authentication order.

Step 6 Enable or disable audit logs in the **Disable Audit Logs** field.

Step 7 Enable or disable user accounting in the **Enable/disable user accounting** field.

Step 8 Click **Save**.

Configure RADIUS

Use these steps to configure RADIUS servers in Cisco SD-WAN Manager for centralized authentication, authorization, and accounting:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage**.

Step 2 Click **Remote AAA**.

Step 3 Expand the **RADIUS** tab to configure a RADIUS server.

Step 4 Enter the duration to wait for replies from the RADIUS server in the **Timeout** field.

Step 5 Enter the number of times you want to contact a RADIUS server in the **Retransmit Count** field.

Step 6 Click **New RADIUS Server** to add a new RADIUS server.

Table 11: Radius server details

Field	Description
RADIUS Server Details	
Address	IP address of the RADIUS server.
Authentication Port	Port to connect to the RADIUS server.
Accounting Port	Port used to connect to the server.
Key	Password to access the RADIUS server.
Secret Key	AES encrypted key to access the RADIUS server.
Priority	Enter the server priority.
VPN ID	Enter the VPN in which the RADIUS server. **Note** This option is available in Cisco Catalyst SD-WAN Manager Release 20.15.x and earlier.
VPN IP Subnet	Enter the VPN IP subnet (VXLAN tunnel VPN IP subnet) in which the RADIUS server is located. **Note** This option is available in Cisco Catalyst SD-WAN Manager Release 20.15.x and earlier.
Network Connectivity **Note** This Network Connectivity option is available from Cisco Catalyst SD-WAN Manager Release 20.16.1.	

Field	Description
Source VPN	Choose from these VPN options, the location of the RADIUS server: • **0**: Transport VPN. • **512**: Management VPN. Configure these fields only if you have specified the tenant to manage the AAA server. These fields do not appear if the multitenant setup is configured to be managed by the provider. • (Optional) **Source Subnet**: Enter the VPN IP subnet that is unique within the tenant network. • (Optional) **Destination VPN**: Enter the VPN in which the RADIUS server is located.

Step 7 Click **Save and Add**.

Configure TACACS

Use these steps to configure TACACS:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**.

Step 2 Click **Remote AAA**.

Step 3 Expand the **TACACS** tab to configure TACACS.

Step 4 Enter the duration to wait for replies from the TACACS server in the **Timeout** field.

Step 5 Choose the TACACS authentication type from the **Authentication** drop-down list.

- ASCII
- PAP

Step 6 Click **New TACACS Server** to add a new TACACS server.

Field	Description
TACACS Server Details	
Address	Enter the IP address of the TACACS server.
Authentication Port	Enter the port to connect to a TACACS server.
Key	Enter the password to access the TACACS server.
Secret Key	Enter the AES encrypted key to access the TACACS server.

Field	Description
Priority	Enter the TACACS server priority.
VPN ID	Enter the VPN in which the TACACS server. **Note** This option is available in Cisco Catalyst SD-WAN Manager Release 20.15.1 and earlier.
VPN IP Subnet	Enter the VPN IP subnet in which the TACACS server is located. **Note** This option is available in Cisco Catalyst SD-WAN Manager Release 20.15.1 and earlier.
Network Connectivity **Note** The Network Connectivity option is available from Cisco Catalyst SD-WAN Manager Release 20.16.1.	
Source VPN	Choose from these VPN options, the location of the TACACS server: • **0**: Transport VPN. • **512**: Management VPN. Configure these fields only if you have specified the tenant to manage the AAA server. These fields do not appear if the multitenant setup is configured to be managed by the provider. • (Optional) **Source Subnet**: Enter the VPN IP subnet that is unique within the tenant network. • (Optional) **Destination VPN**: Enter the VPN in which the TACACS server is located.

Step 7 Click **Add**.

Configure RADIUS and TACACS for multitenancy using CLI

The following is a sample of RADIUS and TACACS configuration on Cisco IOS XE Catalyst SD-WAN devices using the CLI.

```
device# interface GigabitEthernet4
 description VTEP Interface
 no shutdown
 arp timeout 1200
 ip address 172.1.1.101 255.255.255.0
```

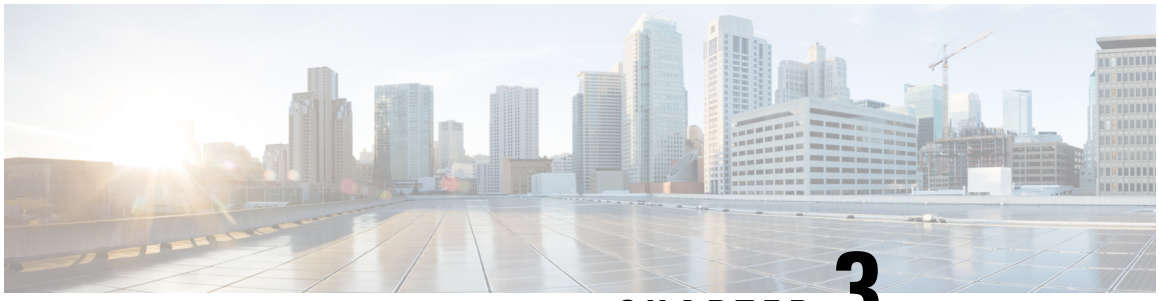
```
 no ip redirects
 ip mtu 1500
 load-interval 30
 mtu  1500
 negotiation auto
exit
```

Verify RADIUS and TACACS

Use the **show ip interface brief** command to verify the AAA configuration:

```
device# show ip interface brief | i VPN IP SUBNET of VxTunnel
```

Here, *VPN IP SUBNET of VxTunnel* is the subnet configured under **Tenant** > **Administration** > **Remote AAA**.



CHAPTER 3

Users and Access

This table describes the developments of this feature, by release.

Table 12: Feature history

Feature name	Release Information	Description
Inactivity lockout	Cisco Catalyst SD-WAN Manager Release 20.12.1	You can configure Cisco SD-WAN Manager to lock out users who have not logged in for a designated number of consecutive days.
Unsuccessful login attempts lockout	Cisco Catalyst SD-WAN Manager Release 20.12.1	You can configure Cisco SD-WAN Manager to lock out users who have made a designated number of consecutive unsuccessful login attempts within a designated period.
Configure Sessions in Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco vManage Release 20.3.1	You can set client session timeouts, session lifetimes, server session timeouts, and enable the maximum number of user sessions in Cisco SD-WAN Manager.

- Users and access, on page 43
- Account lockout, on page 50
- User sessions, on page 53
- Ciscotac user access, on page 56

Users and access

Users and access

Users and access is a feature in SD-WAN Manager that

- controls and manages the authorization permissions for users on Cisco IOS XE Catalyst SD-WAN devices

- involves defining users who are allowed to log in
- enables grouping these users into user groups, and
- associating privileges with each group to specify the commands users are authorized to execute.

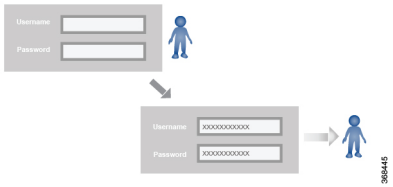
Users and user groups

Users are entities that represent individuals or processes authorized to access and operate Cisco IOS XE Catalyst SD-WAN devices.

User groups are collections of users based on common roles or privileges to control authorization permissions on Cisco IOS XE Catalyst SD-WAN.

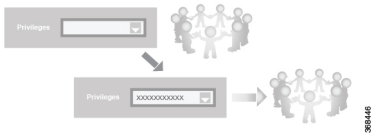
Users and user groups

All users who are permitted to perform operations on a Cisco IOS XE Catalyst SD-WAN device device must have a login account. For the login account, you configure a username and a password on the device itself. These allow the user to log in to that device. A username and password must be configured on each device that a user is allowed to access.

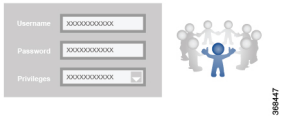


The Cisco Catalyst SD-WAN software provides one standard username, admin, which is a user who has full administrative privileges, similar to a UNIX superuser. By default, the admin username password is admin. You cannot delete or modify this username, but you can and should change the default password.

User groups pool together users who have common roles, or privileges, on the Cisco IOS XE Catalyst SD-WAN device. As part of configuring the login account information, you specify which user group or groups that user is a member of. You do not need to specify a group for the admin user, because this user is automatically in the user group netadmin and is permitted to perform all operations on the SD-WAN device.



The user group itself is where you configure the privileges associated with that group. These privileges correspond to the specific commands that the user is permitted to execute, effectively defining the role-based access to the Cisco Catalyst SD-WAN software elements.



Standard user groups

Cisco Catalyst SD-WAN software provides standard user groups and allows creation of custom user groups as needed.

- **basic**: The basic group is a configurable group and can be used for any users and privilege levels. This group is designed to include users who have permission to both view and modify information on the device.
- **operator**: The operator group is also a configurable group and can be used for any users and privilege levels. This group is designed to include users who have permission only to view information.
- **netadmin**: The netadmin group is a non-configurable group. By default, this group includes the admin user. You can add other users to this group. Users in this group are permitted to perform all operations on the device.
- **network_operations**: From Cisco vManage Release 20.9.1, network_operations user group is supported. The network_operations group is a non-configurable group. Users in this group can perform all non-security-policy operations on the device and only view security policy information. For example, users can create or modify template configurations, manage disaster recovery, and create non-security policies such as application aware routing policy or CFlowD policy.
- **security_operations**: From Cisco vManage Release 20.9.1, security_operations user group is supported. The **security_operations** group is a non-configurable group. Users in this group can perform all security operations on the device and only view non-security-policy information. For example, users can manage umbrella keys, licensing, IPS signatures auto update, TLS/SSL proxy settings, and so on.

Users of the **network_operations** group are authorized to apply policies to a device, revoke applied policies, and edit device templates. Users of the **security_operations** group require **network_operations** users to intervene on day-0 to deploy security policy on a device and on day-N to remove a deployed security policy. However, after a security policy is deployed on a device, **security_operations** users can modify the security policy without needing the **network_operations** users to intervene.



Note All user groups, regardless of the read or write permissions selected, can view the information displayed on the Cisco SD-WAN Manager Dashboard screen.

Only admin users can view running and local configuration. Users associated with predefined operator user group do not have access to the running and local configurations. The predefined user group operator has only read access for the template configuration. If you need only a subset of admin user privileges, then you need to create a new user group with the selected features from the features list with both read and write access and associate the group with the custom user.



Note Previously, users with roles other than netadmin, such as basic, network_operations, security_operations, and operator, could execute arbitrary commands on the host system, which posed a significant security risk. To resolve this issue, only specific users (root, vmanage-admin, ciscotacro, ciscotacrw) were given permission to execute the commands. Now, only ciscotacro and ciscotacrw users have access to the **request execute** function, while netadmin group members are permitted access only when Cisco SD-WAN Manager is enabled. This change blocks unauthorized users from alternative shell or command execution methods, enforces proper restrictions, and mitigates the security risk.

User group permissions

You can add, edit, view, or delete users and user groups based on the permissions listed here.

- Only an admin or a user who has Manage Users write permission can add, edit, or delete users and user groups from SD-WAN Manager.
- Each user group can have read or write permission. Write permission includes read permission.
- All user groups, regardless of the read or write permissions selected, can view the information displayed in the SD-WAN Manager dashboard.

Table 13: User group permissions for different device types

Permissions	Sections
User group permissions related to Cisco IOS XE Catalyst SD-WAN device configuration.	User group permissions for Cisco IOS XE Catalyst SD-WAN devices, on page 90
User group permissions related to Cisco Catalyst Wireless Gateway device configuration.	User group permissions for Cisco Catalyst Wireless Gateway devices, on page 109

Configure users using CLI commands

You can use the CLI to configure user credentials on each device. This way, you can create additional users and give them access to specific devices.

The credentials you create for a user through the CLI can be different from SD-WAN Manager credentials. You can create different credentials for a user on each device. All Cisco IOS XE Catalyst SD-WAN device users with the netadmin privilege can create a new user.

To create a user account, configure the username and password, and place the user in a group.

This example shows the addition of user, Bob, to an existing group:

```
Device(config)# system aaa user bob group basic
```

Similarly this example shows the addition of user, Alice, to a new group `test-group`:

```
Device(config)# system aaa user test-group
Device(config)# system aaa user alice group test-group
```

Table 14: username, password, and group name requirements

username	The username can be 1 to 128 characters long, and must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any uppercase letters. Some usernames are reserved, you cannot configure them. For a list of reserved usernames, see the **aaa** configuration command in the Cisco Catalyst SD-WAN Command Reference Guide.

password	Each username must have a password, and users are allowed to change their own password. The CLI immediately encrypts the string and does not display a readable version of the password. When a user logs in to a Cisco IOS XE Catalyst SD-WAN device, they have five chances to enter the correct password. After the fifth incorrect attempt, the user is locked out of the device, and must wait for 15 minutes before attempting to log in again.
group name	Group name is the name of a standard SD-WAN group (**basic**, **netadmin**, or **operator**) or of a group configured with the **usergroup** command (discussed below). If an admin user changes the permission of a user by changing their group, and if that user is currently logged in to the device, the user is logged out and must log back in again.



Note Enclose any user passwords that contain the special character ! in double quotation marks (“ “). If a double quotation is not included for the entire password, the config database (?) treats the special character as a space and ignores the rest of the password.

For example, if the password is C!sc0, use “C!sc0”.

Configure password for admin users using CLI commands

The factory-default password for the admin username is admin and we recommend to modify this password the first time you configure a Cisco IOS XE Catalyst SD-WAN device.

Procedure

Step 1 Modify the factory-default password for admin the first time you configure a Cisco IOS XE Catalyst SD-WAN device:

Example:

```
Device(config)# username admin password $9$3/IL3/UF2F2F3E$J9NKBeKlWrq9ExmHk6F5VAiDMOFQfD.QPAmMxDdxz.c
```

Step 2 Configure the password as an ASCII string. The CLI immediately encrypts the string and does not display a readable version of the password.

Example:

```
Device# show run | sec username
username admin privilege 15 secret 9 $9$3F2M2l2G2/UM3U$TGe2kqoIibdIRDEj4cOVKbVFP/o4vnlFAwWnmzx1rRE
username appnav privilege 15 secret 9 $9$3l2L2V.F2VIM1k$p3MBAyBtGxKf/yBGnUSHQ1g/ae1QhfIbieg28buJJGI
username eft secret 9 $9$3FMJ3/UD2VEL2E$d.kE4.an41v7wEhrQc6k5wIfE9M9WkNAJxUvbbempS.
username lab privilege 15 secret 9 $9$3l.J3FUD2F.E2.$/AiVn9PmLCpgr6ExVrE7dH979Wu8nbdtAfbzUtfysg.
username test secret 9 $9$1l2J3l6D3/QL3k$7PZOXJAJOI1os5UI763G3XcpVhXlqcwJ.qEmgmx4X9g
username vbonagir privilege 15 secret 9 $9$3/2K2UwF2lQF3U$VbdQ5bq18590rRthF/NnNnOsw.dw1/EViMTFZ5.ctus
Device#
```

Step 3 If you are using RADIUS to perform AAA authentication, you can configure a specific RADIUS server to verify the password:

```
Device(config)# radius server tag
```

The tag is a string that you defined with the **radius server tag**command, as described in the Cisco Catalyst SD-WAN Command Reference Guide.

Create user groups

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**.
Step 2 Click **User Groups**.
Step 3 Click **Add User Group**.
Step 4 Enter **User Group Name**.
Step 5 Select the **Read** or **Write** check box against feature that you want to assign to a user group.
Step 6 Click **Add**.
Step 7 You can view the new user group in the left navigation path. Click **Edit** to edit the existing read or write rules.
Step 8 Click **Save**.

Create user groups using CLI commands

Create additional custom groups and configure privilege roles that the group members have.

The Cisco Catalyst SD-WAN software provides default user groups: **basic**, **netadmin**, **operator**, **network_operations**, and **security_operations**. The username **admin** is automatically placed in the **netadmin** user group.

Procedure

Step 1 To create a custom group with specific authorization, configure the group name and privileges:

Example:

```
Device(config)# aaa authentication login user1 group radius enable
Device(config)# aaa authentication login user2 group radius enable
Device(config)# aaa authentication login user3 group radius enable
Device(config)#
```

Group name can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any uppercase letters. Some group names are reserved, so you cannot configure them. For a list of them, see the aaa configuration command.

If a remote RADIUS or TACACS+ server validates authentication but does not specify a user group, the user is placed into the basic user group. If a remote server validates authentication and specifies a user group (say, X) using VSA Cisco SD-WAN-Group-Name, the user is placed into that user group only. However, if that user is also configured locally and belongs to a user group (say, Y), the user is placed into both the groups (X and Y).

Step 2 Under task, list the roles that the group members have.

The role can be one or more of the following: interface, policy, routing, security, and system.

Delete a user group

You can delete a user group when it is no longer needed. For example, you might delete a user group that you created for a specific project when that project ends.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**.

Step 2 Click **User Groups**.

Step 3 Click the name of the user group you wish to delete.

Note
You cannot delete any of the default user groups—basic, netadmin, operator, network_operations, and security_operations.

Step 4 Click **Trash** icon.

Step 5 To confirm the deletion of the user group, click **OK**.

Edit user group privileges

You can edit group privileges for an existing user group.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**.

Step 2 Click **User Groups**.

Step 3 Select the name of the user group whose privileges you wish to edit.

Note
You cannot edit privileges for the any of the default user groups—basic, netadmin, operator, network_operations, and security_operations.

Step 4 Click **Edit**, and edit privileges as needed.

Step 5 Click **Save**.

If an admin user changes the privileges of a user by changing their group, and if that user is currently logged in to the device, the user is logged out and must log back in again.

Account lockout

Account Lockout

Account Lockout is a configuration category within Cisco SD-WAN Manager that

- defines security features to control and manage user access to Cisco SD-WAN Manager, and
- includes mechanisms such as inactivity lockout and unsuccessful login attempts lockout.

Account Lockout options

From Cisco Catalyst SD-WAN Manager Release 20.12.1, a netadmin user can enable the following account lockout options:

- Inactivity lockout: You can configure SD-WAN Manager to lock out users who have not logged in for a designated number of consecutive days. Locked out users cannot log in to SD-WAN Manager until an administrator unlocks their accounts. See Configure Account Lockout.
- Unsuccessful login lockout: You can configure SD-WAN Manager to prevent users who make a designated number of consecutive unsuccessful login attempts within a designated time period from logging in to SD-WAN Manager until a configured amount of time passes or an administrator unlocks their user accounts.

  By default, SD-WAN Manager locks out users for 15 minutes after five consecutive unsuccessful login attempts within 15 minutes. After the lockout period expires, a user can log in with the correct user name and password.

  See Configure unsuccessful login attempts lockout.

Configure Account Lockout

Note To unlock a user account, see Reset a Locked User.

Use this procedure to lock out users.

Before you begin

From Cisco Catalyst SD-WAN Manager Release 20.12.1, you can configure Cisco SD-WAN Manager to lock out users who have not logged in for a designated number of consecutive days.

Cisco SD-WAN Manager marks locked out users as inactive, and they cannot log in again until an administrator unlocks their accounts in Cisco SD-WAN Manager.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Step 2 Click **Account Lockout** and enable the **Inactive days before locked out** option.

In Cisco Catalyst SD-WAN Manager Release 20.12.x, locate **Account Lockout**, click **Edit**, and enable **Inactive days before locked out**.)

Step 3 Configure the following options:

Field	Description
Inactive days before account locked out	Enable this option and enter the number of consecutive inactive days after which Cisco SD-WAN Manager locks out a user. An inactive day is defined as a day on which a user does not log in to Cisco SD-WAN Manager. Valid values are 2 through 90.
Number of failed login attempts before lockout	Enter the number of failed login attempts after which Cisco SD-WAN Manager locks out a user. Possible values: 1 through 3600 Default: 3600
Duration within which the failed attempts are counted (minutes)	Enter the period, in minutes, during which the system counts consecutive unsuccessful login attempts. For example, if you set this period to 10 minutes, and set the number of failed login attempts before lockout to 5, Cisco SD-WAN Manager locks out a user if the user makes 5 consecutive unsuccessful login attempts within 10 minutes. Possibe values: 1 through 60 Default: 60
Cooldown or Lockout period	This option controls whether Cisco SD-WAN Manager automatically resets a user who is locked because of unsuccessful login attempts. This option is enabled by default. If you disable it, an administrator must manually unlocks the account of a locked-out user. **a.** Click **Enabled** adjacent to **Cooldown or Lockout period**. **b.** In the **Lockout Interval (minutes)** field, enter the number of minutes after which Cisco SD-WAN Manager automatically resets a locked out user. Possible values: 1 through 60 Default: 15

Step 4 Click **Save**.

Configure unsuccessful login attempts lockout

Use this procedure to configure Cisco SD-WAN Manager to lock out users after a specified number of consecutive unsuccessful login attempts within a defined timeframe

Before you begin

From Cisco Catalyst SD-WAN Manager Release 20.12.1, you can configure Cisco SD-WAN Manager to lock out users who have made a designated number of consecutive unsuccessful login attempts within a period of time.

Note From Cisco Catalyst SD-WAN Manager Release 20.13.1 or later, use the procedure described in Configure Account Lockout, on page 50.

Cisco SD-WAN Manager prevents locked out users from logging in again until a configured amount of time has passed or an administrator unlocks their accounts in Cisco SD-WAN Manager.

Note To unlock a user account, see Reset a Locked User

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Step 2 Click **Account Lockout**.

Step 3 In the **Lockout on failed login attempts** row, click **Edit**.

Step 4 Configure the following options:

Field	Description
Number of failed login attempts before lockout	Enter the number of failed login attempts after which Cisco SD-WAN Manager locks out a user. Possible values: 1 through 3600 Default: 3600

Field	Description
Duration within which the failed attempts are counted (minutes)	Enter the period, in minutes, during which the system counts consecutive unsuccessful login attempts. For example, if you set this period to 10 minutes, and set the number of failed login attempts before lockout to 5, Cisco SD-WAN Manager locks out a user if the user makes 5 consecutive unsuccessful login attempts within 10 minutes. Possibe values: 1 through 60 Default: 60
Cooldown or Lockout period	This option controls whether Cisco SD-WAN Manager automatically resets a user who is locked because of unsuccessful login attempts. This option is enabled by default. If you disable it, an administrator must manually unlocks the account of a locked-out user. **a.** Click **Enabled** adjacent to **Cooldown or Lockout period**. **b.** In the **Lockout Interval (minutes)** field, enter the number of minutes after which Cisco SD-WAN Manager automatically resets a locked out user. Possible values: 1 through 60 Default: 15

User sessions

User sessions

A user session is a period of interaction between a user and a system that

- begins when the user successfully authenticates or logs in
- maintains state and context for the user's activities, and
- ends when the user logs out or the session expires due to inactivity or timeout.

Restrictions for configuring user sessions

Client Session Timeout

You can edit **Client Session Timeout** in a multitenant environment only if you have provider access.

Session Lifetime

You can edit **Session Lifetime** in a multitenant environment only if you have provider access.

Server Session Timeout

You cannot access **Server Session Timeout** in a multitenant environment, even if you have provider access or tenant access.

Configure a client session timeout in SD-WAN Manager

Use this procedure to set a client session timeout in Cisco SD-WAN Manager. When a timeout is set, such as no keyboard or keystroke activity, the client is automatically logged out of the system.

Before you begin

You can edit Client Session Timeout in a multitenant environment only if you have a Provider access.

Procedure

Step 1 From the Cisco SD-WAN Managermenu, choose **Administration** > **Settings**.
Step 2 Click **User Sessions**.
Step 3 Under **Client Session Timeout**, click **Session Timeout**.
Step 4 Specify the timeout value, in minutes.
Step 5 Click **Save**.

Configure a session lifetime in SD-WAN Manager

Use this procedure to specify how long to keep your session active by setting the session lifetime, in minutes.

A session lifetime indicates the amount of time for which a session can be active. If you keep a session active without letting the session expire, you will be logged out of the session in 24 hours, which is the default session timeout value.

The default session lifetime is 1440 minutes or 24 hours.

Before you begin

You can edit Session Lifetime in a multitenant environment only if you have a Provider access.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
Step 2 Click **User Sessions**.
Step 3 In the **SessionLifeTime Timeout (minutes) field**, specify the session timeout value, in minutes, from the drop-down list.

Step 4 Click **Save**.

Configure the Server Session Timeout in SD-WAN Manager

Use this procedure to configure the **Server Session Timeout** in Cisco SD-WAN Manager.

The **Server Session Timeout** indicates how long the server should keep a session running before it expires due to inactivity. The default server session timeout is 30 minutes.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Step 2 Click **User Sessions**.

Step 3 In **Server Session Timeout Timeout(minutes)** field, specify the timeout value, in minutes.

Step 4 Click **Save**.

Set the maximum sessions per user role

You can configure the maximum number of concurrent login sessions for each configured user role. This maximum value applies to all users assigned to that role.

If the **Max Sessions Per User** value for the netadmin role is set to 3, then each user assigned to the netadmin role can have up to 3 concurrent login sessions across the platform. If a fourth session is initiated by one of those users, an error message appears.

Range for **Max Sessions Per User**: 1 to 255.

Default: If undefined, there is no limit on the number of concurrent sessions for that role.

The value also applies to CLI sessions.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Users and Access** > **Roles** .

The **Max user sessions value** is displayed for each defined role, including both default and custom roles.

Step 2 Click the role name, edit the **Max user sessions** value, and click **Update**.

Note
From Cisco Catalyst SD-WAN Manager Release 20.18.1, the previous method for changing this value in **Settings** > **Trust and Privacy** is no longer supported. If a **Max user sessions** value has been defined on your system by that method, that value serves as the maximum value for all user roles until changed.

Ciscotac user access

Ciscotac user access

Cisco Edge software provides two special user accounts, ciscotacro and ciscotacrw, for use by the Cisco Support team. These user accounts

- operate using a consent-token challenge and token response authentication, requiring a new token for each login session, and
- can access SD-WAN Manager web server, SSH Terminal on SD-WAN Manager using a token, including SD-WAN Validator, SD-WAN Controllers, and Cisco vEdge devices.

You can use these user accounts in both cloud and on-premises installations.

Ciscotac user accounts and privileges

The default CLI templates include configuration for the ciscotacro and ciscotacrw users. These users are enabled by default but you can disable them if needed.

- ciscotacro user: This account belongs to the operator user group and has read-only privileges. This account allows monitoring configurations but does not permit operations that modify network configurations.
- ciscotacrw user: This account belongs to the netadmin user group and has read-write privileges. This account allows modification of network configurations. Only this user can access the root shell using a consent token.

To allow the network administrator can access system shell, use the **tools consent-token** command. Starting Cisco Catalyst SD-WAN Control Components Release 20.12.x, the **request support ciscotac** command is deprecated.

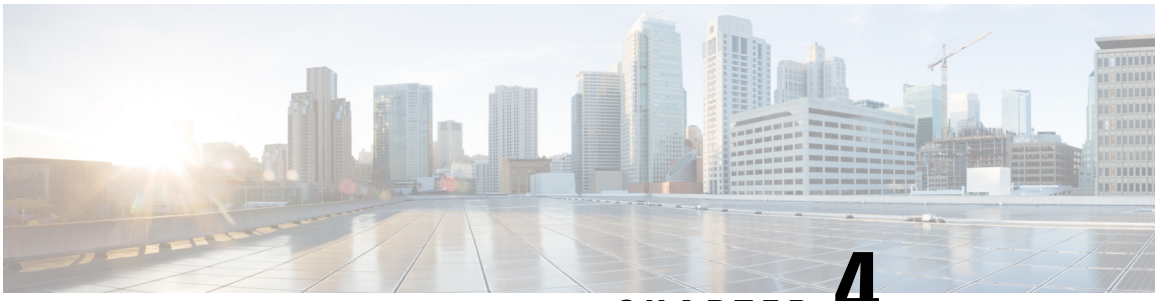
Limitations for Ciscotac user access

Ciscotac user sessions

- Only 16 concurrent sessions are supported for the ciscotacro and ciscotacrw users.
- The session duration is restricted to four hours. It is not configurable.
- The inactivity timer functionality closes user sessions that have been idle for a specified period of time. This feature is enabled by default and the timeout value is 30 minutes. However, the user configuration includes the option of extending the inactivity timer.

Removing Ciscotac users

You can remove the ciscotacro and ciscotacrw users. If removed, you can open a case and share temporary login credentials or share the screen with the Cisco Support team for troubleshooting an issue.



CHAPTER 4

Password Management

This table describes the developments of this feature, by release.

Table 15: Feature History

Feature Name	Release Information	Description
Hardened passwords	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	You can enable the password policy rules in Cisco SD-WAN Manager. After password policy rules are enabled, Cisco SD-WAN Manager enforces the use of strong passwords.
	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	This feature lets you configure Cisco SD-WAN Manager to enforce predefined-medium security or high-security password criteria.
Type 6 Passwords on Cisco IOS XE SD-WAN Routers	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	This feature allows you to use type 6 passwords that use secure reversible encryption. This encryption provides enhanced security by using more secure algorithms to encrypt your passwords. These passwords are supported for the templates detailed in Supported platforms and templates, on page 61.

- Hardened passwords, on page 58
- Type 6 passwords, on page 61

Hardened passwords

Restrictions for passwords

Password attempts and password change

You are allowed five consecutive password attempts before your account is locked. After six failed password attempts, you are locked out for 15 minutes. If you enter an incorrect password on the seventh attempt, you are not allowed to log in, and the 15-minute lock timer starts again.

If your account is locked, wait for 15 minutes for the account to automatically be unlocked. Alternatively, reach out to an administrator to reset the password, or have an administrator unlock your account.



Note Your account gets locked even if password is not entered multiple times. When you do not enter anything in the password field, it is considered as invalid or wrong password.

Password change policy

When resetting your password, you must set a new password. You cannot reset a password using an old password.

In Cisco vManage Release 20.6.4, Cisco vManage Release 20.9.1 and later releases, a user that is logged out, or a user whose password has been changed locally or on the remote TACACS server cannot log in using their old password. The user can log in only using their new password.

Password requirements

SD-WAN Manager enforces these password requirements after you have enabled the password policy rules.

The following password requirements are applicable to releases before Cisco vManage Release 20.9.1:

- Must contain a minimum of eight characters and a maximum of 32 characters.
- Must contain at least one uppercase character.
- Must contain at least one lowercase character.
- Must contain at least one numeric character.
- Must contain at least one of the following special characters: # ? ! @ $ % ^ & * -.
- Must not contain the full name or username of the user.
- Must not reuse a previously used password.
- Change at least four characters so their positions differ from those in your old password.

From Cisco IOS XE Catalyst SD-WAN Release 17.9.1a:

Table 16: Password criteria and requirements

Password criteria	Requirements
Medium security	• Must contain a minimum of eight characters • Must contain no more than 32 characters • Must contain at least one lowercase character • Must contain at least one uppercase character • Must contain at least one numeric character • Must contain at least one of the following special characters: # ? ! @ $ % ^ & * - • Must not be identical to any of the last five passwords used • Must not contain the full name or username of the user
High security	• Must contain a minimum of 15 characters • Must contain no more than 32 characters • Must contain at least one lowercase character • Must contain at least one uppercase character • Must contain at least one numeric character • Must contain at least one of the following special characters: # ? ! @ $ % ^ & * - • Must not be identical to any of the last five passwords used • Must not contain the full name or username of the user • Change at least eight characters so their positions differ from those in your old password

Enable Password Policy

Enable password policy rules in Cisco SD-WAN Manager to enforce use of strong passwords.

After you enable a password policy rule, the passwords that are created for new users must meet the requirements defined by the rule. From Cisco vManage Release 20.9.1, you are prompted to change your password the next time you log in if your existing password does not meet the requirements defined by the rule.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Step 2 Click **Password Policy**.

Step 3 Perform one of these actions, based on your SD-WAN Manager release:

a) For releases before Cisco vManage Release 20.9.1, click **Enabled**.

b) From Cisco vManage Release 20.9.1, click **Medium Security** or **High Security** to choose the password criteria.

By default, **Password Policy** is set to **Disabled**.

Step 4 Click **Save**.

Reset a locked user using SD-WAN Manager

If a user is locked out after multiple incorrect password attempts, an administrator with the necessary rights can update the user's password. You can unlock the user account by either changing the password or by getting the user account unlocked.

Note Only a netadmin user or a user with the User Management Write role can perform this operation.

Follow these steps to reset a locked user.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**).

Step 2 Choose the user account you want to unlock.

Step 3 Click **. . .** and choose **Reset Locked User**.

Step 4 Click **OK** to confirm that you want to reset the password of the locked user. This operation cannot be undone.

Alternatively, click **Cancel** to cancel the operation.

Reset a locked user using CLI commands

Use this procedure to reset a locked user by changing the password using CLI commands.

Procedure

Step 1 Log in to the device as an admin user.

Step 2 Run the following command:

Example:

```
Device# request aaa unlock-user username
```

Step 3 When prompted, enter a new password for the user.

Type 6 passwords

Type 6 passwords

Type 6 password is an encryption method that

- enables secure reversible encryption for authentication, authorization, and accounting (AAA) and Simple Network Management Protocol (SNMP) configurations using the advanced encryption scheme (AES) algorithm
- uses a symmetric key to encrypt and decrypt stored passwords, and
- is the default password format in SD-WAN Manager templates released Cisco vManage Release 20.4.1 onwards.

Reversible encryption is the process by which a password is encrypted with a reversible, symmetric encryption algorithm. To check if the password entered by the user is valid, the password is decrypted and compared to the user-input password. To perform this encryption, the symmetric encryption algorithm requires a key that you can provide. The encryption algorithm used is advanced encryption standard (AES) algorithm in Cipher Block Chaining (CBC) mode with a PKCS#5 padding. This algorithm is used for AAA features such as RADIUS, TACACS+, SNMP, and TrustSec.

Type 6 passwords in SD-WAN Manager

SD-WAN Manager encrypts the passwords and sends the passwords to the router over a secure tunnel. The router encrypts the passwords in type 6 format and stores them on the device. You cannot use type 6 passwords on Viptela software.

Use type 6 passwords to reduce the risks of attacks on password integrity. When you upgrade your devices to Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, all AAA, RADIUS key, and TACACS+ keys are encrypted to type 6.

Note SD-WAN Manager encrypted passwords show up as either 6 or 8 whereas, Cisco IOS XE devices use encryption streams defined as type 0, type 5, type 6, type 8, and similar types. On the other hand, SD-WAN Manager runs on Viptela OS which is based on Linux. Linux uses hashing and encryption schemes. Encrypted passwords on SD-WAN Manager starting with 6 refer to sha512-crypt. Passwords beginning with 8 represent aes-cfb 128 encryption.

Note On Cisco IOS XE Catalyst SD-WAN devices, an admin user with privilege 15 is created by default during day-0 bringup of the device. We recommend that users do not delete this admin user.

Supported platforms and templates

Type 6 passwords are supported for these platforms and templates.

Supported platforms:

- Cisco IOS XE Catalyst SD-WAN devices

Supported templates:

- RADIUS and TACACS authentication using the Cisco AAA template
- SNMP template
- CLI add-on template

Restrictions for Type 6 passwords

SNMP templates

In SNMP templates, the community name is encrypted by default. To upgrade your SNMP templates to use type 6 passwords, delete and re-create the community and trap target.

Password length

When you use type 6 passwords with the keychain key-string command, you can enter up to 38 characters in clear text.

In CLI templates or CLI configuration groups, any "\" character in a type 6 password string must be escaped as "\\" before deployment. This is necessary because Cisco SD-WAN Manager trims the "\" character, so escaping it with "\\" ensures the device can correctly decrypt the password.

Upgrade existing templates to Type 6 passwords

Use this procedure to upgrade passwords in your existing templates on Cisco SD-WAN Manager to type 6 passwords.

When you upgrade your routers to Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, all supported passwords are automatically upgraded to type 6 passwords.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**.

Note
In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

Step 3 For the template that you want to upgrade to type 6 passwords, click **…**.

Step 4 Click **Edit**.

Step 5 Click **Save**.

To update the passwords, you do not need to make any other changes to the template. When you click **Save**, SD-WAN Manager automatically upgrades the passwords to type 6 passwords.

Type 6 encryption for CLI commands

This section explains how you can encrypt your passwords to Type 6 using a CLI add-on template.

In the CLI add-on template, you can encrypt supported CLIs including passwords, keys, secret text, community name, and other strings. See Commands supported for Type 6 encryption for more information.

Simply select the plaintext password, key, or similar in the CLI and click the **Encrypt Type 6** button and save the configuration.

Methods for verifying Type 6 passwords

You can use one or more of these verification commands to verify that your passwords are upgraded to type 6 passwords.

Verifying using SD-WAN Manager

In Cisco SD-WAN Manager, when you attach a configuration that supports type 6 passwords to your device, the configuration preview displays the encrypted password.

For example:

```
snmp-server community 0 $CRYPT_CLUSTER$ptqX7nQr6QvC8YZuoMGOkw==$6cVCeSpOfoVFe5iqhJqvQQ==
ro
```

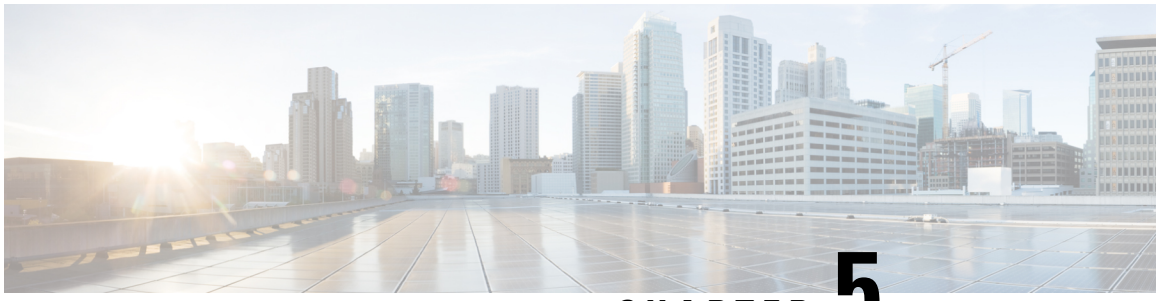
Although the command displays the type as `0`, the `$CRYPT_CLUSTER$ptqX7nQr6QvC8YZuoMGOkw==$6cVCeSpOfoVFe5iqhJqvQQ==` string represents your encrypted password. If your password is encrypted, it will begin with `$CRYPT_CLUSTER$`.

Verifying on a device

You can run the following command on your device to display your encrypted passwords:

```
Device#show run | sec aaa
aaa new-model
aaa group server tacacs+ tacacs-0
server-private 10.0.0.1 key 6 BibgKcVeWF]^aK[XfEIICXMCbdScBYAAB
aaa group server radius radius-0
server-private 10.0.0.2 timeout 5 retransmit 3 key 6 CHd_VK[]NHEdcVCWGCaENGINQHLBEhDBe
```

The output indicates that your password is type 6 and includes your encrypted password.



CHAPTER 5

Role-Based Access Control

This table describes the developments of this feature, by release.

Table 17:

Feature Name	Release Information	Feature Description
Co-Management: Granular Role-Based Access Control	Cisco Catalyst SD-WAN Manager Release 20.13.1	This feature introduces Role-Based Access Control (RBAC) based on sites, scope, or roles. It is a method of authorizing system access for users based on a combination of role and scope of a user. You can create scopes, users, and roles with required read and write permissions for Cisco SD-WAN Manager policies. RBAC prevents unauthorized access and reduces the risk of data breaches and other security incidents.
Canadian French language support on Cisco Catalyst SD-WAN Manager	Cisco Catalyst SD-WAN Manager Release 20.13.1	Added support for using Canadian French for Cisco SD-WAN Manager user interface.
RBAC by scope	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature introduces Role-Based Access Control (RBAC) based on sites or scope. It is a method of authorizing system access for users based on a combination of users and scope. For large Cisco Catalyst SD-WAN deployments across multiple geographical locations, this feature helps you to split the network administration among different regional administrators.

Feature Name	Release Information	Feature Description
RBAC for policies	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature allows you to create users and user groups with required read and write permissions for Cisco SD-WAN Manager policies. RBAC for policies provides users with the access to all the details of policies to help maximize the operational efficiency. It makes it easier to meet configuration requirements and ensures that authorized users on the system are only given access to what they need.
Co-Management: Granular RBAC for feature templates	Cisco vManage Release 20.7.1	This feature introduces greater granularity in assigning RBAC permissions for template use. This enables you to give a tenant self-management of network configuration tasks. Network administrators and managed service providers can use this feature to assign permissions to their end customers.
Co-Management: Improved granular configuration task permissions	Cisco vManage Release 20.9.1	To enable a user to self-manage specific configuration tasks, you can assign the user permissions to perform specific configuration tasks while excluding other tasks. This feature introduces numerous new permission options, enabling fine granularity in determining which configuration task permissions to provide to a user.

Feature Name	Release Information	Feature Description
RBAC for security operations and network operations default user groups	Cisco vManage Release 20.9.1	This feature provides the following default user groups: • network_operations user group for non-security policies • security_operations user group for security policies RBAC for policies allows you to create users and user groups with the required read and write permissions for security and non-security policies. Users can perform configuration and monitoring actions only for the authorized policy type.
Co-Management: Improved granular configuration for scope features	Cisco vManage Release 20.11.1	To enable a user to self-manage specific configuration tasks, you can assign the user permissions to perform specific configuration tasks while excluding other tasks. This feature introduces new permission options for the following configuration groups and feature profiles. • AppQoE under other feature profile • GPS under transport feature profile • Cisco VPN Interface GRE under WAN/LAN profile. • Cisco VPN Interface IPsec under WAN profile. • Cisco Multicast under LAN profile. • UCSE under other feature profile. • IPv4 Tracker and Tracker Group under transport and service feature profiles. • IPv6 DIA Tracker and Tracker Group, under transport feature profile.

Feature Name	Release Information	Feature Description
Assigning roles locally for SSO-authenticated users	Cisco vManage Release 20.11.1	If you are using an identity provider, such as Okta, for security assertion markup language (SAML)-based single sign-on (SSO), then in most use cases, you define user roles through the identity provider. This feature enables you to assign users locally in Cisco SD-WAN Manager, in case no roles are defined for the user by the identity provider.

- Role-Based Access Control, on page 68
- Restrictions for configuring RBAC, on page 70
- RBAC by VPN, on page 70
- RBAC with AAA, on page 71
- User authorization rules for operational and configuration commands, on page 73
- RBAC by scope, on page 80
- Granular RBAC, on page 83
- RBAC for policies, on page 84
- Configure RBAC for CFlowd policy, on page 85
- Assigning roles to users defined by identity providers , on page 86
- Configure RBAC, on page 87
- Prerequisites for **Application Catalog** features, on page 89
- Manage user group permissions, on page 90
- Configure Users, on page 111
- Configure user sessions, on page 115
- Configure VPN segments, on page 115
- Configure VPN groups, on page 116
- Verify granular RBAC permissions, on page 116
- Monitor devices for VPN groups, on page 116

Role-Based Access Control

Role-Based Access Control (RBAC) is a method of restricting or authorizing system access for users based on user roles and scope.

A role is a set of permissions the user receives that

- defines the privileges a user has in the system
- specifies the allowed actions (read, write, or deny) for different APIs or functionalities, and
- determines access based on the organizations or domains (locales) assigned to the user.

Scope defines the set of objects (sites, devices or templates) a user can act on.

Users

A user is an entity that performs different actions in Cisco SD-WAN Manager and belongs to a role.

Users are not directly assigned privileges. To manage individual user privileges, you can assign the appropriate roles and scopes. A user is granted write access to system resources only when both the assigned role provides access privileges and the assigned locale permits access.

Permissions for users

- Users with read or write access can view and make changes to the selected features.
- Users with read access can only view information.
- Users with deny access cannot view information or make changes to Cisco IOS XE Catalyst SD-WAN.

System default roles

You cannot change system default roles. Cisco IOS XE Catalyst SD-WAN software provides these system default roles:

- basic: The basic role is a system default role and is pre-built in Cisco SD-WAN Manager. You cannot modify or delete it. To modify the role, create a copy and modify the copy as a new customer role.
- operator: The operator role is configurable and can be assigned to users at any privilege level. This role is intended for users who have permission to only view information.
- netadmin: The netadmin role is a non-configurable role. By default, this role includes the admin user. You can add other users to this role. Users with this role are permitted to perform all operations on the device.
- network_operations: The network_operations role is a non-configurable role. Users in this role can perform all non-security-policy operations on the device and only view security policy information. For example, users can create or modify template configurations, manage disaster recovery, and create non-security policies such as an application aware routing policy or Cflowd policy. Users with this role are authorized to apply policies to a device, revoke applied policies, and edit device templates.
- security_operations: The security_operations role is a non-configurable role. Users in this role can perform all security operations on the device and only view non-security-policy information. For example, users can manage umbrella keys, licensing, IPS signatures auto-update, TLS/SSL proxy settings, and so on. Users with this role require network_operations users to intervene on day-0 to deploy a security policy on a device and on day-N to remove a deployed security policy. However, after a security policy is deployed on a device, security_operations users can modify the security policy without needing the network_operations users to intervene.



Note Only netadmin users can view the running and local configuration. Users associated with a predefined operator role do not have access to the running and local configurations. The predefined operator role provides read access for the template configuration. To assign a subset of admin privileges, create a new role with the selected features from the features list, grant both read and write access, and associate the role with the custom user.

Privileges for Role-Based Access Control

Role-based access privileges are arranged into five categories, which are called tasks:

- Interface: Privileges for controlling the interfaces on the Cisco IOS XE Catalyst SD-WAN device.
- Policy: Privileges for controlling the control plane policy, OMP, and data plane policy.
- Routing: Privileges for controlling the routing protocols, including BFD, BGP, OMP, and OSPF.
- Security: Privileges for controlling the security of the device, including installing software and certificates. Only users who belong to the netadmin group can install software on the system.
- System: General system-wide privileges.

Restrictions for configuring RBAC

Role and scope per user

From Cisco Catalyst SD-WAN Manager Release 20.13.1, you can only configure one role and one scope per user.

Enabling or disabling Cloud SaaS feeds

To enable or disable Cloud SaaS feeds, a user role requires write permission for the **Application Priority Write** option.

In Cisco Catalyst SD-WAN Manager Release 20.13.x and Cisco Catalyst SD-WAN Manager Release 20.14.x, a user with the security_operations role can enable or disable Cloud SaaS feeds. From Cisco Catalyst SD-WAN Manager Release 20.15.1, the security_operations role does not include write permission for the **Application Priority Write** option, and does not support enabling or disabling Cloud SaaS feeds.

Granular RBAC for feature templates

To use any of the template restriction options that are provided for RBAC for co-management, provide permissions for the **Template Configuration** option. If a specific user role does not have any permissions assigned in the **Template Configuration** option, the **Templates** menu will not be visible to the user in SD-WAN Manager.

To enable an RBAC user to apply templates to devices, provide write permission to the **Template Deploy** option.

RBAC by VPN

RBAC by VPN is a network access control method that enables administrators to

- define VPN groups with one or more network segments
- assign users to specific VPN groups to manage and control their access, and
- restrict user permissions so that access and monitoring are limited to devices and features within designated VPN groups in Cisco SD-WAN Manager.

Restricted access capabilities for users assigned to a VPN group

RBAC by VPN provides these restricted access to users configured with a VPN group:

- Access to the VPN dashboard
- Monitor devices, network, and application status via VPN dashboard
- VPN dashboard information restricted to devices with segments in the VPN group
- Monitor option restricted to devices with segments in the VPN group
- Interface monitoring on each device restricted to interfaces of segments in the VPN group

VPN dashboard

Users configured with VPN group can access only the VPN dashboard in read-only mode. Users with admin access can create the VPN groups and access both the Admin Dashboard and VPN Dashboard(s). An admin user can access these dashboards by choosing **Dashboard** from the Cisco SD-WAN Manager menu.

RBAC with AAA

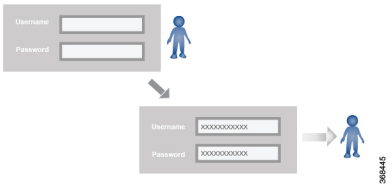
The Cisco Catalyst SD-WAN AAA software implements role-based access to control the authorization permissions for users on Cisco IOS XE Catalyst SD-WAN devices.

RBAC consists of three components:

- Users: They are allowed to log in to a Cisco IOS XE Catalyst SD-WAN device.
- User groups: They are collections of users.
- Privileges: These are associated with each group. Privileges define the commands that the users are authorized to issue.

Users and user groups

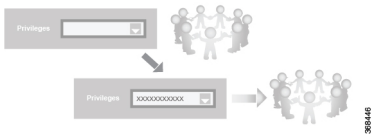
All users who are permitted to perform operations on a Cisco IOS XE Catalyst SD-WAN device device must have a login account. For the login account, you configure a username and a password on the device itself. These allow the user to log in to that device. A username and password must be configured on each device that a user is allowed to access.



The Cisco Catalyst SD-WAN software provides one standard username, admin, which is a user who has full administrative privileges, similar to a UNIX superuser. By default, the admin username password is admin. You cannot delete or modify this username, but you can and should change the default password.

User groups pool together users who have common roles, or privileges, on the Cisco IOS XE Catalyst SD-WAN device. As part of configuring the login account information, you specify which user group or groups that

user is a member of. You do not need to specify a group for the admin user, because this user is automatically in the user group netadmin and is permitted to perform all operations on the SD-WAN device.



The user group itself is where you configure the privileges associated with that group. These privileges correspond to the specific commands that the user is permitted to execute, effectively defining the role-based access to the Cisco Catalyst SD-WAN software elements.



Standard user groups

Cisco Catalyst SD-WAN software provides standard user groups and allows creation of custom user groups as needed.

- **basic**: The basic group is a configurable group and can be used for any users and privilege levels. This group is designed to include users who have permission to both view and modify information on the device.
- **operator**: The operator group is also a configurable group and can be used for any users and privilege levels. This group is designed to include users who have permission only to view information.
- **netadmin**: The netadmin group is a non-configurable group. By default, this group includes the admin user. You can add other users to this group. Users in this group are permitted to perform all operations on the device.
- **network_operations**: From Cisco vManage Release 20.9.1, network_operations user group is supported. The network_operations group is a non-configurable group. Users in this group can perform all non-security-policy operations on the device and only view security policy information. For example, users can create or modify template configurations, manage disaster recovery, and create non-security policies such as application aware routing policy or CFlowD policy.
- **security_operations**: From Cisco vManage Release 20.9.1, security_operations user group is supported. The **security_operations** group is a non-configurable group. Users in this group can perform all security operations on the device and only view non-security-policy information. For example, users can manage umbrella keys, licensing, IPS signatures auto update, TLS/SSL proxy settings, and so on.

Users of the **network_operations** group are authorized to apply policies to a device, revoke applied policies, and edit device templates. Users of the **security_operations** group require **network_operations** users to intervene on day-0 to deploy security policy on a device and on day-N to remove a deployed security policy. However, after a security policy is deployed on a device, **security_operations** users can modify the security policy without needing the **network_operations** users to intervene.

Note All user groups, regardless of the read or write permissions selected, can view the information displayed on the Cisco SD-WAN Manager Dashboard screen.

Only admin users can view running and local configuration. Users associated with predefined operator user group do not have access to the running and local configurations. The predefined user group operator has only read access for the template configuration. If you need only a subset of admin user privileges, then you need to create a new user group with the selected features from the features list with both read and write access and associate the group with the custom user.

Note Previously, users with roles other than netadmin, such as basic, network_operations, security_operations, and operator, could execute arbitrary commands on the host system, which posed a significant security risk. To resolve this issue, only specific users (root, vmanage-admin, ciscotacro, ciscotacrw) were given permission to execute the commands. Now, only ciscotacro and ciscotacrw users have access to the **request execute** function, while netadmin group members are permitted access only when Cisco SD-WAN Manager is enabled. This change blocks unauthorized users from alternative shell or command execution methods, enforces proper restrictions, and mitigates the security risk.

User authorization rules for operational and configuration commands

The user authorization rules for operational commands are based simply on the username. Any user who is allowed to log in to the Cisco IOS XE Catalyst SD-WAN device can execute most of the operational commands. However, only the admin user can issue commands that affect the fundamental operation of the device, such as installing and upgrading the software and shutting down the device.

Any user can issue the **config** command to enter configuration mode. In configuration mode, users are allowed to issue any general configuration command. Also, users can configure their passwords using the **system aaa user** *self* **password** *password* command and then commit the configuration change. For the actual commands that configure device operation, authorization is defined according to user group membership. See User group authorization rules for configuration commands.

This table lists the AAA authorization rules for general CLI commands. All the commands are operational commands except as noted. Also, some commands available to the "admin" user are available only if that user is in the "netadmin" user group.

CLI Command	Any User	Admin User
clear history	X	X
commit confirm	X	X
complete-on-space	X	X
config	X	X
exit	X	X

CLI Command	Any User	Admin User
file	X	X
help	X	X
[no] history	X	X
idle-timeout	X	X
job	X	X
logout	—	X (users in netadmin group only)
monitor	X	X
nslookup	X	X
paginate	X	X
ping	X (users in netadmin group only)	X (users in netadmin group only)
poweroff	—	X(users in netadmin group only)
prompt1	X	X
prompt2	X	X
quit	X	X
reboot	—	X (users in netadmin group only)
request aaa request admin-tech request firmware request interface-reset request nms request reset request software	—	X (users in netadmin group only)
request execute request download request upload	X	X
request (everything else)	—	X
rollback (configuration mode command)	—	X (users in netadmin group only)
screen-length	X	X
screen-width	X	X
show cli	X	X
show configuration commit list	X	X
show history	X	X

CLI Command	Any User	Admin User
show jobs	X	X
show parser dump	X	X
show running-config	X	X
show users	X	X
system aaa user *self* password *password* (configuration mode command) (Note: A user cannot delete themselves)		
tcpdump	X	X
timestamp	X	X
tools ip-route	X	X
tools netstat	X	X
tools nping	X	X
traceroute	X	X
vshell	X (The availability of vshell command is unavailable to all users that are not in netadmin group in Cisco vManage Release 20.9.5.)	X (The vshell AAA authorized access is limited only to users that are in netadmin group.)

User group authorization rules for operational commands

This table lists the user group authorization rules for operational commands.

Table 18: User group authorization rules for operational commands

Operational Command	Interface	Policy	Routing	Security	System
clear app		X			
clear app-route		X			
clear arp	X				
clear bfd			X		X
clear bgp			X		X
clear bridge	X				

Operational Command	Interface	Policy	Routing	Security	System
clear cellular	X				
clear control				X	
clear crash					X
clear dhcp					X
clear dns					X
clear igmp			X		
clear installed-certificates				X	
clear interface	X				
clear ip			X		
clear notification					X
clear omp			X		
clear orchestrator				X	
clear ospf			X		
clear pim			X		
clear policy		X			
clear pppoe	X				
clear system					X
clear tunnel				X	
clear wlan	X				
clear ztp				X	X
clock					X
debug bgp			X		
debug cellular	X				
debug cflowd		X			
debug chmgr					X
debug config-mgr					X
debug dhcp-client					X

Operational Command	Interface	Policy	Routing	Security	System
debug dhcp-helper					X
debug dhcp-server					X
debug fpm		X			
debug ftm					X
debug igmp			X		
debug netconf					X
debug omp			X		
debug ospf			X		
debug pim			X		
debug resolver			X		
debug snmp					X
debug sysmgr					X
debug transport					X
debug ttm					X
debug vdaemon				X	X
debug vrrp				X	
debug wlan	X				
request certificate				X	
request control-tunnel				X	
request controller				X	
request controller-upload				X	
request csr				X	
request device				X	
request device-upload				X	
request on-vbond-controller				X	

Operational Command	Interface	Policy	Routing	Security	System
request port-hop				X	
request root-cert-chain				X	
request security				X	
request vedge				X	
request vedge-upload				X	
request vsmart-upload				X	
show aaa					X
show app		X			
show app-route		X			
show arp	X				
show bfd			X		X
show bgp			X		
show boot-partition					X
show bridge	X				
show cellular	X				
show certificate				X	
show clock					X
show control				X	X
show crash					X
show debugs—same as debug commands					
show dhcp					X
show external-nat				X	X
show hardware					X
show igmp			X		
show interface	X				
show ip			X		X

Operational Command	Interface	Policy	Routing	Security	System
show ipsec				X	
show licenses					X
show logging					X
show multicast			X		
show nms-server					X
show notification					X
show ntp					X
show omp		X	X		X
show orchestrator				X	
show ospf			X		
show pim			X		
show policer		X			
show policy		X			
show ppp	X				
show pppoe	X				
show reboot					X
show security-info				X	
show software					X
show system					X
show transport					X
show tunnel				X	
show uptime					X
show users					X
show version					X
show vrrp	X				
show wlan	X				
show ztp				X	

User group authorization rules for configuration commands

This table lists the user group authorization rules for configuration commands.

Table 19: User group authorization rules for configuration commands

Configuration Command	Interface	Policy	Routing	Security	System
apply-policy		X			
banner					X
bfd			X		X
bridge	X				
omp		X	X		X
policy		X			
security				X	X
snmp					X
system					X
vpn interface	X				
vpn ip			X		
vpn router			X		
vpn service			X		
vpn (everything else, including creating, deleting, and naming)					X
wlan	X				

RBAC by scope

RBAC by scope

RBAC by scope is a method of restricting or authorizing system access for users based on user groups and scope.

A user group defines the privileges of a user in the system and the scope defines the organizations (domains) to which a user is allowed access.

Assigning user and scope

Users are not directly assigned privileges, but you can manage individual user privileges by assigning the appropriate user and scope.

For large Cisco Catalyst SD-WAN deployments across multiple geographical locations, you can split the network administration among different regional administrators.

Network administrators can be classified as global administrators or regional administrators, based on the user groups and scope assigned to them:

- Global administrators have access to all resources in every scope and have complete read-write privileges for all features.
- Regional administrators also have full read-write privileges for all the features. However, the resources they can access are limited by the scope assigned to them.

Global admin

A global admin is responsible for overseeing the entire network, but is not involved in the operations of the individual devices on a daily basis. User accounts in the global scope have access to all resources.

Any user in a single tenant setup with netadmin privileges who is also part of global scope is considered a global admin. The default admin user on SD-WAN Manager is also a global-admin. The global scope contains all WAN edges and controllers in a single view.

A global admin can:

- assign devices to their corresponding regions
- assign regional admin accounts
- manage controllers
- maintain sharable and centralized configurations
- operate on the individual devices when necessary
- switch to view only a specific scope and can create templates
- assign more global admins

Local scope admins, also called regional admins can clone global templates and reuse them within their scope.

Regional admin

A regional admin is responsible for day-to-day operations (configuration, monitoring, onboarding, and so on) for devices in the corresponding regions. Regional admins do not have access to or visibility into devices outside of their region. A regional admin can create these user groups:

- Scope admin – full read/write access to devices in the corresponding scope, can troubleshoot, monitor, attach, or detach templates for the WAN edges in their group
- Scope operator – read-only access to WAN edges within their scope
- Scope basic – basic access within their scope

Scope admins can create new templates and attach or detach them from WAN edges in their group. They can also copy and reuse global templates.

The scope determines the resources accessible to a user; however, the level of access is controlled by the existing user group.

- If a user is in scope scope_a and user group scope_admin, they have full read/write access to all resources in scope_a.
- If a user is in scope scope_a and user group scope_operator, they have read-only access to all resources in rscope_a.
- If a user is in scope scope_a and user group scope_basic, they have read-only access to interface and system resources in scope_a.

Global scope

The global group is a special, system-predefined scope with these different access control rules:

- Users within this group are considered as global-admins, who can have full access to all resources (devices, templates and policies) in the system and they can manage the scope and assign resources and users to groups.
- All other users have read-only access to resources within this group.
- The system default admin account (or tenantadmin account in a multitenant setup) is always in this group. This privilege cannot be changed. However, the admin account may add/remove other user accounts to or from this group.

IdP (SSO)-managed group

An identity provider (IdP) is a service that stores and verifies user identity. IdPs typically work with single sign-on (SSO) providers to authenticate users. If a user is authenticated with a SSO service of an IdP, the group information is also provided and managed by the IdP. An IdP passes the information about the user, including the user name and all the group names, where the user belongs to. SD-WAN Manager matches the group names with the group names stored in the database to further distinguish if a particular group name passed from IdP is for user group or scope or VPN group.

Multitenancy support

With Cisco Catalyst SD-WAN multitenancy, a service provider can manage multiple customers, called tenants, from Cisco SD-WAN Manager. The tenants share Cisco SD-WAN Manager instances, Cisco SD-WAN Validator, and Cisco SD-WAN Controller. The domain name of the service provider has subdomains for each tenant. Cisco SD-WAN Manager is deployed and configured by the service provider. The provider enables multitenancy and creates a Cisco SD-WAN Manager cluster to serve tenants. Only the provider can access a Cisco SD-WAN Manager instance through the SSH terminal.

Provider has these features:

- Scope is not applicable as the provider manages only the controllers.
- When provider provisions a new tenant, the default user account for the tenant is tenantadmin.
- Other user accounts created by the provider are included in the default global scope.
- When a provider creates a template for a tenant, the template is included in the globalscope.

Granular RBAC

Granular RBAC for templates

When setting user group permissions, use the template permissions defined in this section. This approach allows you to provide an RBAC user with specific access to various types of templates and control which device configurations they can apply.

From Cisco vManage Release 20.7.1, you can use these template permissions:

Permission	Description
CLI Add-On Template	Provides access to the CLI add-on feature template.
Device CLI Template	Provides access to the device CLI template.
SIG Template	Provides access to the SIG feature template and SIG credential template.
Other Feature Templates	Provides access to all feature templates except the SIG feature template, SIG credential template, and CLI add-on feature template.
Feature Profile	Provides access to all feature profiles.
Config Group	Provides access to all configuration groups.

Expand each feature profile to specify granular RBAC. After you set the permissions for the user group, verify that you can access the required feature profiles under **Templates** > **Configuration Groups**.

Single-tenant and multi-tenant scenarios

You can use granular RBAC for feature templates in single-tenant and multi-tenant Cisco SD-WAN Manager scenarios.

You can create user groups to assign specific permissions to a tenant's various teams, enabling teams to manage only specific network services without granting permission to use device CLI templates.

Avoid granting tenants the permission to apply device CLI templates because they can override any other template or device configuration. For example, create a user group for a tenant's security operations group. Grant them read/write access only to the SIG Template option to enable them to manage security configurations.

Benefits of granular RBAC

From Cisco vManage Release 20.7.1, the permissions configured for co-management in Cisco Catalyst SD-WAN allow for very detailed and specific control over who can access and modify network configurations. They are useful when using Cisco Catalyst SD-WAN with tenants, enabling you to provide a tenant access to specific types of templates. This setup lets tenants manage their own network configuration tasks within their own VPN.

RBAC for policies

RBAC for policies

RBAC for policies allows a user or user group to have selective read and write (RW) access to Cisco SD-WAN Manager policies.

From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1, a user can perform these actions with read and write access:

- For Cflowd policy: Configure Cflowd policy, but cannot configure application-aware routing policy.
- For application aware routing (AAR) policy: Configure application-aware routing policy, but cannot configure other policies.

Note This feature is only supported for centralized and localized policies, but not supported for security policies.

Configure RBAC for policies

From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1, you can configure required access for policies.

Procedure

Step 1 Create user groups with required read or write access to selected control or data policies.

For information about managing user group permissions, refer to Manage user group permissions, on page 90.

Step 2 Create users and assign them to required user groups. .

Refer to Add user, on page 111.

Step 3 Create or modify or view policy configurations as required.

For information about configuring policies, see Configure Centralized Policies Using Cisco SD-WAN Manager.

Modify policy configurations

FromCisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1, you can modify or update policy configurations as per your requirement.

Simply log in to Cisco SD-WAN Manager to view the user group components that are assigned to you and you can modify the policy configurations. For more details on configuring policies, see Cisco Catalyst SD-WAN Policies Configuration Guide

Configure RBAC for CFlowd policy

Create a CFlowd user group

From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1, you can create a CFlowd user group and assign users to modify a CFlowd data policy.

Procedure

Step 1 From Cisco SD-WAN Manager, choose **Administration** > **Manage Users**.

Step 2 Click **User Groups** and **Add User Group**.

Step 3 Enter **User Group Name**.

For example, cflowd-policy-only.

Step 4 Check the Read or Write check box against the CFlowD Policy feature that you want to assign to a user group.

Step 5 Click **Add**.

You can view the new user group in the left navigation path.

Step 6 Click **Edit** to edit the existing read or write rules.

Step 7 Click **Save**.

Create a CFlowd policy user

To modify a CFlowd policy, create a CFlowd policy user and assign it to the Cflowd policy user group.

Procedure

Step 1 From Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**.

Step 2 Click **Users**.

Step 3 Click **Add User**.

Step 4 In the Add New User page, enter **Full Name**, **Username**, **Password**, and **Confirm Password** details.

Step 5 Choose **cflowd-policy-only** from the **User Groups** drop-down list.

Allow the **Scope** to select the default scope.

Step 6 Click **Add**.

You can view the new user in the **Users** window.

Step 7 To edit the existing read or write rules for a user, click **Edit**.

Modify a CFlowd policy

You can modify CFlowd policies associated with the related CFlowd user group.

Procedure

Step 1 Log in to Cisco SD-WAN Manager with the CFlowd user credentials.

You can access only CFlowd policies as your login is associated to cflowd-policy-only user group.

Step 2 You can create, modify, or update the configurations based on your requirement.

Assigning roles to users defined by identity providers

From Cisco vManage Release 20.11.1 you can manage user roles and permissions through the identity provider (IdP) when users authenticate via Okta to log into Cisco SD-WAN Manager.

When a user logs in, SD-WAN Manager retrieves the user's role(s) from the IdP and maps them to user group permissions in SD-WAN Manager. The permissions granted to the user correspond to these mapped user groups.

If a user does not have a role defined in the IdP, a network administrator—who has access to SD-WAN Manager but does not have access to the IdP—can assign the user to a specific local user group within SD-WAN Manager to provide the necessary permissions.

However, if both a role is defined for a user in the IdP and a user group is assigned locally in SD-WAN Manager, the role defined in the IdP will take precedence over the local assignment.

This table summarizes the methods available for assigning specific permissions to a user:

IdP for SAML SSO	Roles defined in the IdP	How user permissions are defined
Not using an IdP	Not applicable	In SD-WAN Manager, assign a user to one or more user groups locally. This provides the user with the corresponding user group permissions.

IdP for SAML SSO	Roles defined in the IdP	How user permissions are defined
Using an IdP	IdP has one or more roles defined for the user.	Define roles for the user through the IdP. SD-WAN Manager provides the user with the user group permissions corresponding to the roles.
	IdP does not have a role defined for the user.	Use the **Remote User** option for adding a user (**Administration** > **Manage Users** > **Add User**). See Add a User. In SD-WAN Manager, assign a user to one or more user groups locally. This provides the user with the corresponding user group permissions.

Configure RBAC

Configure scope

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Users and Access**.

By default **Scope** menu is selected. The table displays the list of scopes configured in the device.

Step 2 Click **Add Scope**.

Step 3 Enter **Scope Name** and **Description**.

Step 4 Click **Add Nodes**.

Step 5 Choose the required nodes and click **Save**.

You can click **Edit Nodes** to update the existing nodes in the list.

Step 6 (Optional) In the **Associations** pane, click **Add Users** to associate users.

a) In the **Add Users** pop-up window, choose the users that you want to add.

b) Click **Save**.

The selected users are associated to a scope.

Step 7 (Optional) In the **Configurations** tab, click **Add Configurations** to add configurations. Choose the available configurations from the following tabs:

a) **Configuration Group**

b) **Device Template**

c) **Feature Template**

d) **Feature Profile**
e) **Security Policy**
f) **Localized Policy**

Step 8 Click **Save**.

A new scope with nodes, users and required configurations is created.

Configure roles

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Users and Access**.

Step 2 Click **Roles**.

The table displays the list of roles configured in the device.

Step 3 Click **Add Role**.

Step 4 Enter **Custom Role Name** in the **Add Custom Role** page.

Step 5 Select the **Deny**, **Read**, or **Write** check box against the feature or sub feature that you want to assign a role.

Step 6 Click **Add**.

You can view the new role in the table in the **Roles** page.

Copy custom role

To create a copy of a custom role, use these steps.

Procedure

Step 1 In the list of roles, for the role you wish to copy, click **...**, and click **Copy**.

The **Copy Custom Role** page is displayed.

Step 2 Enter **Custom Role Name**.

Step 3 Select the **Deny**, **Read**, or **Write** check box against the feature or sub feature that you want to update for a role.

Step 4 Click **Copy**.

You can view the new role in the table in the **Roles** page.

Edit custom role

Procedure

Step 1 In the list of roles, for the role you wish to copy, click **...**, and click **Edit**.

The **Edit Custom Role** page is displayed.

Step 2 Select the **Deny**, **Read**, or **Write** check box against the feature or sub feature that you want to update for a role.

Note
Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, the permissions for a role and its descendents may differ in the Deny/Read/Write table. Therefore, do not assume the parent role as the entire role for the sub-tree under it.

If you have a role with write permissions for Configuration Groups but deny or read permission for deploy, a **Change device variables** button appears instead of **Deploy** button. This button allows you to modify device-specific values during the deploy process, without initiating the deployment.

Step 3 Click **Update**.

You can view the updated role in the table in the **Roles** page.

Delete a role

You can delete a role when it is no longer needed. For example, you might delete a role that you created for a specific project when that project ends.

Procedure

Step 1 Choose the role you wish to delete, click **...**, and click **delete**.

The **Warning** page is displayed.

Step 2 To confirm the deletion of the role, click **Delete**.

This deletes the role.

Prerequisites for Application Catalog features

You can grant certain permissions to a custom role for viewing and creating applications through the **Discovered Applications** page. **Discovered Applications** appear on the **Configuration** > **Application Catalog** > **Discovered Applications** page.

To enable a custom role to view discovered applications, grant these permissions:

- read permission for **Cloud OnRamp**

- read permission for
  - **Policy Configuration**
  - **Policy Group**
  - **Security Policy Configuration**
  - **Feature Profile** > **Embedded Security**, or
  - **Feature Profile** > **Embedded Security** > **NgFirewall**

To enable a custom role to create custom applications from **Discovered Applications**, grant write permissions for these:

- **Policy Configuration**
- **Policy Group**
- **Security Policy Configuration**
- **Feature Profile** > **Embedded Security**, or
- **Feature Profile** > **Embedded Security** > **NgFirewall**

Manage user group permissions

User group permissions for Cisco IOS XE Catalyst SD-WAN devices

Table 20: User Group Permissions: Cisco IOS XE Catalyst SD-WAN devices

Feature	Read Permission	Write Permission
Alarms	Set alarm filters and view the alarms generated on the devices on the **Monitor** > **Logs** > **Alarms** page. Cisco vManage Release 20.6.x and earlier: Set alarm filters and view the alarms generated on the devices on the **Monitor** > **Alarms** page.	No additional permissions.

Feature	Read Permission	Write Permission
Audit Log	Set audit log filters and view a log of all the activities on the devices on the **Monitor** > **Logs** > **Alarms** page and the **Monitor** > **Logs** > **Audit Log** page. Cisco vManage Release 20.6.x and earlier: Set audit log filters and view a log of all the activities on the devices on the **Monitor** > **Alarms** page and the **Monitor** > **Audit Log** page.	No additional permissions.
Certificates	View a list of the devices in the overlay network under **Configuration** > **Certificates** > **WAN Edge List**. View a certificate signing request (CSR) and certificate on the **Configuration** > **Certificates** > **Controllers** window. **Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.	Validate and invalidate a device, stage a device, and send the serial number of valid controller devices to the Cisco Catalyst SD-WAN Validator on the **Configuration** > **Certificates** > **WAN Edge List** window. Generate a CSR, install a signed certificate, reset the RSA key pair, and invalidate a controller device on the **Configuration** > **Certificates** > **Controllers** window. **Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.
CLI Add-On Template (Minimum supported release: Cisco vManage Release 20.7.1)	View the CLI add-on feature template on the **Configuration** > **Templates** window. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, delete, and copy a CLI add-on feature template on the **Configuration** > **Templates** window. **Note** These operations require write permission for **Template Configuration**.

Feature	Read Permission	Write Permission
Cloud OnRamp	View the cloud applications on the**Configuration** > **Cloud OnRamp for SaaS** and **Configuration** > **Cloud OnRamp for IaaS** window.	No additional permissions.
Cluster	View information about the services running on SD-WAN Manager, a list of devices connected to a SD-WAN Manager server, and the services that are available and running on all the SD-WAN Manager servers in the cluster on the **Administration** > **Cluster Management** window.	Change the IP address of the current SD-WAN Manager, add a SD-WAN Manager server to the cluster, configure the statistics database, edit, and remove a SD-WAN Manager server from the cluster on the **Administration** > **Cluster Management** window.
Colocation	View the cloud applications on the **Configuration** > **Cloud OnRamp for Colocation** window.	No additional permissions.
Config Group > **Device** > **Deploy** (Minimum supported release: Cisco vManage Release 20.9.1)	This permission does not provide any functionality.	Deploy a configuration onto Cisco IOS XE Catalyst SD-WAN devices. **Note** To edit an existing feature configuration requires write permission for **Template Configuration**. For more details on deploying devices, see Deploy Devices.
Device CLI Template (Minimum supported release: Cisco vManage Release 20.7.1)	View the device CLI template on the **Configuration** > **Templates** window. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, delete, and copy a device CLI template on the **Configuration** > **Templates** window. **Note** These operations require write permission for **Template Configuration**.

Feature	Read Permission	Write Permission
Device Inventory	View the running and local configuration of devices, a log of template activities, and the status of attaching configuration templates to devices on the **Configuration** > **Devices** > **WAN Edge List** window. View the running and local configuration of the devices and the status of attaching configuration templates to controller devices on the **Configuration** > **Devices** > **Controllers** window. **Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.	Upload a device's authorized serial number file to SD-WAN Manager, toggle a device from SD-WAN Manager configuration mode to CLI mode, copy a device configuration, and delete the device from the network on the **Configuration** > **Devices** > **WAN Edge List** window. Add and delete controller devices from the overlay network, and edit the IP address and login credentials of a controller device on the **Configuration** > **Devices** > **Controllers** window. **Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

Feature	Read Permission	Write Permission
Device Monitoring	View the geographic location of the devices on the **Monitor** > **Geography** window. View events that have occurred on the devices on the **Monitor** > **Logs** > **Events** page. Cisco vManage Release 20.6.x and earlier: View events that have occurred on the devices on the **Monitor** > **Events** page. View a list of devices in the network, along with device status summary, SD-WAN Application Intelligence Engine (SAIE) and Cflowd flow information, transport location (TLOC) loss, latency, and jitter information, control and tunnel connections, system status, and events on the **Monitor** > **Devices** page (only when a device is selected). **Note** In Cisco vManage Release 20.7.x and earlier releases, the SAIE flow is called the deep packet inspection (DPI) flow. Cisco vManage Release 20.6.x and earlier: Device information is available in the **Monitor** > **Network** page.	Ping a device, run a traceroute, and analyze the traffic path for an IP packet on the **Monitor** > **Devices** page (only when a device is selected). **Note** These operations require read and write permissions for **Device Monitoring**.
Device Reboot	View the list of devices on which the reboot operation can be performed on the **Maintenance** > **Device Reboot** window.	Reboot one or more devices on the **Maintenance** > **Device Reboot** window.
Disaster Recovery	View information about active and standby clusters running on SD-WAN Manager on the **Administration** > **Disaster Recovery** window.	No additional permissions.

Feature	Read Permission	Write Permission
Events	View the geographic location of the devices on the **Monitor** > **Logs** > **Events** page. View the geographic location of the devices on the **Monitor** > **Events** page.	Ping a device, run a traceroute, and analyze the traffic path for an IP packet on the **Monitor** > **Logs** > **Events** page (only when a device is selected).
Feature Profile > **Other** > **Thousandeyes** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **ThousandEyes** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Other Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **ThousandEyes** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Other Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Service** > **Dhcp** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **DHCP** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **DHCP** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Service** > **Lan/Vpn** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **LAN/VPN** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **LAN/VPN** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Service** > **Lan/Vpn/Interface/Ethernet** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Ethernet Interface** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Ethernet Interface** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section. **Note** These operations require write permission for **Template Configuration**.

Feature	Read Permission	Write Permission
Feature Profile > **Service** > **Lan/Vpn/Interface/Svi** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **SVI Interface** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **SVI Interface** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Service** > **Routing/Bgp** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Routing/BGP** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Routing/BGP** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Service** > **Routing/Ospf** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Routing/OSPF** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Routing/OSPF** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Service** > **Switchport** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Switchport** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Switchport** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section. **Note** These operations require write permission for **Template Configuration**.

Feature	Read Permission	Write Permission
Feature Profile > **Service** > **Wirelesslan** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Wireless LAN** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Wireless LAN** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **System** > **Interface/Ethernet** > **Aaa** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **AAA** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **AAA** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **System** > **Interface/Ethernet** > **Banner** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Banner** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Banner** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **System** > **Basic** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Basic** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Basic** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section. **Note** These operations require write permission for **Template Configuration**.

Feature	Read Permission	Write Permission
Feature Profile > **System** > **Bfd** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **BFD** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **BFD** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **System** > **Global** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Global** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Global** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **System** > **Logging** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Logging** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Logging** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **System** > **Ntp** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **NTP** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **NTP** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section. **Note** These operations require write permission for **Template Configuration**.

Feature	Read Permission	Write Permission
Feature Profile > **System** > **Omp** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **OMP** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **OMP** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **System** > **Snmp** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **SNMP** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **SNMP** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Transport** > **Cellular Controller** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Cellular Controller** settings on the **Configuration** > **Templates** > **(View a configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Cellular Controller** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Transport** > **Cellular Profile** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Cellular Profile** settings on the **Configuration** > **Templates** > **(View a configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Cellular Profile** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.

Feature	Read Permission	Write Permission
Feature Profile > **Transport** > **Management/Vpn** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Management VPN** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Management VPN** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Transport** > **Management/Vpn/Interface/Ethernet** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Management Ethernet Interface** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Management VPN and Management Internet Interface** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Transport** > **Routing/Bgp** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **BGP Routing** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **BGP Routing** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Transport** > **Tracker** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Tracker** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Tracker** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.

Feature	Read Permission	Write Permission
Feature Profile > **Transport** > **Wan/Vpn** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Wan/Vpn** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Wan/Vpn** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Transport** > **Wan/Vpn/Interface/Cellular** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Wan/Vpn/Interface/Cellular** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Wan/Vpn/Interface/Cellular** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Transport** > **Wan/Vpn/Interface/Ethernet** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Wan/Vpn/Interface/Ethernet** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Wan/Vpn/Interface/Ethernet** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.
Integration Management	View information about controllers running on SD-WAN Manager, on the **Administration** > **Integration Management** window.	No additional permissions.
License Management	View license information of devices running on SD-WAN Manager, on the **Administration** > **License Management** window.	On the **Administration** > **License Management** page, configure use of a Cisco Smart Account, choose licenses to manage, and synchronize license information between SD-WAN Manager and the license server.

Feature	Read Permission	Write Permission
Interface	View information about the interfaces on a device on the **Monitor** > **Devices** > **Interface** page. Cisco vManage Release 20.6.x and earlier: View information about the interfaces on a device on the **Monitor** > **Network** > **Interface** page	Edit **Chart Options** to select the type of data to display, and edit the time period for which to display data on the **Monitor** > **Devices** > **Interface** page.
Application Monitoring (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.12.1)	View the application health of the devices on the **Monitor** > **Applications** window.	View the application health of the devices on the **Monitor** > **Applications** window.
Manage Users	View users and user groups on the **Administration** > **Manage Users** window.	Add, edit, and delete users and user groups from SD-WAN Manager, and edit user group privileges on the **Administration** > **Manage Users** window.
Other Feature Templates (Minimum supported release: Cisco vManage Release 20.7.1)	View all feature templates except the SIG feature template, SIG credential template, and CLI add-on feature template on the **Configuration** > **Templates** window. **Note** This operation requires read permission for **Template Configuration**. **Note** To check the mutual authentication option, you need read permission for certificates. (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.12.1)	Create, edit, delete, and copy all feature templates except the SIG feature template, SIG credential template, and CLI add-on feature template on the **Configuration** > **Templates** window. **Note** These operations require write permission for **Template Configuration**. **Note** To check the mutual authentication option, you need write permission for certificates. (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.12.1)
Policy	View the common policies for all Cisco Catalyst SD-WAN Controllers or devices in the network on the **Configuration** > **Policies** window.	Create, edit, and delete the common policies for all Cisco Catalyst SD-WAN Controllers or devices in the network on the **Configuration** > **Policies** window.

Feature	Read Permission	Write Permission
Policy Configuration	View the list of policies created and details about them on the **Configuration** > **Policies** window.	Create, edit, and delete the common policies for all the Cisco Catalyst SD-WAN Controllers and devices in the network on the **Configuration** > **Policies** window.
Policy Deploy	View the current status of the Cisco Catalyst SD-WAN Controllers to which a policy is being applied on the **Configuration** > **Policies** window.	Activate and deactivate the common policies for all SD-WAN Manager servers in the network on the **Configuration** > **Policies** window.
RBAC VPN	View the VPN groups and segments based on roles on the **Monitor** > **VPN** page. Cisco vManage Release 20.6.x and earlier: View the VPN groups and segments based on roles on the **Dashboard** > **VPN Dashboard** page.	Add, edit, and delete VPNs and VPN groups from SD-WAN Manager, and edit VPN group privileges on the **Administration** > **VPN Groups** window.
Routing	View real-time routing information for a device on the **Monitor** > **Devices** > **Real-Time** page. Cisco vManage Release 20.6.x and earlier: View real-time routing information for a device on the **Monitor** > **Network** > **Real-Time** page.	Add command filters to speed up the display of information on the **Monitor** > **Devices** > **Real-Time** page.
Security	View the current status of the Cisco Catalyst SD-WAN Controllers to which a security policy is being applied on the **Configuration** > **Security** window.	Activate and deactivate the security policies for all SD-WAN Manager servers in the network on the **Configuration** > **Security** window.
Security Policy Configuration	Activate and deactivate the common policies for all SD-WAN Manager servers in the network on the **Configuration** > **Security** > **Add Security Policy** window.	Activate and deactivate the security policies for all SD-WAN Manager servers in the network on the **Configuration** > **Security** > **Add Security Policy** window.
Session Management	View user sessions on the **Administration** > **Manage Users** > **User Sessions** window.	Add, edit, and delete users and user groups from SD-WAN Manager, and edit user sessions on the **Administration** > **Manage Users** > **User Sessions** window.

Feature	Read Permission	Write Permission
Settings	View the organization name, Cisco Catalyst SD-WAN Validator DNS or IP address, certificate authorization settings, software version enforced on a device, custom banner on the SD-WAN Manager login page, and the current settings for collecting statistics on the **Administration** > **Settings** window.	Edit the organization name, Cisco Catalyst SD-WAN Validator DNS or IP address, certificate authorization settings, software version enforced on a device, custom banner on the SD-WAN Manager login page, current settings for collecting statistics, generate a certificate signing request (CSR) for a web server certificate, and install a certificate on the **Administration** > **Settings** window.
SIG Template (Minimum supported release: Cisco vManage Release 20.7.1)	View the SIG feature template and SIG credential template on the **Configuration** > **Templates** window. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, delete, and copy a SIG feature template and SIG credential template on the **Configuration** > **Templates** window. **Note** These operations require write permission for **Template Configuration**.
SIG Tunnels (Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.12.x	View information about the SIG tunnels on the **Monitor** > **Tunnels** > **SIG Tunnels** page.	View information about the SIG tunnels on the **Monitor** > **Tunnels** > **SIG Tunnels** page.
Software Upgrade	View a list of devices, the custom banner on SD-WAN Manager on which a software upgrade can be performed, and the current software version running on a device on the **Maintenance** > **Software Upgrade** window.	Upload new software images on devices, upgrade, activate, and delete a software image on a device, and set a software image to be the default image on devices on the **Maintenance** > **Software Upgrade** window.
System	View system-wide parameters configured using SD-WAN Manager templates on the **Configuration** > **Templates** > **Device Templates** window. **Note** In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.	Configure system-wide parameters using SD-WAN Manager templates on the **Configuration** > **Templates** > **Device Templates** window. **Note** In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.

Feature	Read Permission	Write Permission
Template Configuration	View feature and device templates on the **Configuration** > **Templates** window.	Create, edit, delete, and copy a feature or device template on the **Configuration** > **Templates** window. **Note** From Cisco vManage Release 20.7.1, to create, edit, or delete a template that is already attached to a device, the user requires write permission for the Template Deploy option.
Template Deploy	View the devices attached to a device template on the **Configuration** > **Templates** window.	Attach a device to a device template on the **Configuration** > **Templates** window.
Tools	Use the **admin tech** command to collect the system status information for a device on the **Tools** > **Operational Commands** window.	Use the **admin tech** command to collect the system status information for a device, and use the **interface reset** command to shut down and then restart an interface on a device in a single operation on the **Tools** > **Operational Commands** window. Rediscover the network to locate new devices and synchronize them with SD-WAN Manager on the **Tools** > **Operational Commands** window. Establish an SSH session to the devices and issue CLI commands on the **Tools** > **Operational Commands** window.
vAnalytics	Launch Cisco SD-WAN Analytics from > **vAnalytics** window.	No additional permissions.
Workflows	Launch workflow library from > **Workflows** window.	No additional permissions.

Feature	Read Permission	Write Permission
Config Group > **Device** > **Deploy** (Minimum supported release: Cisco vManage Release 20.11.1)	View the devices associated to a configuration group on the **Configuration** > **Templates** > **Edit Configuration Group** > **Associated Devices** window.	Deploy a configuration onto Cisco IOS XE Catalyst SD-WAN devices. **Note** To edit an existing feature configuration requires write permission for **Template Configuration**. For more details on deploying devices, see Deploy Devices.
Feature Profile > **Transport** > **IPv4 Tracker and Tracker Group** (Minimum supported release: Cisco vManage Release 20.11.1)	View the IPv4 Tracker and Tracker Group settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **IPv4 Tracker and Tracker Group** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Transport** > **IPv6 Tracker and Tracker Group** (Minimum supported release: Cisco vManage Release 20.11.1)	View the IPv6 Tracker and Tracker Group settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **IPv6 Tracker and Tracker Group** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Transport** > **Gps** (Minimum supported release: Cisco vManage Release 20.11.1)	View the GPS settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Gps** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.

Feature	Read Permission	Write Permission
Feature Profile > **Other** > **APPQoE** (Minimum supported release: Cisco vManage Release 20.11.1)	View the APPQoE settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Other** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **APPQoE** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Other** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Other** > **UCSE** (Minimum supported release: Cisco vManage Release 20.11.1)	View the UCSE settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Other** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **UCSE** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Other** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Wan Profile** > **Cisco VPN Interface IPSec** (Minimum supported release: Cisco vManage Release 20.11.1)	View the Cisco VPN Interface IPSec settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Wan Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Cisco VPN Interface IPSec** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Wan Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Wan/Lan Profile** > **Cisco VPN Interface GRE** (Minimum supported release: Cisco vManage Release 20.11.1)	View the Cisco VPN Interface GRE settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Wan/Lan Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Cisco VPN Interface GRE** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Wan/Lan Profile** section. **Note** These operations require write permission for **Template Configuration**.

Feature	Read Permission	Write Permission
Feature Profile > **Lan Profile** > **Cisco Multicast** (Minimum supported release: Cisco vManage Release 20.11.1)	View the Cisco Multicast settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Lan Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Cisco Multicast** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Lan Profile** section. **Note** These operations require write permission for **Template Configuration**.

To create Service, System, and Transport feature profiles using configuration groups, provide read and write permissions for each of these features to access each configuration group.

Permission type	Features
Read and write permissions	**Feature Profile** > **System**
	Feature Profile > **System** > **AAA**
	Feature Profile > **System** > **BFD**
	Feature Profile > **System** > **Banner**
	Feature Profile > **System** > **Basic**
	Feature Profile > **System** > **Logging**
	Feature Profile > **System** > **NTP**
	Feature Profile > **System** > **OMP**
	Feature Profile > **System** > **SNMP**
	Feature Profile > **Service**
	Feature Profile > **Service** > **BFD**
	Feature Profile > **Service** > **LAN/VPN**
	Feature Profile > **Service** > **LAN/VPN/Interface/Ethernet**
	Feature Profile > **Service** > **Routing/BGP**
	Feature Profile > **Service** > **Routing/OSPF**
	Feature Profile > **Service** > **Routing/DHCP**
	Feature Profile > **Service** > **Routing/Multicast**
	Feature Profile > **Transport**
	Feature Profile > **Transport** > **Routing/BGP**
	Feature Profile > **Transport** > **WAN/VPN**
	Feature Profile > **Transport** > **WAN/VPN/Interface/Ethernet**

Note For more details on configuring features using Configuration Groups, see Feature Management.

User group permissions for Cisco Catalyst Wireless Gateway devices

This table lists the user group read or write permissions for Cisco Catalyst Wireless Gateway devices.

Table 21: User group permissions: Cisco Catalyst Wireless Gateway devices

Feature	Read Permission	Write Permission
Feature Profile > **Teleworker** > **Basic** (Minimum supported release: Cisco vManage Release 20.9.1)	View the basic settings on the **Configuration** > **Templates** > **(View mobility configuration group)** page, in the **Global Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Configure tthe basic settings on the **Configuration** > **Templates** > **(Add or edit mobility configuration group)** page, in the **Global Profile** section. **Note** This operation requires write permission for **Template Configuration**.
Feature Profile > **Teleworker** > **Cellular** (Minimum supported release: Cisco vManage Release 20.9.1)	View the cellular network settings on the **Configuration** > **Templates** > **(View mobility configuration group)** page, in the **Global Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Configure the cellular network settings on the **Configuration** > **Templates** > **(Add or edit mobility configuration group)** page, in the **Global Profile** section. **Note** This operation requires write permission for **Template Configuration**.
Feature Profile > **Teleworker** > **Ethernet** (Minimum supported release: Cisco vManage Release 20.9.1)	View the ethernet settings on the **Configuration** > **Templates** > **(View mobility configuration group)** page, in the **Global Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Configure the ethernet settings on the **Configuration** > **Templates** > **(Add or edit mobility configuration group)** page, in the **Global Profile** section. **Note** This operation requires write permission for **Template Configuration**.
Feature Profile > **Teleworker** > **NetworkProtocol** (Minimum supported release: Cisco vManage Release 20.9.1)	View the network protocol settings on the **Configuration** > **Templates** > **(View mobility configuration group)** page, in the **Global Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Configure the network protocol settings on the **Configuration** > **Templates** > **(Add or edit mobility configuration group)** page, in the **Global Profile** section. **Note** This operation requires write permission for **Template Configuration**.

Feature	Read Permission	Write Permission
Feature Profile > **Teleworker** > **SecurityPolicy** (Minimum supported release: Cisco vManage Release 20.9.1)	View the security policy settings on the **Configuration** > **Templates** > **(View mobility configuration group)** page, in the **Global Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Configure the security policy settings on the **Configuration** > **Templates** > **(Add or edit mobility configuration group)** page, in the **Global Profile** section. **Note** This operation requires write permission for **Template Configuration**.
Feature Profile > **Teleworker** > **Vpn** (Minimum supported release: Cisco vManage Release 20.9.1)	View the VPN settings on the **Configuration** > **Templates** > **(View mobility configuration group)** page, in the **Global Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Configure the VPN settings on the **Configuration** > **Templates** > **(Add or edit mobility configuration group)** page, in the **Global Profile** section. **Note** This operation requires write permission for **Template Configuration**.
Feature Profile > **Teleworker** > **Wifi** (Minimum supported release: Cisco vManage Release 20.9.1)	View the Wi-Fi settings on the **Configuration** > **Templates** > **(View mobility configuration group)** page, in the **Global Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Configure the Wi-Fi settings on the **Configuration** > **Templates** > **(Add or edit mobility configuration group)** page, in the **Global Profile** section. **Note** This operation requires write permission for **Template Configuration**.

Configure Users

Add user

Use these steps to add users.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Users and Access**.

Step 2 Click **Users**.

Step 3 Click **Add User**.

Step 4 Configure these fields:

Field	Description
Full Name	Enter the full name of the user.
User Name	Enter the user name.
Password	Enter a password.
Remote User	Enable the **Remote User** option for remote users. If you enable this option, enter an email for the user.
Roles	Choose roles for the user.
Scope	Choose the scope for the user.
Select Locale	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) Choose a locale to set the language for SD-WAN Manager user interface.

Note
In Cisco Catalyst SD-WAN Manager Release 20.12.1 and earlier releases, SD-WAN Manager only supported the English language on the user interface. From Cisco Catalyst SD-WAN Manager Release 20.13.1, SD-WAN Manager user interface supports Canadian French.

Note
From Cisco IOS XE Catalyst SD-WAN Release 17.18.1a and later releases, SD-WAN Manager user interface supports Japanese.

Step 5 Click **Add** to add the user.

What to do next

When creating a new user, you have an option for creating a remote user. You can create from SD-WAN Manager or using an API for external integrations like Security Cloud Control. You can also edit the remote user using SD-WAN Manager like any other user. However, if the user is created programmatically through API for external integrations, the user will have an impact when they login next time.

Edit user

To edit user details after adding users, use these steps.

Procedure

Step 1 In the **Users** page, for the user you wish to edit, click **...**, and click **Edit**.

The **Edit User** page is displayed.

Step 2 Enter **Full Name**, **Username**.

Step 3 Choose the role from the **Roles** drop-down list.

Step 4 Choose the scope from the **Scope** drop-down list.

Step 5 Choose the locale from the **Select Locale** drop-down list.

From Cisco Catalyst SD-WAN Manager Release 20.13.1 this option is available.

Step 6 Click **Update**.

Copy user

Create a copy of the user details with these steps:

Procedure

Step 1 To create a copy of the user, click **...**, and click **Copy**.

The **Copy User** page is displayed.

Step 2 Enter **Full Name**, **Username**.

Step 3 If the user is a remote user, then:

a) Enable the **Remote User** option.

b) Enter the email in the **Email** and **Confirm Email** field.

Step 4 If the user is not a remote user, then:

a) Enter the password in the **Password** and **Confirm Password**fields.

Step 5 Choose the role from the **Roles** drop-down list.

Step 6 Choose the scope from the **Scope** drop-down list.

Step 7 Choose the locale from the **Select Locale** drop-down list.

From Cisco Catalyst SD-WAN Manager Release 20.13.1 **Select Locale** option is available.

Step 8 Click **Copy**.

Delete user

If a user no longer needs access to devices, you can delete the user. Deleting a user does not log out the user if the user is logged in.

Procedure

Step 1 For the user you wish to delete, click **...**, and click **Delete**.

Step 2 To confirm the deletion of the user, click **OK**.

Change user password

Change user password with these steps.

Procedure

Step 1 To change the password for a user, click **...** and click **Change Password**.
Step 2 Enter the current user password in **Current logged in User Password** field.
Step 3 Enter the new password in the **New Password for User** field.
Step 4 Enter the new password again in the **Confirm New Password for User** field.
Step 5 Click **Update**.

Reset locked user

Procedure

Step 1 To reset the lock for a user, click **...** and click **Reset Locked User**.
Step 2 In the **Reset Locked User** pop-up menu, click **Yes**.

Apply administrative lock

Procedure

Step 1 To apply administrative lock for a user, click **...** and click **Administrative Lock**.
Step 2 In the **Lock User** pop-up menu, click **Yes**.

View users logged in to a device using SSH sessions

You can monitor users logged in to a device using SSH sessions using these steps.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

For Cisco vManage Release 20.6.x and earlier, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

Step 2 Select the device you want to use under the **Hostname** column.

Step 3 Click **Real Time**.

Step 4 From **Device Options**, choose **AAA users** for Cisco IOS XE Catalyst SD-WAN devices.

You will see a list of users logged in to the device.

View users with active HTTP sessions

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**.

Step 2 Click **User Sessions**.

A list of all the active HTTP sessions within Cisco SD-WAN Manager is displayed, including, username, domain, source IP address, and so on.

Configure user sessions

User Sessions page shows a list of all the active HTTP sessions within SD-WAN Manager, including username, domain, source IP address, and so on.

To remove a user session, choose the session from the list, and click **Remove Session**.

Configure VPN segments

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **VPN Segments**.

A web page displays the list of configured segments.

Step 2 To edit or delete an existing segment, click **…**, and click **Edit** or **Delete**.

Step 3 To add new segment, click **Add Segment**.

Step 4 Enter the name of the segment in the **Segment Name** field.

Step 5 Enter the number of VPNs you want to configure in **VPN Number** field.

Step 6 To add a new segment, click **Add**.

Configure VPN groups

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **VPN Groups**.

A web page displays the list of groups that are configured.

Step 2 To edit or delete a VPN group, click **…**, and click **Edit** or **Delete**.

Step 3 To view the existing VPN in the dashboard, click **…**, and click **View Dashboard**.

The **VPN Dashboard** displays the device details of the VPN device configured.

Step 4 To add a new VPN group, click **Add VPN Group** and enter these details:

a) Provide a VPN group name in the **VPN Group Name** field.
b) Enter a brief description of the VPN in the **Description** field.
c) Check **Enable User Group access** check box and enter the user group name.
d) From **Assign Segment**, click **Add Segment** drop-down list to add a new or existing segment to the VPN group.
e) Enter the **Segment Name** and **VPN Number** in the respective fields.

Step 5 Click **Save**.

Verify granular RBAC permissions

Use this procedure to verify the permissions that you have configured for a user group.

Before you begin

This verification method is supported for Cisco vManage Release 20.7.1 and later.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**.

Step 2 Click **User Groups**.

Step 3 In the pane that displays the user groups, select a user group to display the read and write permissions assigned to the user group.

Step 4 Scroll to the permissions that control template access to verify your configuration for the user group.

Monitor devices for VPN groups

To monitor devices for VPN groups, use these instructions.

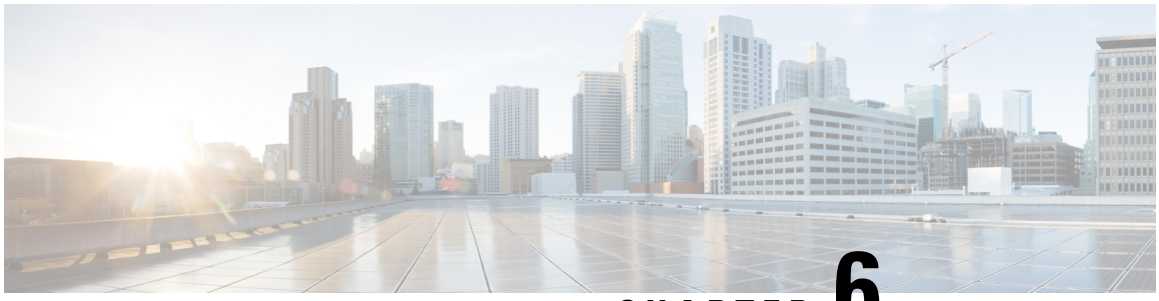
Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

Step 2 Click **WAN - Edge**.

Step 3 Select the **VPN Group** and **VPN Segment** for which you want to monitor the network.

A web page displays the list of VPN groups and segments that are configured to a device.



CHAPTER 6

System Logging

- Feature history: System logging, on page 119
- System logging, on page 119
- Configure system logging, on page 125
- Create a certificate signing request and install feature certificates, on page 139
- Viewing system log information, on page 139
- Verifying the trustpoint configuration on a device, on page 140
- Remote logging over TCP and TLS, on page 141

Feature history: System logging

Developments in system logging, release by release.

Table 22: Feature history

Feature Name	Release Information	Description
Ability to Send Syslog Messages over TLS	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This feature allows you to transport syslog messages to external configured hosts by establishing a Transport Layer Security (TLS) connection. Using the TLS protocol enables the content of syslog messages to remain confidential, secure, and untampered or unaltered during each hop.
Remote Logging Over TCP and TLS in Cisco Catalyst SD-WAN Control Components	Cisco Catalyst SD-WAN Control Components Release 20.13.1	The feature allows remote logging of syslog messages through TCP and TLS. This feature is now available on Cisco Catalyst SD-WAN Control Components (Cisco Catalyst SD-WAN Controller, Cisco Catalyst SD-WAN Validator, and Cisco Catalyst SD-WAN Manager) in addition to Cisco IOS XE Catalyst SD-WAN devices.

System logging

System logging is a process that

- records a text log of system events using a mechanism similar to the UNIX syslog command,
- allows devices to send log messages with configurable priority levels to UNIX-style syslog services, and
- supports secure transmission over the Transport Layer Security (TLS) protocol.

Priority levels

Log messages have levels that indicate their priority. These are the same as for standard UNIX commands. You can configure the priority of syslog messages.

Security

Cisco IOS XE Catalyst SD-WAN devices send syslog messages to syslog servers on configured external hosts using TCP and UDP. When the devices send the syslog messages, the messages might transit several hops to reach the output destination. The intermediate networks during the hops might not be trustworthy, be in a different domain, or have a different security level. Therefore, Cisco IOS XE Catalyst SD-WAN devices support sending secure syslog messages over TLS as described in RFC 5425. To secure the syslog message content from potential tampering, the TLS protocol is used for certificate exchange, mutual authentication, and ciphers negotiation.

Cisco IOS XE Catalyst SD-WAN devices support both mutual and server authentication for sending syslog messages over TLS.

Benefits of using TLS

- Message confidentiality

  Confidentiality of message content where each TLS session begins with a handshake between the Cisco IOS XE Catalyst SD-WAN device and the syslog server. The Cisco IOS XE Catalyst SD-WAN device and syslog server agree on the specific security key and the encryption algorithms to be used for that session. The TLS session opposes any disclosure of the contents of the syslog message.

- Message integrity

  Integrity-checking of the content of each message to disable modifications to a message during transit on a hop-by-hop basis.

- Authentication

  Mutual authentication between the Cisco IOS XE Catalyst SD-WAN device and syslog server ensures that the syslog server accepts log messages only from authorized clients through certificate exchange.

System log files

System log (syslog) messages that are at or above the default or configured priority value are recorded in a number of files in the `/var/log` directory on the local device of the syslog server. The log files contain these items.

Table 23: Log files

File	Contents
auth.log	Login, logout, and superuser access events, and usage of authorization systems.

File	Contents
kern.log	Kernel messages.
messages.log	Consolidated log file that contains syslog messages from all sources.
vconfd.log	All configuration-related syslog messages.
vdebug.log	All debug messages for modules whose debugging is turned on. All syslog messages that are above the default priority value. The debug log messages support various levels of logging based on the module. The different modules implement the logging levels differently. For example, the system manager (sysmgr) has two logging levels (on and off), while the chassis manager (chmgr) has four different logging levels (off, low, normal, and high). You cannot send debug messages to a remote host. To enable debugging, use the **debug** operational command.
vsyslog.log	All syslog messages from Cisco Catalyst SD-WAN processes (daemons) that are above the configured priority value. The default priority value is "informational", so by default, all "notice", "warning", "error", "critical", "alert", and "emergency" syslog messages are saved.
vmanage-syslog.log	Cisco SD-WAN Manager audit log messages

Unused log files

Cisco Catalyst SD-WAN does not use these standard Linux files, which are available in the `/var/log` directory:

- cron.log
- debug.log
- lpr.log
- mail.log
- syslog

System log formats

Syslog messages begin with a percent sign (%) and come in these formats:

- Sequence and timestamp

  sequence-number:*timestamp*: %*facility-severity-MENEMONIC*:*description (hostname-n)*

- Format based on RFC5424

  <pri>ver timestamp hostname appname procid msgid structured-data description/*msg*

  The optional fields such as *hostname*, *appname*, *procId*, *msgId*, and *structured-data* are specified with a -.

Table 24: Field descriptions

Field	Description
facility	Sets the logging facility to a value other than 20, which UNIX systems expect.
severity	Importance or severity of the message, 0 to 7. A lower number indicates a greater severity of the system condition.
msg or description	Text string that describes the condition of the syslog server. This portion of the syslog message sometimes includes IP addresses, interface names, port numbers, or usernames. In syslog message formats based on RFC5424, the description is: *%facility-severity-MENEMONIC:description*

Examples

This system logging message includes a priority value, sequence number, and timestamp:

*<45>10: polaris-user1: *Jun 21 10:76:84.100: %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to administratively down*

This RFC5424-format message has a priority value, version of syslog protocol specification, and timestamp:

<45>1 2003-10-11T22:14:15.003Z 10.64.48.125 polaris-user1 - - - %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to administratively down

Note The time stamp formats are not the same in both the syslog message formats. In the message format based on RFC5424, T, and Z are mandatory where T represents a separator and Z represents zero timezone.

System log message levels

Each system log (syslog) message has a severity, or priority, level. A lower severity number means a higher severity. The default priority value is 6 (informational). By default, all syslog messages are recorded.

Table 25: System log message severity levels

Severity level	Name	Description
0	Emergency	System is unusable.
1	Alert	System in a state that requires immediate action.
2	Critical	Serious condition.
3	Error	Error condition that does not fully impair system usability.
4	Warning	Minor error condition.

Severity level	Name	Description
5	Notice	Normal operation, but with a significant condition requiring notice.
6	Informational	Routine condition (default).
7	Debug	Debug messages.

Sending system log messages to a server, using TLS

Transport layer security (TLS) is a networking protocol that provides secure communication through a network.

Benefits of using TLS for sending syslog messages

The benefits of using TLS for sending syslog messages are:

- Confidentiality

  Confidentiality of message content where each TLS session begins with a handshake between the Cisco IOS XE Catalyst SD-WAN device and the syslog server. The Cisco IOS XE Catalyst SD-WAN device and syslog server agree on the specific security key and the encryption algorithms to be used for that session. The TLS session opposes any disclosure of the contents of the syslog message.

- Integrity-checking

  Integrity-checking of the content of each message to disable modifications to a message during transit on a hop-by-hop basis.

- Mutual authentication

  Mutual authentication between the Cisco IOS XE Catalyst SD-WAN device and syslog server ensures that the syslog server accepts log messages only from authorized clients through certificate exchange.

Authentication type

- **Server**

  With server authentication, edge devices verify the identity of the syslog server. If the syslog server and the certificate are legitimate entities, the device establishes a TLS connection with the server.

  As part of server authentication, the syslog server shares its public certificate with the devices.

  See the prerequisite in the "Before you begin" section of this procedure.

  With this option, all information about TLS profiles, except the trustpoint information, is saved.

- **Mutual**

  With mutual authentication, edge devices and the syslog server authenticate each other at the same time.

  Devices require root or identity certificates for mutual authentication of the TLS session.

  With this option, a trustpoint, such as SYSLOG-SIGNING-CA certificate, is saved on the device. This enables SD-WAN Manager to install the certificate from the edge device.

Restrictions for system logging

Disabling system logging to disk

Disabling system logging to disk (`no system logging disk enable`) does not disable `vsyslog`.

Storage restrictions

The messages sent to syslog files are not rate-limited and consequently:

- A storage limit of 10 log files with a capacity of up to 16 MB size is set for each syslog file.
  - When the storage capacity exceeds the 16 MB size limit, the log file is saved as a .GZ file along with the date appended to it.
  - When the storage limit exceeds 10 log files, the oldest log file is dropped.
- If many syslog messages are generated in a short span of time, the overflowing messages are buffered and queued to be stored in the syslog file.

Repeating or identical messages

For repeating syslog messages or identical messages that occur multiple times in succession, only one copy of the message is placed in the syslog file. The message is annotated to indicate the number of times the message occurred.

Maximum length

The maximum length of a log message is 1024 bytes. The longer messages are truncated.

The maximum length of a log message for Cisco SD-WAN Manager audit logs is 1024 bytes. The longer messages are truncated into smaller fragments and each of these fragments are indicated by an identifier. The identifiers are

- fragment 1/2
- fragment 2/2

and so on.

For example, a long audit log message when truncated into smaller fragments appears as:

```
local6.info: 18-Oct-2020 17:42:07 vm10 maintenance-fragment-1/2: {“logid”: “d9ed576a-...”,
 “entry_time”:
1576605512190, “statcycletime” 34542398334245, “logmodule”:”maintenance”, “logfeature”:
“upgrade”, “loguser”: “admin”, “logusersrcip”:
“10.0.1.1”, “logmessage”: “Device validation Upgrade to version :  Validation success”,
“logdeviceid”:”Validation”, “auditdetails” :
[“[18-Oct-2020 17:42:08 UTC] Published messages to vmanage(s)”, “auditdetails”:[“[18-Oct-2020
 17:42:07 UTC] Software image: vmanage-99.99.999-
x86_64.tar.gz”, “Software image download may take up to 60}

local6.info: 18-Oct-2020 17:42:07 vm10 maintenance-fragment-2/2: { minutes”, “logprocessid”:
 “software_install-7de0ec44-...”, “tenant”:, “default”}
```

AAA authentication and Netconf CLI access

Syslog messages related to AAA authentication and Netconf CLI access and usage are placed in the auth.log and messages.log files. Each time a Cisco SD-WAN Manager logs into a router to retrieve statistics and status information and to push files to the router, the router generates AAA and Netconf log messages. Over time, these messages can fill the log files. To prevent these messages from filling the log files, you can disable the logging of AAA and Netconf syslog messages.

Restrictions for TLS authentication

Cisco IOS XE Catalyst SD-WAN devices support both server authentication and mutual TLS (mTLS) authentication for syslog over TLS.

Cisco Catalyst SD-WAN Control Components support only server authentication for syslog over TLS. Mutual TLS (mTLS) authentication is not supported.

Configure system logging

Use one of these methods to configure system logging:

- Configuration group
- Feature template
- CLI commands



Note Some configurations and protocols are identified as insecure and is a security risk for Cisco devices. Existing deployments continue to function, but new installations require intentional enablement. For more information on remediation, refer to Resilient Infrastructure: Cisco Catalyst SD-WAN and Routing

Configure system logging using a configuration group

System logging is the process of keeping a text log of system events.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Follow these steps to configure system logging for a device, using a configuration group:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure a Logging feature in a System profile.

a) Enter the disk information.

Table 26: Disk

Field	Description
Enable Disc	Enable this option to allow syslog messages to be saved in a file on the local hard disk, or disable this option to disallow it. By default, logging to a local disk file is enabled on all Cisco IOS XE Catalyst SD-WAN devices.
Max File Size(In Megabytes)	Enter the maximum size of syslog files. The syslog files are rotated on an hourly basis based on the file size. When the file size exceeds the configured value, the file is rotated and the syslog process is notified. Range: 1 to 20 MB Default: 10 MB
Rotations	Enter the number of syslog files to create before discarding the oldest files. Range: 1 to 10 Default: 10

b) Enter the TLS Profile information.

Table 27: TLS Profile

Field	Description
Add TLS Profile	
TLS Profile Name*	Enter the name of the TLS profile.
TLS Version	Choose a TLS version: • **TLSv1.1** • **TLSv1.2**
Authentication Type*	Choose **Server**.

Field	Description
Cipher Suite List	Choose groups of cipher suites (encryption algorithm) based on the TLS version. Cipher suites: • **aes-128-cbc-sha**: Encryption type tls_rsa_with_aes_cbc_128_sha • **aes-256-cbc-sha**: Encryption type tls_rsa_with_aes_cbc_256_sha • **dhe-aes-cbc-sha2**: Encryption type tls_dhe_rsa_with_aes_cbc_sha2 (TLS1.2 and above) • **dhe-aes-gcm-sha2**: Encryption type tls_dhe_rsa_with_aes_gcm_sha2 (TLS1.2 and above) • **ecdhe-ecdsa-aes-gcm-sha2**: Encryption type tls_ecdhe_ecdsa_aes_gcm_sha2 (TLS1.2 and above) SuiteB • **ecdhe-rsa-aes-cbc-sha2**: Encryption type tls_ecdhe_rsa_aes_cbc_sha2 (TLS1.2 and above) • **ecdhe-rsa-aes-gcm-sha2**: Encryption type tls_ecdhe_rsa_aes_gcm_sha2 (TLS1.2 and above) • **rsa-aes-cbc-sha2**: Encryption type tls_rsa_with_aes_cbc_sha2 (TLS1.2 and above) • **rsa-aes-gcm-sha2**: Encryption type tls_rsa_with_aes_gcm_sha2 (TLS1.2 and above)

c) Enter the server information.

Table 28: Server

Field	Description
Add Server	
Hostname/IPv4 Address*	Enter the DNS name, hostname, or IP address of the system on which to store syslog messages. To add another syslog server, click the plus sign (+). To delete a syslog server, click the trash icon to the right of the entry.
VPN*	Enter the identifier of the VPN in which the syslog server is located or through which the syslog server can be reached. Range: 1 to 65525, excluding 512. For details see the VRF range behavior change described here.
Source Interface	Enter the specific interface to use for outgoing system log messages. The interface must be located in the same VPN as the syslog server. Otherwise, the configuration is ignored. If you configure multiple syslog servers, the source interface must be the same for all of them.

Field	Description
Priority	Select the severity of the syslog message to save. The severity indicates the seriousness of the event that generated the message. Priority can be one of these: • **informational**: Routine condition (the default) (corresponds to syslog severity 6) • **debugging**: Prints additional logs to help debugging the issue. • **notice**: A normal, but significant condition (corresponds to syslog severity 5) • **warn**: A minor error condition (corresponds to syslog severity 4) • **error**: An error condition that does not fully impair system usability (corresponds to syslog severity 3) • **critical**: A serious condition (corresponds to syslog severity 2) • **alert**: Action must be taken immediately (corresponds to syslog severity 1) • **emergency**: System is unusable (corresponds to syslog severity 0)
TLS Enable*	Enable this option to allow syslog over TLS. When you enable this option, these fields appear: **TLS Properties Custom Profile**: Enable this option to choose a TLS profile. When you enable this option, the following field appears: **TLS Properties Profile**: Choose a TLS profile that you have created for server or mutual authentication in the IPv4 server configuration.
Add IPv6 Server	
Hostname/IPv6 Address*	Enter the DNS name, hostname, or IP address of the system on which to store syslog messages. To add another syslog server, click the plus sign (+). To delete a syslog server, click the trash icon to the right of the entry.
VPN*	Enter the identifier of the VPN in which the syslog server is located or through which the syslog server can be reached. Range: 1 to 65525, excluding 512. For details see the VRF range behavior change described here.
Source Interface	Enter the specific interface to use for outgoing system log messages. The interface must be located in the same VPN as the syslog server. Otherwise, the configuration is ignored. If you configure multiple syslog servers, the source interface must be the same for all of them.

Field	Description
Priority	Select the severity of the syslog message to save. The severity indicates the seriousness of the event that generated the message. Priority can be one of these: • **informational**: Routine condition (the default) (corresponds to syslog severity 6) • **debugging**: Prints additional logs to help debugging the issue. • **notice**: A normal, but significant condition (corresponds to syslog severity 5) • **warn**: A minor error condition (corresponds to syslog severity 4) • **error**: An error condition that does not fully impair system usability (corresponds to syslog severity 3) • **critical**: A serious condition (corresponds to syslog severity 2) • **alert**: Action must be taken immediately (corresponds to syslog severity 1) • **emergency**: System is unusable (corresponds to syslog severity 0)
TLS Enable*	Enable this option to allow syslog over TLS.
TLS Properties Custom Profile*	Enable this option to choose a TLS profile.
TLS Properties Profile	Choose a TLS profile that you have created for server or mutual authentication in the IPv6 server configuration.

What to do next

Refer to Deploy a Configuration Group in the *Cisco Catalyst SD-WAN Configuration Groups Reference Guide*.

Configure system logging using a template

System log (syslog) messages are a text log of system events.

On Cisco IOS XE Catalyst SD-WAN devices, you can save system log messages locally or to a remote server.

Before you begin

Follow these steps to configure system logging for a device, using a feature template.

Procedure

Step 1 Create a System Logging feature template.

Refer to Create a System Logging feature template, on page 130.

Step 2 Choose whether to save system log messages locally or to a syslog server. If saving messages to a server, choose whether to use the Transport Layer Security (TLS) protocol.

Configure a device to save system log messages to a server, using TLS, on page 131

a) If you choose to save syslog messages locally, do this:

Configure a device to save system log messages locally, on page 130

b) If you choose to save syslog messages to a syslog server, without using TLS, do this:

c) If you choose to save syslog messages to a syslog server, using TLS, with authentication by the server, do this:

d) If you choose to save syslog messages to a syslog server, using TLS, with mutual authentication by the edge device and the server, do this:

Create a System Logging feature template

System log (syslog) messages are a text log of system events.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**, and select **Add Template**.

In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

Step 3 From **Select Devices**, select the device for which you wish to create a template.

Step 4 To create a template for logging, select **Cisco Logging**.

The Cisco logging template form displays fields for naming the template and defining the logging parameters. Click a tab or the plus sign (+) to view additional fields.

When you first open a feature template, SD-WAN Manager sets the scope to default, for parameters that have a default value. The default setting or value appears next to each parameter. To change the default or enter a value, select a different option from the scope drop-down list to the left of the parameter field.

Step 5 In **Template Name**, enter a name for the template.

The name may contain up to 128 alphanumeric characters.

Step 6 In **Template Description**, enter a description of the template.

The description may contain up to 2048 alphanumeric characters.

Configure a device to save system log messages locally

System log (syslog) messages are a text log of system events.

You can save system log messages locally or to an external server. This procedure configures a device to save system messages locally.

Before you begin

Follow these steps to configure a device to save system log messages to a local drive.

Procedure

Step 1 In a System Logging template, in the **Disk** section, configure these parameters:

Field	Description
Enable Disk	To save syslog messages in a file on the local hard disk, click **On** or **Off** to disallow saving. Default: Logging to a local disk file is enabled.
Maximum File Size	Enter the maximum size of syslog files. The system log files are rotated on an hourly basis based on the file size. When the file size exceeds the configured value, the file is rotated and the syslogd process is notified. Range: 1-20 MB Default: 10 MB
Rotations	Enter the number of syslog files to create before discarding the earliest created files. Range: 1-10 MB Default: 10 MB

Step 2 To save the feature template, click **Save**.

Configure a device to save system log messages to a server, using TLS

System log (syslog) messages are a text log of system events.

You can send system log messages to an external server over a Transport Layer Security (TLS) connection.

For the TLS connection, there are two methods of authentication, configured by the **Authentication Type** parameter.

- Server authentication: Authentication by the server.
- Mutual authentication: Authentication by both the device and the server.

See Sending system log messages to a server, using TLS, on page 123.

Before you begin

For the server authentication option, edge devices must have a root certificate authority (CA) preinstalled, which you configure using cryptographic module CLIs. See *Install root CA on Cisco IOS XE Catalyst SD-WAN device*.

Follow these steps to configure the TLS parameters for saving syslog messages to an external server over a TLS connection.

Procedure

Step 1 In a System Logging template, in the **TLS** section, click **New Profile**.

Step 2 Configure these parameters:

Field	Description
Profile Name	Enter the TLS profile name.
TLS Version	Choose TLS versions v1.1 or v1.2.
Authentication Type	Choose the authentication type: • **Server** With server authentication, edge devices verify the identity of the syslog server. If the syslog server and the certificate are legitimate entities, the device establishes a TLS connection with the server. As part of server authentication, the syslog server shares its public certificate with the devices. See the prerequisite in the "Before you begin" section of this procedure. With this option, all information about TLS profiles, except the trustpoint information, is saved. • **Mutual** With mutual authentication, edge devices and the syslog server authenticate each other at the same time. Devices require root or identity certificates for mutual authentication of the TLS session. With this option, a trustpoint, such as SYSLOG-SIGNING-CA certificate, is saved on the device. This enables SD-WAN Manager to install the certificate from the edge device.
Ciphersuites	Choose cipher suites (encryption algorithms) based on the TLS version.

Step 3 To save the feature template, click **Save**.

Configure a device to save system log messages to a server

System log (syslog) messages are a text log of system events.

Before you begin

Follow these steps to configure a device to save system log messages to a server.

Procedure

Step 1 Click **Server**.

Step 2 Click **Add New Server**, and configure these parameters:

Field	Description
Hostname/IP Address	Enter the DNS name, hostname, or IPv4, IPv6 address of the system on which to store syslog messages. To add another syslog server, click **+**. To delete a syslog server, click .
VPN ID	Enter the identifier of the VPN in which the syslog server is located or through which the syslog server can be reached. VPN ID Range: 0 to 65530
Source Interface	Enter the specific interface to use for outgoing system log messages. The interface must be located in the same VPN as the syslog server. Otherwise, the configuration of syslog servers is ignored. If you configure multiple syslog servers, the source interface must be same for all of them.
Priority	Choose a severity of the syslog message to be saved. The severity indicates the seriousness of the event that generated the syslog message. See System log message levels, on page 122.
TLS	For Cisco IOS XE Catalyst SD-WAN devices, click **On** to enable syslog over TLS.
Custom Profile	For Cisco IOS XE Catalyst SD-WAN devices, click **On** to enable choosing a TLS profile, or click **Off** to disable choosing a TLS profile.
TLS Profile	For Cisco IOS XE Catalyst SD-WAN devices, choose a TLS profile that you have created for server or mutual authentication in IPv4 or IPv6 server configuration.

Step 3 To save the feature template, click **Save**.

Configure system logging using CLI commands

You can save event notification system log (syslog) messages locally or to a remote server. These event notification logs are converted to system log files and exported to the syslog server. You can then retrieve system log information from the syslog server.

- Configure system logging, saved locally, using CLI commands, on page 134
- Configure system logging, saved remotely, using CLI commands, on page 135

Configure system logging, saved locally, using CLI commands

System logging is the process of keeping a text log of system events.

By default, a priority level of "information" is enabled when you log syslog messages to a file on a local device.

For more information about logging disk commands, see the logging disk command.

Before you begin

Follow these steps to configure system logging for a device, saving syslog messages locally, using CLI commands:

Procedure

Step 1 Log syslog messages to a drive.

logging disk

Step 2 Enable logging to a drive.

enable

Step 3 Specify the size of syslog files in megabytes (MB).

By default, the syslog files are 10 MB. You can configure the size of syslog files to be 1 to 20 MB.

file size *size*

Step 4 Rotate syslog files on an hourly basis based on the size of the file.

By default, 10 syslog files are created. You can configure the rotate command to be a number from 1 through 10.

file rotate *number*

Example

```
Device(config-system)# logging disk
Device(config-logging-disk)# enable
Device(config-logging-disk)# file size 3
Device(config-logging-disk)# file rotate 3
```

Configure system logging, saved remotely, using CLI commands

System logging is the process of keeping a text log of system events.

If the syslog server is unreachable, the system suspends sending syslog messages for 180 seconds. When the server becomes reachable, logging resumes. For more information about logging server commands, see the logging server command.

Before you begin

Follow these steps to configure system logging for a device, saving syslog messages a remote server, using CLI commands:

Procedure

Step 1 Log syslog messages to a remote host or syslog server.

You can configure the name of the server by DNS name, hostname, or IP address. You can configure up to four syslog servers.

logging server

Step 2 If using a VPN, specify the VPN ID of the syslog server.

vpn *vpn-id*

Step 3 (Optional) Specify the source interface to reach the syslog server.

The interface name can be a physical interface or a sub-interface (a VLAN-tagged interface). Ensure that the interface is located in the same VPN as the syslog server. Otherwise, the configuration is ignored. If you configure multiple syslog servers, the source interface must be the same for all of them.

source interface *interface*

Step 4 Specify the severity of the syslog message to be saved.

The default priority value is "informational" and by default, all syslog messages are recorded. See the logging server command reference documentation for priority values.

priority *alert*

Example

```
Device(config-system)# logging server 192.168.0.1
Device(config-server-192.168.0.1)# source interface eth0
Device(config-server-192.168.0.1)# priority notice
```

Install a root certificate on a device for mutual authentication

To configure Cisco IOS XE Catalyst SD-WAN devices with Transport Layer Security (TLS) syslog protocol, the devices must have root or identity certificates for mutual authentication of TLS session. You can either use a third-party Certificate Authority (CA) to get public key infrastructure (PKI) services, or Microsoft Active

Directory Certificate Services (AD CS). AD CS allows you to build a PKI and provide public key cryptography, digital certificates, and digital signature capabilities for your requirement.

Before you begin

Follow these steps to install a root certificate on a device for mutual authentication.

Procedure

Step 1 Generate the enterprise root certificate using a third party CA or Microsoft Active Directory Certificate Services.

Step 2 Download the root CA in base 64 format, select and copy the content of root CA.

Step 3 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Step 4 Click **Enterprise Feature Certificate Authorization**.

Step 5 Paste the root CA content in the **Enterprise Root Certificate** box.

Step 6 If you want to generate a certificate signing request (CSR), check the **Set CSR Properties** check box.

Step 7 Click **Close**.

The root CA is uploaded to SD-WAN Manager, and SD-WAN Manager saves the root certificate to the device.

Install a root certificate authority on a syslog server for server authentication

This procedure sets up the syslog-ng server tool on a server using Linux. The tool supports TLS.

The details of setting up a server, and installing the syslog-ng tool are beyond the scope of this documentation. The basic information provided here is for reference, and is subject to change.

Before you begin

Follow these steps to install a root certificate authority on a syslog server for server authentication.

Procedure

Step 1 On the Linux server, install the syslog-ng package.

```
apt-get install syslog-ng openssl
```

Step 2 In the directory of the syslog-ng tool, create directories to store root certificates.

```
# cd /etc/syslog-ng
# mkdir cert.d
# mkdir key.d
# mkdir ca.d
# cd cert.d
# openssl req -new -x509 -out cacert.pem -days 1095 -nodes
# mv privkey.pem ../key.d
```

After using the **openssl** command, an encoded root certificate is available in `cacert.pem` file. The file is located in the `cd/etc/syslog-ng/cert.d` directory.

Step 3 Copy the contents of the `cacert.pem` file when installing root certificate on a device.

Install a root certificate authority on a device for server authentication, using CLI commands

Before you begin

Generate an encoded CA certificate on the syslog server. This is required in one of the steps. For instructions, see Install a root certificate authority on a syslog server for server authentication, on page 136.

Follow these steps to install a root certificate authority on a device, for server authentication.

Procedure

Step 1 To configure a public key infrastructure (PKI) trustpoint for a certificate authority, use these commands on a device, for authorizing and revocation of certificates in PKI.

a) Enable privileged EXEC mode.

```
enable
```

b) Enter configuration mode.

```
config-transaction
```

c) Declare the trustpoint and a given name and enter CA-trustpoint configuration mode. Specify the enrollment parameters and fingerprint for the CA. Obtain the fingerprint from the fingerprint.txt.

```
crypto pki trustpoint name
```

Example:

```
Device(config)# crypto pki authenticate PROXY-SIGNING-CA
        enrollment url bootflash:
        revocation-check none
        rsakeypair PROXY-SIGNING-CA 2048
        subject-name cn=proxy-signing-cert
        fqdn none
        fingerprint 54F371C8EE2BFB06E2C2D0944245C288FBB07163
```

d) If the authentication in the previous step fails, contact the PKI team for assistance.

For information about syslog configuration, see Cisco SD-WAN IOS XE TLS Syslog Configuration on syslog-ng Server.

e) Configure the level to which a certificate chain is processed on all certificates.

```
chain-validation [{stop | continue}[parent-trustpoint]]
```

Example:

```
Device(ca-trustpoint)# chain-validation stop
```

f) Optionally, check the revocation status of a certificate.

```
revocation-check method
```

Example:

```
Device(ca-trustpoint)# revocation-check none
```

g) Return to global configuration mode.

exit

Example:

```
Device(ca-trustpoint)# exit
```

Step 2 Authenticate the root CA.

This is necessary before installing the server's root certificate.

crypto pki authenticate

Example:

```
Device(config)# crypto pki authenticate root
```

Step 3 Copy the block of text containing the base 64 encoded CA certificate from the syslog server, and paste it at the prompt.

The prerequisites section refers to the instructions for generating the encoded CA certificate on the syslog server.

Example:

An example encoded CA certificate:

```
-----BEGIN CERTIFICATE-----
MIID9jCCAt6gAwIBAgIJAM5b3nyjDAKIMA0GCSqGSIb3DQEBCwUAMIGPMQswCQYD
VQQGEwJJTjESMBAGA1UECAwJS2FybmF0YWthMRIwEAYDVQQHDAlCYW5nYWxvcmUx
...
+3RcM0VqjScIOZhp97dqfBlHEdqUE/QfKlBt12KU+0sj8yJJC+cuKlHQj5JGmGLI
Y6r7bMcn99Y6Rw==
-----END CERTIFICATE-----
```

Step 4 Enter **yes** to confirm the acceptance of the certificate.

The root CA certificate from the syslog server is installed on a device, enabling server authentication.

```
crypto pki trustpoint PROXY-SIGNING-CA
    enrollment url bootflash:
    revocation-check none
    rsakeypair PROXY-SIGNING-CA 2048
    subject-name cn=proxy-signing-cert
    fqdn none
    fingerprint 54F3...7163  >> The fingerprint configured was obtained from the
fingerprint.txt file.
commit
```

```
crypto pki authenticate PROXY-SIGNING-CA
Reading file from bootflash:PROXY-SIGNING-CA.ca
Certificate has the following attributes:
Fingerprint MD5: 7A97B30B ... 66488DCF
Fingerprint SHA1: 21E0F09B ... D39A268A
Trustpoint Fingerprint: 21E0F09B ... D39A268A
Certificate validated - fingerprints matched.
Trustpoint CA certificate accepted.
```

Create a certificate signing request and install feature certificates

This procedure validates and authenticates devices and the syslog server.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.

Step 2 From **Certificates**, select a device.

a) Generate a feature certificate signing request (CSR).

Refer to Certificate Management in the *Cisco Catalyst SD-WAN Getting Started Guide*.

After you generate the feature CSR, the **View Feature CSR** and **Install Feature certificate** options are available.

b) View and download the feature CSR.

Refer to Certificate Management in the *Cisco Catalyst SD-WAN Getting Started Guide*.

Step 3 To sign the certificate, send the certificate to a third-party signing authority.

Step 4 Import the certificate into Cisco IOS XE Catalyst SD-WAN devices.

Refer to Certificate Management in the *Cisco Catalyst SD-WAN Getting Started Guide*.

SD-WAN Manager uses the signed certificate and installs it on devices.

After the feature certificate installation is successful, options are available in SD-WAN Manager to revoke or view a feature certificate.

Viewing system log information

View system log information, using SD-WAN Manager or using CLI commands.

View system logs using SD-WAN Manager

System logging records a text log of system events.

Before you begin

In SD-WAN Manager, in **Administration** > **Settings**, enable **Data Stream**.

View device-specific system log (syslog) files in Cisco SD-WAN Manager.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

In Cisco vManage Release 20.6.x and earlier, choose **Monitor** > **Network**.

Step 2 Select a device.

Step 3 Click **Troubleshooting**.

Step 4 In the **Logs** section, click **Debug Log**.

Step 5 From **Log Files**, select the name of a log file to view the log information.

Viewing system log information using CLI commands

You can use these CLI commands to view system log (log) information.

Viewing system log settings

To view system log settings after logging system log messages to a remote host, use the **show logging** command.

```
Host(config-server-192.168.0.1)# show logging
System logging
    server 192.168.0.1
    source interface eth0
    exit
!
!
```

Viewing system log files

To view the contents of the system log file, use the **show log** command.

```
Host(config-server-192.168.0.1)# show log nms/vmanage-syslog.log tail 10
```

Verifying the trustpoint configuration on a device

Display the contents of a syslog file to verify the trustpoint configuration.

Verifying server authentication

Example:

```
Cisco XE SD-WAN# show crypto pki trustpoints status
crypto pki trustpoint SYSLOG-SIGNING-CA
  enrollment url bootflash:vmanage-admin/
  fqdn none
  fingerprint xxxxxx
  revocation-check none
  subject-name CN=CSR-cbc47d9d-..._vManage Root CA
```

Verifying mutual authentication

Example:

```
Cisco XE SD-WAN# show crypto pki trustpoints status

crypto pki trustpoint SYSLOG-SIGNING-CA
  enrollment url bootflash:vmanage-admin/
  fqdn none
  fingerprint xxxxxx
  revocation-check none
  rsakeypair SYSLOG-SIGNING-CA 2048
  subject-name CN=CSR-cbc47d9d-..._vManage Root CA
```

Verify trustpoints on a device for a syslog-signing-CA certificate

Example:

```
Cisco XE SD-WAN# show crypto pki trustpoints SYSLOG-SIGNING-CA status

Trustpoint SYSLOG-SIGNING-CA:

 Issuing CA certificate not configured.

State:

Keys generated ..... No

 Issuing CA authenticated ..... No

  Certificate request(s) ..... None
```

Remote logging over TCP and TLS

Remote logging refers to saving system log information on a remote server.

From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1, remote logging of syslog messages can include TCP and TLS transport methods, in addition to UDP. This applies to SD-WAN Control Component.

The default transport type for remote logging is UDP. But you can optionally select TCP or TLS as the transport method for remote logging.

Benefits of remote logging over TCP and TLS

These are benefits of remote logging over TCP and TLS.

- Syslog over TCP and TLS supports large-scale network environments. While TCP can handle large volumes of data, TLS can ensure that the log data is securely sent and protected from unauthorized access or tampering.
- You can configure up to four separate remote syslog servers with the option to assign each server a unique transport protocol such as UDP, TLS, or TCP. Alternatively, you can choose to use the same transport protocol for all four servers.
- For remote logging over TLS, a TLS profile supports TLS version 1.2. Also, various cipher suites can be accommodated within the TLS profile, depending on the TLS version.

Configure remote logging over TCP using CLI commands

Before you begin

Follow these steps to configure remote logging over TCP using CLI commands.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Configure a remote server with transport type TCP.

```
system
 logging
  server server-ip-address
  transport tcp port 514
```

```
system
logging
  disk
   enable
  !
  server 10.0.1.56
   transport tcp
  exit
!
!
```

Configure remote logging over TLS using CLI commands

Before you begin

Follow these steps to configure remote logging over TLS using CLI commands.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Use these steps to install, list, and uninstall the certificate authority (CA) certificate from the syslog server.

a) Install a certificate.

```
request logging ca-cert
install new syslog-ng ca
```

b) List all installed certificates.

```
show logging cacert
```

c) Uninstall a certificate if necesseary.

```
request logging ca-cert uninstall cert-name
```

Step 3 Create a TLS profile.

```
system
 logging
 tls-profile profile-name
  tls-version TLSv1.2
  ciphersuite ciphersuite1 ciphersuite2
```

Creating a TLS profile involves specifying the protocols and cipher suites that a device will use for secure communication. You can configure up to four TLS profiles.

Step 4 Attach a TLS profile to a remote logging server.

```
server server-ip-address
 vpn vpn-instance-of-logging-server
 source-interface interface-num
 transport tls
 tls-profile tls-profile-name
```

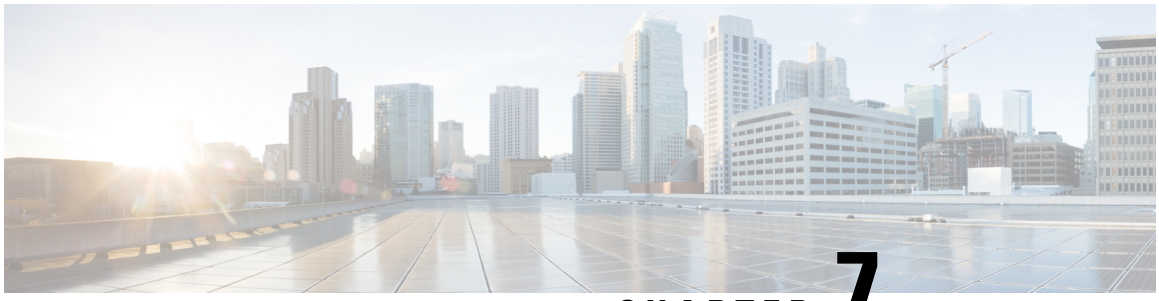
```
system
logging
  disk
   enable
  !
  tls-profile profile1
   version     TLSv1.2
   ciphersuite ECDHE-ECDSA-AES128-SHA256 AES256-GCM-SHA384 PSK-AES256-GCM-SHA384
PSK-AES128-GCM-SHA256 AES256-SHA256
  exit
  server 10.0.1.55
   source interface 10.1.1.12
   transport   tls
   tls-profile profile1
  exit
!
!
```

Verifying remote logging over TCP and TLS

View the installed certificates to verify that remote logging is possible over TCP and TLS.

The **show logging cacert** command shows installed certificates.

```
Device# show logging cacert
INDEX  NAME      VALIDITY
-----------------------------------------
0      cert.pem  Fri Jun 21 20:35:10 2024
```



CHAPTER 7

Device Tagging

- Feature history: Device tagging, on page 145
- Device tagging, on page 145
- Add device tags, on page 146
- Delete device tags, on page 147

Feature history: Device tagging

Feature history of device tagging, by release.

Table 29: Feature History

Feature Name	Release Information	Feature Description
Device tagging	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	Device tags are labels for tagging devices. You can use the tags for grouping, describing, finding, or managing devices.
Enhancements to user-defined device tagging	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	Device tagging has the following new functionality: • When you add devices to a configuration group using rules, you can choose **Match All** or **Match Any**. • You can use **Starts With** and **Ends With** operator conditions when you add devices to a configuration group using rules. In addition, the button formerly called **Add New Tag** is now **Create New Tag**.

Device tagging

Device tags are labels that

- help you group, describe, and locate devices more effectively, and
- enable adding devices to configuration groups using tag-based rules.

  For information about creating rules, refer to the information about adding devices to a configuration group using rules, in Using Configuration Groups in the *Cisco Catalyst SD-WAN Configuration Groups Reference Guide*.

You can assign multiple tags to a single device.

Single-tenant and multitenant support

You can use device tagging in both the single-tenant and multitenant deployments.

Restrictions for device tagging

Maximum number of tags

In Cisco vManage Release 20.11.1 and earlier:

- Use a maximum of 25 tags per Cisco SD-WAN Manager instance.
- Use a maximum of 25 tags per device.

Permitted characters

In Cisco vManage Release 20.11.1 and earlier:

- Maximum characters in a tag: 25
- Permitted characters: Only alphanumeric characters, hyphens (–), and underscores (_).
- Cannot contain space or any other special characters.
- Tag name is case-sensitive.

Maximum tag rules per configuration group

Cisco vManage Release 20.11.1 and earlier: You can add only one tag rule to a configuration group.

Add device tags

Device tags are labels that help you group, describe, locate, or perform actions on devices efficiently.

You can add multiple tags to a device and you can delete unwanted tags from a device. You can also add device tags to devices using the Quick Connect workflow. Refer to the Quick Connect Workflow section of the *Cisco Catalyst SD-WAN Onboarding Guide*.

Follow these steps to add a tag to a device.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.

Step 2 Click **WAN edge list** and choose a device.

Step 3 Click **Add tags**.

Step 4 Choose a tag from the list of existing tags or click **Create new tag**.

In Cisco vManage Release 20.11.1 and earlier, this was called **Add new tag**.

Step 5 Click **Apply**.

The specified tag is added to the device.

Delete device tags

You can delete only those tags that are not added to a device or are not a part of a tag rule.

Follow these steps to delete device tags from a device.

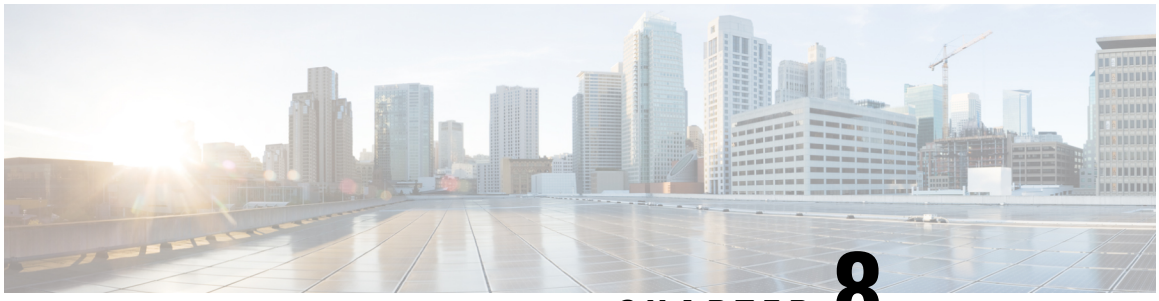
Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Tag Management**.

Step 2 Choose the tags that you want to delete.

Step 3 Click **Delete tags**.

Step 4 Click **Yes** to confirm.



CHAPTER 8

Configure Devices

- Feature history for configure devices, on page 149
- Configure devices in Cisco Catalyst SD-WAN, on page 150
- Configure and manage device templates, on page 156
- Configuration prerequisites, on page 169
- Device configuration workflow, on page 169
- Configure and manage devices using SD-WAN Manager, on page 170

Feature history for configure devices

Developments in device configuration, release by release.

Table 30: Feature history

Feature name	Release information	Description
Support for Draft Mode in Device Template	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature allows you to save the device template configuration changes in Cisco SD-WAN Manager, and then apply these configuration changes to multiple Cisco IOS XE Catalyst SD-WAN devices later. The ability to save configuration changes simplifies generating larger device template configurations and applying them to devices.
Retrieve Last Edited Configuration	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature allows you to review the last edited configuration when a configuration push to the device fails. A copy of the last edited configuration is saved and can be retrieved to allow edits to the configuration before the next push.

Feature name	Release information	Description
Default Device Templates	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	A default device template provides basic information that you can use to bring up devices in a deployment quickly. This feature is supported on the Cisco Cloud Services Router 1000V Series, Cisco C1111-8PLTELA Integrated Services Routers, and Cisco 4331 Integrated Services Routers.
Remove Certificate SUDI requirement	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature allows you to use a subject SUDI serial number instead of a certificate serial number to add a device to a Cisco Catalyst SD-WAN overlay network.
Create a UCS-E Template	Cisco IOS XE Catalyst SD-WAN Release 16.12.1b	This feature allows you to connect a UCS-E interface with a UCS-E server through the interface feature template.

Configure devices in Cisco Catalyst SD-WAN

Describes template-based device configuration, covering types of templates, use of template variables, populating parameters through files and CSV formats, and procedures for skeleton CSV generation, file import, and manual value entry.

You can use SD-WAN Manager to create and store configurations for all devices. The SD-WAN Manager systems themselves, SD-WAN Controllers, SD-WAN Validator, and routers. When the devices start up, they contact SD-WAN Manager, which then downloads the device configuration to them. (A device starting up first contacts the SD-WAN Validator, which validates the device and sends it the IP address of SD-WAN Manager.)

The general procedure for creating configurations for all devices is the same. This section provides a high-level description of the configuration procedure and describes the prerequisite steps you must complete before creating configurations and configuring devices in the overlay network.

Types of templates

There are two types of templates:

- Feature templates
- Device templates

Feature templates

Feature templates are the building blocks of complete configuration for a device. For each feature that you can enable on a device, Cisco SD-WAN Manager provides a template form that you fill out. The form allows you to set the values for all configurable parameters for that feature.

Because device configurations vary for different device types and the different types of routers, feature templates are specific to the type of device.

Some features are mandatory for device operation, so creating templates for these features is required. Also for the same feature, you can create multiple templates for the same device type.

Special Characters in Feature Template

In releases prior to Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, if you enter **<** or **>** special characters in a SD-WAN Manager feature template definition or description, SD-WAN Manager generates a 500 exception error while attempting to preview a SD-WAN Manager feature template.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, if you enter **<** or **>** special characters in a SD-WAN Manager feature template definition or description, the special characters are converted to their HTML equivalents, **<** and **>**.

This applies to all feature templates. You no longer receive a 500 exception error when previewing a SD-WAN Manager feature template.

Device templates

Device templates contain the complete operational configuration for a device and are created by consolidating feature templates.

- Each device template is specific to a device type.
- If multiple devices of the same type share the same configuration, you can use the same template for all of them. Differences between devices are handled using configuration variables.
- If devices of the same type have different configurations, you create separate templates.

CLI-based device templates

You can create a device template by entering a CLI-style configuration directly in SD-WAN Manager by

- Uploading a text file with the configuration
- Copying and pasting configuration text
- Typing the configuration directly into SD-WAN Manager

From Cisco IOS XE Catalyst SD-WAN Release 17.5.1a and Cisco vManage Release 20.5.1, you can review your last edited configuration when your latest configuration is not being pushed to the device. For more information, see Edit a device template when a push fails.

From Cisco vManage Release 20.5.1, device variable page shows text area instead of text input field to configure CLI device template for the ease of configuration.

Template variables

Within a feature template, some configuration commands and options are identical across all device types, while others are variable, changing from device to device. Examples of variable parameters include:

- Device system IP address
- Geographic latitude and longitude
- Timezone
- Overlay network site identifier

When you attach a device template to a device, you are prompted to enter the actual values for these variables. You can provide these values in two ways:

1. Manually: Type the values for each variable for each device.
2. Bulk upload: Upload an excel file in CSV format containing the values for all devices.

Use variable values in configuration templates

In an overlay network, multiple devices of the same type might have similar configurations. This often happens with routers in different stores or branch locations that provide identical services but have unique hostnames, IP addresses, GPS locations, and site-specific properties such as BGP neighbors. It also applies to redundant controllers like Cisco SD-WAN Controllers and Cisco SD-WAN Manager systems, where each controller has its own hostname and IP address.

To simplify configuration, create a single configuration template with both static and variable values. Static values remain common across all devices, while variable values apply to individual devices. You provide the variable values when attaching a device to the configuration template.

You can configure variable values in a feature template in two ways:

- Set the parameter scope to Device Specific:

  For a parameter, select **Device Specific** to mark it as a variable. Each variable has a unique key. When you select **Device Specific**, the Enter Key box appears with a default key. You can use the default key, or you can change it by typing a new string and then moving the cursor out of the Enter Key box.

- Mark a group of parameters as optional:

  For some features in some feature configuration templates, you can mark the entire feature as optional. To mark the feature in this way, click Mark as Optional Row in a section of a feature configuration template. The variable parameters are then dimmed, and you cannot configure values for them in the feature configuration template.

Enter device-specific values for the variables when attaching the device to the configuration using one of these methods:

- From a file: When you are attaching a template to a device, you load a file to SD-WAN Manager. This is an Excel file in CSV format that lists all the variables and defines the variable's value for each device.
- Manually: When you attach a device template to a device, the SD-WAN Manager prompts you for the values for each of device-specific parameters, and you type in the value for each parameter.

Cisco Catalyst SD-WAN supports up to 500 variables in a single template push operation.

Use a file for variable parameters

To load device-specific variable values, create a template variables file in Excel CSV format. This file lists all the variables in your device configurations and defines their values. Create the file offline, and then import

it into the SD-WAN Manager server when you attach a device configuration to one or more devices in the overlay network.

We recommend creating a template variables CSV file if your overlay network includes more than a few Cisco IOS XE Catalyst SD-WAN devices.

CSV file format

File description

The CSV file is an Excel spreadsheet with one column for each variable required to configure a device. The header row lists the variable names (one variable per column), and each subsequent row represents a device and defines its variable values.

Spreadsheet options

You can create one spreadsheet for all devices in the overlay network: Cisco IOS XE Catalyst SD-WAN devices, SD-WAN Manager systems, SD-WAN Controller, and SD-WAN Validators, or create a separate spreadsheet for each device type. The system identifies the device type by its serial number.

In the spreadsheet, specify values only for the required variables for each device type and device. If a variable does not need a value, leave the corresponding cell blank.

Make the first three columns in the spreadsheet these items, and arrange them in the order shown:

Column	Column heading	Description
1	csv-deviceId	Serial number of the device (used to uniquely identify the device). For Cisco IOS XE Catalyst SD-WAN devices, you receive the serial numbers in the authorized serial number file sent to you from Cisco. For other devices, the serial number is included in the signed certificate you receive from Symantec or from your root CA.
2	csv-deviceIP	System IP address of the device (used to populate the **system ip address** command).
3	csv-host-name	Hostname of the device (used to populate the **system hostname** command).

Use unique variable keys from the Enter Key box of a feature configuration template as the headings for the remaining columns. You can arrange these columns in any order.

Generate a skeleton CSV file

To have SD-WAN Manager generate a skeleton CSV file:

You create a template variables CSV file manually using the format described in the previous section, or let SD-WAN Manager generate a skeleton CSV file containing all required columns and headings. The generated CSV file includes one row for each Cisco device type and column headings for all variables required by the feature templates in the device configuration. The column headings use the key strings that identify device-specific parameters. Then fill each row with values for the corresponding variables.

Procedure

Step 1 From the SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**, and click **Add Template**.

In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

Step 3 Create the required feature templates for one Cisco IOS XE Catalyst SD-WAN device router, one Cisco Catalyst SD-WAN Controller, one Cisco SD-WAN Manager system, and one Cisco Catalyst SD-WAN Validator.inf

In each feature template:

- For fields that have default values, verify that you want to use that value for all devices. If you do not want to use the default, change the scope to **Global** or **Device-specific**.
- For fields that apply to all devices, select the **Global** icon next to the field and set the desired global values.
- For fields that are device specific, select the **Device-specific** icon next to the field and leave the field blank.

Step 4 For each Cisco device type, create a device template.

Step 5 From the SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 6 Click **Device Templates**, and select the desired device template from the template list table.

In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

Step 7 Click **…**, and click **Export CSV**.

Step 8 Repeat Steps 7 and 8 for each device template.

Edit the exported CSV file to include at least the device serial number, system IP address, and hostname for each device in the overlay network. Then enter values for the desired device-specific variables. Ensure that variable names do not include forward slashes (/), backslashes (), or parentheses (( )).

If needed, combine multiple CSV files into a single file.

Import a CSV file

To import the CSV file containing device-specific variable values when you attach a device template to the Viptela device.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Device Templates**.

In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

Step 3 For the desired template, click **...**, and select **Attach Devices**.

Step 4 In the **Attach Devices** dialog box, select the desired devices in **Available Devices** and click the arrow to move them to **Selected Devices**.

Step 5 Click **Attach**.

Step 6 Click the Up arrow. The Upload CSV File box displays.

Step 7 Choose the CSV file to upload, and click **Upload**.

During the attachment process, click Import file to load the Excel file. If SD-WAN Manager detects duplicate system IP addresses for devices in the overlay network, it shows a warning message or pop-up. Correct the system IP addresses to remove any duplicates before continuing to attach device templates to Viptela devices.

Manually enter values for device-specific variables and for optional rows

To manually enter values for device-specific variables or for variables in optional rows when you attach the template to a device:

When you attach a device template that includes device-specific parameters, SD-WAN Manager prompts you to enter the parameter values. When you attach a device template that includes device-specific parameters, SD-WAN Manager prompts you to enter the parameter values. However, this method does not scale well for larger networks.

When many devices share the same configuration except for a few parameters, you can specify those parameters as optional rows in the feature configuration template. When you select **Optional Row**, the feature template automatically marks those parameters as device-specific and dims them so you cannot modify them in the template. You do not have to individually mark the parameters as device specific. When you attach the device template to a device, SD-WAN Manager prompts you to enter the values for those parameters.

Using optional rows to enter device-specific values is useful when a group of many Cisco IOS XE Catalyst SD-WAN devices provide identical services at their branch or site, but individual routers have their own hostname, IP address, GPS location, and other site or store properties, such as BGP neighbors.

Optional rows are available for some parameters in some feature configuration templates. To treat a parameter or set of parameters as an optional row, click the **Mark as Optional Row** box. For these types of parameters, the feature configuration template has a table listing all the configured parameters. The Optional column indicates which are optional rows

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Device Templates**, and select the desired device template.

Step 3 Click **…**, and click **Attach Devices**.

The **Attach Devices** dialog box opens.

Step 4 Choose one or more devices from **Available Devices** and move them to **Selected Devices**.

Step 5 Click **Attach**.

Step 6 In the **Chassis Number** list, select the desired device.

Step 7 Click **…**, and click **Edit Device Template**. The **Update Device Template** dialog box opens.

Step 8 Enter values for the optional parameters. When you are using optional rows, if you do not want to include the parameter for the specific device, do not specify a value.

Step 9 Click **Update**.

Step 10 Click **Next**.

If any devices have the same system IP address, a dialog box appears or an error message is displayed when you click **Next**. Modify the system IP addresses so that there are no duplicates, and click **Save**. Then click **Next** again.

You need to shut down the OMP on the device, before changing the system-ip on the device.

Step 11 In the left pane, select the device. The right pane displays the device configuration and the **Config Preview** tab in the upper right corner is selected.

Step 12 Click **Config Diff** to preview the differences between this configuration and the configuration currently running on the device, if applicable. To edit the variable values entered in the previous screen, click **Back**.

Step 13 Click **Configure Devices** to push the configuration to the devices.

The Status column displays whether the configuration was successfully pushed. Click the **right angle bracket** to the left of the row to display details of the push operation.

Configure and manage device templates

Describes the creation, management, and application of device templates.

Create a device template

A device template defines a device's complete operational configuration.

It consists of multiple feature templates, each defining the configuration for a specific Cisco Catalyst SD-WAN software feature.

- Some feature templates are mandatory (marked with an asterisk *), while others are optional.
- Each mandatory feature template and some optional ones include a factory-default template.

You can either use the factory-default template `Factory_Default_feature-name_Template` or create a custom feature template.

- Create a device template from feature templates
- Create a device template after building custom feature templates

Create a device template from feature templates

Use these steps to create a device template from feature templates.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Device Templates**.

Step 3 Click the **Create Template** drop-down and select **From Feature Template**.

Step 4 From the **Device Model** drop-down, select the device type for which you wish to create the template.

a. All feature templates for that device type appear.

b. Required templates are marked with *, and optional ones are not.

c. Factory-default templates are preselected.

Step 5 In the **Template Name** field, enter a name using letters, digits (0–9), hyphens (-), or underscores (_).

No spaces or special characters allowed.

Step 6 In the **Description** field, enter a description.

Spaces and any characters allowed

Step 7 To view a factory-default configuration, select a feature template and click **View Template**.

Click **Cancel** to return to the previous screen.

Step 8 To create a **custom template** for a feature:

a) Select the desired factory-default feature template and click **Create Template**.
b) In the **Template Name** and **Description** fields, provide details (same naming rules apply).
c) Configure each parameter as needed.
d) Click tabs or **(+)** to expand additional fields.

Step 9 When you first open a feature template, parameters with default values show a check mark under the **Default** scope. You can change the scope for each parameter:

Parameter scope	Scope description
Device Specific (indicated by a host icon)	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a device to a device template. When you click **Device Specific**, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a device to a device template. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.
Global (indicated by a globe icon)	Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

To make an entire parameter group device-specific, select **Mark as Optional Row**. These parameters are grayed out in the feature template and filled later when attaching the device.

Step 10 Click **Save** after configuring each feature template.

Step 11 Repeat steps 6 through 9 for each additional software feature you want to include.

Step 12 Click **Create**.

- The new device template appears in the Device Template table.

- The Feature Templates column shows how many feature templates it includes.
- The Type column displays Feature, indicating it was created from feature templates.

Create a device template after building custom feature templates

To create device templates after building custom feature templates.

Procedure

Step 1 Click **Feature** > **Add Template**.

Step 2 From **Select Devices**, choose the device type.

You can create a single feature template for features that are available on multiple device types. You must, however, create separate feature templates for software features that are available only on the device type you are configuring.

Step 3 Select the **feature template**.

The template form is displayed.

This form contains fields for naming the template and fields for defining the required parameters. If the feature has optional parameters, then the template form shows a plus sign (+) after the required parameters.

Step 4 In the **Template Name** field, enter a name for the device template.

This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

Step 5 In the **Description** field, enter a description for the device template.

This field is mandatory, and it can contain any characters and spaces.

Step 6 For each required parameter, choose the desired value, and if applicable, select the scope of the parameter. Select the scope from the drop-down list of each parameter's value box.

Click the plus sign (+) from the required parameters to set the values of optional parameters.

Step 7 Click **Save** .

Step 8 Repeat Steps 2 to 7 for each additional feature template you wish to create.

Step 9 Click **Device**.

Step 10 Click the **Create Template** drop-down list and select **From Feature Template**.

Step 11 From the **Device Model** drop-down list, select the type of device for which you wish to create the device template.

SD-WAN Manager displays the feature templates for the device type you selected. The required feature templates are indicated with an asterisk (*). The remaining templates are optional.

Step 12 Repeat step 4 and 5.

Step 13 To view the factory-default configuration for a feature template, select the desired feature template and click **View Template**.

Step 14 Factory default configuration.

a) Click **Cancel** to return to the **Configuration Template** screen.

The new device template is displayed in the **Device Template** table. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "Feature" to indicate that the device template was created from a collection of feature templates.

b) To modify a factory-default configuration, choose a different feature template you created from the drop-down.

Repeat this step for each factory-default feature template you wish to modify.

Step 15 Click **Create**

The new configuration template is displayed in the Device Template table.

The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "Feature" to indicate that the device template was created from a collection of feature templates.

Create a device CLI template

To create a device template by entering a CLI text-style configuration directly on the SD-WAN Manager.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** .

Step 2 Click **Device Templates**.

Step 3 Click the **Create Template** drop-down list and select **CLI Template**.

Step 4 From the **Device** Type drop-down list, select the type of device for which you wish to create the template.

Step 5 In the **Template Name** field, enter a name for the device template.

This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.

Step 6 In the **Description** field, enter a description for the device template.

This field is mandatory, and it can contain any characters and spaces.

Step 7 In the CLI Configuration box, enter the configuration either by typing it, cutting and pasting it, or uploading a file.

Step 8 To convert an actual configuration value to a variable, select the value and click **Create Variable**. Enter the variable name, and click **Create Variable**. You can also type the variable name directly, in the format {{*variable-name*}}; for example, {{hostname}}.

Step 9 Click **Add**. The new device template is displayed in the Device Template table.

The **Feature Templates** column shows the number of feature templates that are included in the device template, and the Type column shows "CLI" to indicate that the device template was created from CLI text.

Default device templates

A default device template includes the basic information needed to bring up devices in a deployment. It allows you to quickly provision devices with the minimum details required for them to operate in your network.

You cannot directly edit or update a default device template, but you can copy it and then edit the copied version.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Device Templates**.

Step 3 From the **Template Type** drop-down list, select **Default**.

A list of default device templates displays.

Step 4 Perform any of these actions:

- To attach a default device template to devices, click **...**, and select **Attach Devices**.

  In the **Attach Devices** dialog box, select the devices that you want attach, and then click **Attach**.

- To view the configuration settings for a default device template, click **...**, and choose **View**.

- To copy a default device template, click **...**, and choose **View**.

  In the **Template Copy** dialog box, enter a unique name and a description for the copy that you are creating, and then click **Copy**.

  The copied version becomes a feature template that you can edit.

- To create an Excel file in CSV format that contains device-specific settings from a device template, click **...**, and choose **Export CSV**. Use the dialog box that displays to open or save the CSV file.

  You can use this CSV file as a reference for device-specific settings when you create other device templates.

Change variable values for a device

When you create a configuration from device configuration templates that contain variables, SD-WAN Manager automatically populates those variables with actual values when you attach the templates to devices. To enable this, create an Excel file listing the variable values for each device and save it in CSV format. You can also manually enter the variable values.

After you push the configuration to a device, you can change the value assigned to any variable.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Device Templates**, and choose the desired device template.

Step 3 Click **...**, and click **Change Device Values**.

The screen displays a table of all the devices that are attached to that device template.

Step 4 For the desired device, click **...**, and click **Edit Device Template**.

Step 5 In the **Update Device Template** dialog box, enter values for the items in the variable list.

Step 6 Click **Update**.

Step 7 Click **Next**.

Step 8 Click **Configure Devices** to push the configuration to the device.

The Status column displays if the configuration was successfully pushed or not. Click the right angle bracket to display the details of the push operation.

Change the device rollback timer

By default, when you attach a configuration template to a Cisco IOS XE Catalyst SD-WAN device, the router rolls back to the previous configuration if it fails to start successfully within 5 minutes. For configurations created from the CLI, you can change the device's rollback timer.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Device Templates**, and choose a device template.

Step 3 Click **…**, and click **Change Device Values**.

The right pane displays the device's configuration, and the **Config Preview** tab is selected.

Step 4 In the left pane, click the name of a device.

Step 5 Click **Configure Device Rollback Timer**. The **Configure Device Rollback Time** pop up page is displayed.

Step 6 From the **Devices** drop-down list, select a device.

Step 7 Enable or disable the rollback timer.

- To enable the rollback timer, in the **Set Rollback slider** drag the slider to the left to enable the rollback timer. When you do this, the slider changes in color from gray to green.
- To disable the rollback timer, click **Enable Rollback slider**. When you disable the timer, the **Password** field dialog box appears.

  Enter the password that you used to log in to SD-WAN Manager.
- In the **Device Rollback Time** slider, drag the slider to the desired value. The default time is 5 minutes. You can configure a time from 6 to 15 minutes.
- To exclude a device from the rollback timer setting, click **Add Exception** and select the devices to exclude.

Step 8 The table of the **Configure Device Rollback Time** dialog box lists all the devices to which you are attaching the template and their rollback time. To delete a configured rollback time, click the **Trash** icon of the device name.

Step 9 Click **Save**.

Step 10 Click **Configure Devices** to push the configuration to the devices.

The Status column displays whether the configuration was successfully pushed. Click **(+)** to display details of the push operation.

Edit a device template when a push fails

If the configuration push to a device fails, you can review the last edited configuration to identify any issues that caused the failure.

See Retrieve last edited configuration.

Retrieve last edited configuration

Before you begin

To review your last edited configuration, a device template must be attached to a device.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **ConfigurationTemplates**.

Step 2 Click **Device Templates** and choose a device template.

Step 3 Click **...**, and choose **Edit**.

The **CLI Configuration** box displays the current running configuration on the device.

Step 4 Click **Load Last Attempted Config** to view the last edited configuration.

Step 5 Click **Config Diff** to view the differences in the current configuration versus the last edited configuration. The **Config Diff** option is available when you modify the configuration or when you click **Load Last Attempted Config**.

Step 6 Click **Config Preview**.

Load Last Attempted Config and the **Config Diff** option is available only when the configuration is not being pushed to the device.

Step 7 Click **Update**.

Step 8 Click **Configure Devices** to push the configuration to the devices.

The Status column displays whether the configuration was successfully pushed. Click > to view the details of the push operation.

Determine why a device rejects a template

To determine why the device rejected the template.

When you attach a template to a device using the screen, the device might reject the template. One reason that this may occur is because the device template contains incorrect variable values. When a device rejects a template, it reverts to the previous configuration.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **ConfigurationTemplates**.
Step 2 Click **Device Templates** and select the desired template.
Step 3 Locate the device. The **Template Status** column indicates why the device rejected the template.

Preview device configuration and view configuration differences

Use these steps for a configuration that you have created using the CLI.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
Step 2 Click **Device Templates**, and choose the desired device template.
Step 3 Click **...**, and click **Change Device Values**.

The right pane displays the device's configuration, and **Config Preview** is selected.

Step 4 Click the name of a device.
Step 5 Click **Config Diff** to view the differences between the current configuration and the one running on the device.
Step 6 Click **Back** to edit the variable values you entered on the previous screen.
Step 7 Click **Configure Devices** to push the configuration to the devices.

The Status column displays whether the configuration was successfully pushed.

Click the right angle bracket to display details of the push operation.

Export a variables-spreadsheet in CSV format for a template

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **ConfigurationTemplates**.
Step 2 Click **Device Templates** and select the desired template.
Step 3 Click **…**, and click **Export CSV**.

Edit a device template

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** .

Step 2 Click **Device Templates** or **Feature Templates** and select a template..

In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**, and **Feature Templates** is titled **Feature**.

Step 3 Click **…**, and click **Edit**.

You cannot change the name of a device or feature template when that is attached to a device.

You can edit templates simultaneously from one or more Cisco SD-WAN Manager servers. For simultaneous template edit operations, the following rules apply:

- You cannot edit the same device or feature template simultaneously.
- When you are editing a device template, all other feature templates attached to that device template are locked and you cannot perform any edit operations on them.
- When you are editing a feature template that is attached to a device template, that device template as well as all other feature templates attached to it are locked and you cannot perform any edit operations on them.

Delete a template

Deleting a template does not remove the associated configuration from devices.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** .

Step 2 Click **Device Templates** or **Feature Templates** and select a template..

In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**, and **Feature Templates** is titled **Feature**.

Step 3 Click **…**, and click **Delete**.

Step 4 To confirm the deletion of the template, click **OK**.

Copy a template

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** .

Step 2 Click **Device Templates** or **Feature Templates** and select a template..

In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**, and **Feature Templates** is titled **Feature**.

Step 3 Click **…**, and click **Copy**.

Step 4 Enter a new template name and description.

Step 5 Click **Copy**.

Edit a CLI device template

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** .

Step 2 Click **Device Templates** and select a template..

In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**, and **Feature Templates** is titled **Feature**.

Step 3 Click **…**, and click **Edit**.

Step 4 Under **Device CLI Template**, edit the template.

Step 5 Click **Update**.

View a template

Use these steps to view a template.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Device Templates** or **Feature Templates**, and select a template you wish to view.

In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**, and **Feature Templates** is titled **Feature**.

Step 3 Click **…**, and then click **View**.

View device templates attached to a feature template

Use these steps to view a template device templates attached to a feature template.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**, and select a template you wish to view.

In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

Step 3 Click **…**, and click **Show Attached Device Templates**.

Step 4 **Device Templates** dailog box opens, displaying the names of the device templates to which the feature template is attached.

View devices attached to a device template

Procedure

Step 1 For a device template that you created from feature templates:

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

b) Click **Device Templates**, and select a template you wish to view.

In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

c) Click **Device Templates**, and select a template you wish to view.

In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

d) Click **…**, and click **Attach Devices**.

e) From **Attach Devices**, click **Attached Devices**.

Step 2 For a device template that you created from a CLI template:

a) From the Cisco SD-WAN Manager, choose **Configuration** > **Templates**.

b) Click **Device Templates**, and select a template you wish to view.

c) Click **…**, and then click **Show Attached Devices**.

Attach templates to devices

Attach and detach a device template

To configure a device on the network, attach a device template to it. You can attach only one device template to each device, and the template, whether created by consolidating individual feature templates or by entering a CLI text-style configuration, must include the complete configuration for that device. You cannot mix and match feature templates with CLI-style configurations.

You need to recreate the feature templates, as the templates created prior to Cisco vManage Release 20.5.1 fail when attached to the device.

Parallel operations

On Cisco IOS XE Catalyst SD-WAN devices in the overlay network, you can perform the same operations in parallel from one or more SD-WAN Manager servers.

You can perform the following template operations in parallel:

- Attach device templates to devices
- Detach device templates from devices
- Change variable values for device templates that have devices attached to them

Configuration deployment behavior

If the device being configured is present and operational on the network, the configuration is sent to the device immediately and takes effect immediately.

If the device has not yet joined the network, the pushing of the configuration to the device is scheduled. When the device joins the network, SD-WAN Manager pushes the configuration immediately after it learns that the device is present in the network.

Rules for template operations

The rules below apply for template operations:

- When a device template is already attached to a device, you can modify one of its feature templates.
- When you click **Update** > **Configure Devices**, all other template operations, including attach devices, detach devices, and edit device values, are locked on all SD-WAN Manager servers until the update operation completes.
- This means that a user on another SD-WAN Manager server cannot perform any template operations until the update completes.
- You can perform the attach and detach device template operations on different devices, from one or more SD-WAN Manager servers, at the same time.
- However, if any one of these operations is in progress on one SD-WAN Manager server, you cannot edit any feature templates on any of the servers until the attach or detach operation completes.

Attach a device template to devices

Use these steps to attach a device template to one or more devices.

You can attach the same templates to multiple devices, and you can do so simultaneously, in a single operation.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Device Templates** and select the desired template.

Step 3 Click **…**, and click **Attach Devices**.

The **Attach Devices** dialog box opens with the **Select Devices** tab.

Step 4 Select devices.

a) In the **Available Devices** column on the left, select a group and search for one or more devices, select a device from the list, or click **Select All**.
b) Click the arrow pointing right to move the device to the **Selected Devices** column on the right.
c) Click **Attach**.

Step 5 Enter variable values.

If the template contains variables, enter the missing values for each device:

- Manually: Enter values in the table or click **…** and **Edit Device Template**.

  When using optional rows, leave a parameter blank if not required.

- Import File: Click **Import File** to upload a CSV file listing all variables and their values.

- Click **Update**, then **Next**.

  If any devices have the same system IP address, a dialog box appears or an error message is displayed when you click **Next**. Modify the system IP addresses so that there are no duplicates, and click **Save**. Then click **Next** again.

Step 6 Preview configuration.

a) In the left pane, select a device to preview its configuration.

   The right pane displays the **Config Preview** tab.

b) To view differences with the running configuration, click the **Config Diff** tab.
c) Click **Back** to edit variables if needed.

Step 7 Click **Configure Device Rollback Timer**.

The **Configure Device Rollback Time** dialog box appears.

a) Select a device from the **Devices** drop-down list.
b) Enable timer: Drag the Set Rollback slider left (gray → green).
c) Disable timer: Click the slider; enter your Cisco SD-WAN Manager password when prompted.
d) Set interval: Drag the Device Rollback Time slider to choose a time (default 5 minutes; range 6–15 minutes).
e) Add Exception: Click **Add Exception** to exclude devices.
f) The bottom table lists devices and their rollback times. Click the Trash icon to delete an entry.
g) Click **Save**.

Step 8 Click **Configure Devices** to push the configuration to all selected devices.

The Status column shows whether the configuration was successfully pushed. Click the right angle bracket (>) to view detailed push operation results.

Configuration prerequisites

General prerequisites

- Before configuring any device in the network, ensure that the device is validated and authenticated so that SD-WAN Manager, Cisco SD-WAN Controllers, and SD-WAN Validators recognize it as authorized in the overlay network.
- A signed certificate must be installed on SD-WAN Manager, Cisco SD-WAN Controllers, and SD-WAN Validators to validate and authenticate them in the overlay network.
- Obtain an authorized serial number file from Cisco, which lists the serial and chassis numbers for all routers permitted in your network. Upload this serial number file to SD-WAN Manager to validate and authenticate the routers.

Variables spreadsheet

Feature templates often include variables. To ensure SD-WAN Manager populates these variables with actual values when attaching a device template to a device, create an Excel spreadsheet containing the variable values for each device, and save it in CSV format.

In the spreadsheet, the header row contains the variable name and each row after that corresponds to a device, defining the values of the variables. The first three columns in the spreadsheet must be the following, in this order:

- csv-deviceId—Serial number of the device (used to uniquely identify the device). For routers, you receive the serial numbers in the authorized serial number file sent to you from Cisco. For other devices, the serial number is included in the signed certificate you receive from Symantec or from your root CA.
- csv-deviceIP—System IP address of the device (used to populate the **system ip address** command).
- csv-host-name—Hostname of the device (used to populate the **system hostname** command).

You can create a single spreadsheet for all devices in the overlay network—Cisco Catalyst SD-WAN Controllers, SD-WAN Validators, and routers. You do not need to specify values for all variables for all devices.SD-WAN Validator

Device configuration workflow

Devices in the overlay network that are managed by SD-WAN Manager must be configured from SD-WAN Manager.

Procedure

Step 1 Create feature templates.

a) From the SD-WAN Manager menu, choose **Configuration** > **Templates**.

b) Click **Feature Templates**, and click **Add Templates**.

In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

Step 2 Create device templates.

a) From the SD-WAN Manager menu, choose **Configuration** > **Templates**.
b) Click **Device Templates**, and click **Create Templates**.

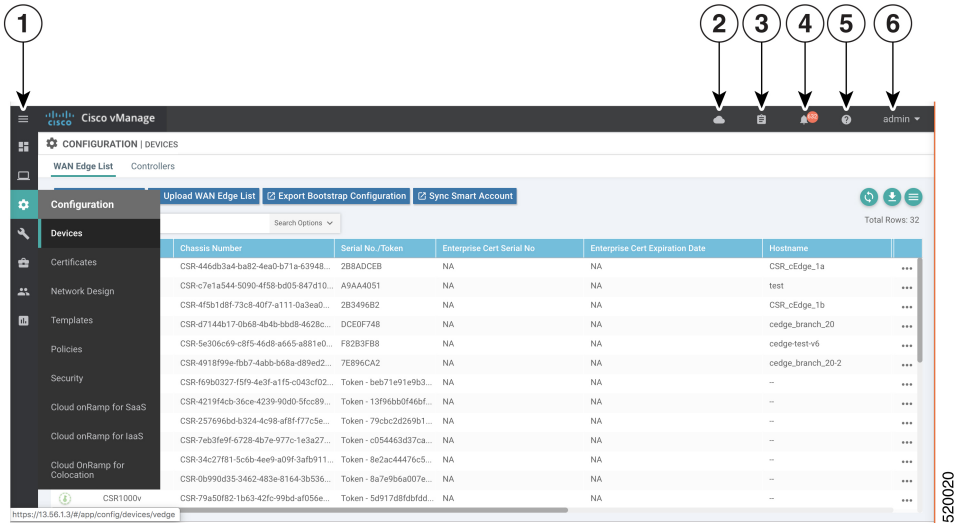
In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

Step 3 Attach device templates to individual devices.

a) From the SD-WAN Manager menu, choose **Configuration** > **Templates**.
b) Click **Device Templates**, and choose a template.
c) Click **…**, and select **Attach Devices**.

Configure and manage devices using SD-WAN Manager

Use the **Devices** screen to add and delete devices, toggle the mode of a device between CLI and SD-WAN Manager, upload the WAN edge serial number file, export bootstrap configuration and, and perform other device-related tasks.



1	Menu
2	CloudExpress
3	Tasks
4	Alarms
5	Help
6	User Profile

Change configuration modes

A device can be in either of these configuration modes:

- Cisco SD-WAN Manager mode–A template is attached to the device and you cannot change the configuration on the device by using the CLI.
- CLI mode – No template is attached to the device and the device can be configured locally by using the CLI.

When you attach a template to a device from Cisco SD-WAN Manager, it puts the device in Cisco SD-WAN Manager mode. You can change the device back to CLI mode if needed to make local changes to its configuration.

Procedure

Step 1 Follow these steps to toggle a router from Cisco SD-WAN Manager mode to CLI mode.

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
b) Click **WAN Edge List**, and select a device.
c) Click the **Change Mode** drop-down list and select **CLI mode**.

- The **Config Lock** (Provision Device) option appears only if a template is attached to the device or if a configuration group is deployed to the device.
- Starting from Cisco IOS XE SD-WAN Release 17.11.1a, click the **...** icon adjacent to the device that you want to change fromCisco SD-WAN Manager mode to the CLI mode and click **Config Lock** (Provision Device).

Step 2 Follow these steps to toggle a controller device from Cisco SD-WAN Manager mode to CLI mode:

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
b) Click **Controllers**, and select a device.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

c) Click the **Change Mode** drop-down list.
d) Select **CLI mode** and then select the device type. The **Change Mode - CLI** window opens.
e) From the **Manager mode** pane, select the device and click the right arrow to move the device to the **CLI mode** pane.
f) Click **Update to CLI Mode**.

An SSH window opens. To log in to the device, enter a username and password. You can then issue CLI commands to configure or monitor the device.

Upload WAN edge router authorized serial number file

To upload the WAN edge router authorized serial number file to SD-WAN Manager and then download it to controllers in the network

- The WAN eEdge router authorized serial number file contains, as applicable, the subject SUDI serial number, the chassis number, and the certificate serial numbers of all valid Cisco IOS XE Catalyst SD-WAN devices in the overlay network.
- You retrieve a serial number file from the Cisco Plug-and-Play (PnP) portal and upload it to SD-WAN Manager. (For more information about Cisco PnP, see Cisco Plug and Play Support Guide for Cisco Catalyst SD-WAN Products.)
- From SD-WAN Manager, you send the file to the controllers in the network. This file is required to allow the Cisco Catalyst SD-WAN overlay network components to validate and authenticate each other and to allow the overlay network to become operational.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.

Step 2 Click **WAN Edge List**, and click **Upload WAN Edge List**.

The Quick Connect workflow opens, enabling you to upload the serial number file. Refer information about the Quick Connect workflow in the *Cisco Catalyst SD-WAN Getting Started Guide*.

Step 3 (This step applies only for releases earlier than Cisco Catalyst SD-WAN Manager Release 20.14.1) Under the **Upload WAN Edge List** screen:

a) Click **Choose File** and select the WAN edge router authorized serial number file you received from Cisco PnP.

b) To automatically validate the routers and send their chassis and serial numbers to the controllers, ensure that the **Validate the uploaded vEdge List and send to controllers** check box is selected. If you do not select this option, you must individually validate each router in **Configuration** > **Certificates** > WAN Edge List.

a) Click **Upload**.

A list of routers in the network is displayed in the router table, with details about each router.

What to do next

Starting from Cisco vManage Release 20.9.2, you can monitor the newly added WAN Edge devices in the **Monitor** > **Devices** page.

Upload WAN edge router serial numbers from Cisco Smart Account

To upload the WAN edge router authorized serial numbers from a Cisco Smart account to SD-WAN Manager and then download it to all the controllers in the overlay network:

- To allow Cisco Catalyst SD-WAN overlay network components to validate and authenticate each other and to allow the overlay network to become operational, Cisco Catalyst SD-WAN requires chassis numbers of all valid Cisco IOS XE Catalyst SD-WAN devices in the overlay network.

  In addition, certificate serial numbers, subject SUDI serial numbers, or both numbers are required for all devices.

Procedure

Step 1 From the SD-WAN Manager menu, choose **Configuration** > **Devices**.

Step 2 Click **WAN Edge List**, and click **Sync Smart Account**.

Step 3 In the **Sync Smart Account** window:s

a) Enter the **Username** and **Password** for your Smart account.

b) To automatically validate the routers and send their chassis and serial numbers to the controllers, check the **Validate the Uploaded WAN Edge List and Send to Controllers** check box. If you do not select this option, you must individually validate each router in **Configuration** > **Certificates** > **WAN Edge List** .

c) Click **Sync**

A list of routers in the network is displayed in the router table, with details about each router.

Starting from Cisco vManage Release 20.9.2, you can monitor the newly added WAN Edge devices in the **Monitor** > **Devices** page.

Export device data in CSV format

In an overlay network, you might deploy multiple devices of the same type that share identical or nearly identical configurations.

- Example 1: In a network with redundant SD-WAN Controllers, you must configure each controller with identical policies.
- Example 2: In a network with Cisco IOS XE Catalyst SD-WAN devices at multiple sites, each device provides identical services at each site.

Using templates for identical configurations

As these devices have essentially identical configurations:

- You can create one set of feature templates.
- You can consolidate them into one device template.
- You can use this single device template to configure all devices.

To assign unique values per device, you can:

- Create an Excel file in CSV format.
- List all the variables.
- Define each device-specific variable value for every device.
- Load this file when you attach the device template to the devices.

How to export data in CSV format

The Export icon lets you create and download device data in a CSV file. This icon, which is a downward-pointing arrow, is located to the right of the filter criteria both in the WAN Edge List and in the Controllers tab.

SD-WAN Manager downloads all data from the device table to an Excel file in CSV format.

View a device's running configuration

Running configuration is configuration information that SD-WAN Manager obtains from the memory of a device. This information can be useful for troubleshooting.

Use these steps to view a device's running configuration:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.

Step 2 Click **WAN Edge List** or **Controllers**, and select the device.

Step 3 Click **…**, and click **Running Configuration**.

View a device's local configuration

Local configuration refers to the configuration that the SD-WAN Manager stores for a device.This information helps troubleshoot issues or determine how to access a device when it is not reachable from SD-WAN Manager.

To view a device's local configuration created using Configuration ► Templates:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.

Step 2 Click **WAN Edge List** or **Controllers**, and select the device.

Step 3 Click **...**, and click **Local Configuration**.

Copy router configuration

Copy the configuration from the old router to the new router.

When you are replacing one router at a site with another router, you copy the old router's configuration to the new router. Then you remove the old router from the network and add the new one.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.

Step 2 Mark the new Cisco IOS XE Catalyst SD-WAN device as invalid.

Step 3 From the Cisco SD-WAN Manager, choose **Configuration** > **Devices**.

Step 4 Under **WAN Edge List,** select the old router.

Step 5 Click **…**, and click **Copy Configuration**.

Step 6 In the **Copy Configuration** window, select the new router.

Step 7 To confirm the copy of the configuration, click **Update**.

After you have copied the configuration to the new router, you can add the new router to the network. First, delete the old router from the network, as described below. Then add the new router to the network:

Step 8 From the Cisco SD-WAN Manager, choose **Configuration** > **Certificates**.

Mark the new router as valid.

Step 9 Click **Send to Controller**.

Delete a WAN edge router

Delete a router to remove it from your deployment. This action also removes the following items associated with the router from the WAN Edge router serial number list:

- Chassis number
- Certificate serial number
- Subject SUDI serial number

Deleting a router also permanently removes the router configuration from SD-WAN Manager.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, **Configuration** > **Certificates**.

Step 2 Mark the WAN Edge router as invalid.

Step 3 From the SD-WAN Manager menu, choose **Configuration** > **Devices**.

Step 4 Click **WAN Edge List,** and select the router.

Step 5 Click **...**, and click **Delete WAN Edge**.

Step 6 To confirm deletion of the device, click **OK**.

Step 7 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.

Step 8 Click **Send to Controller.**

Decommission a cloud router

Decommissioning a cloud router (such as a C8000v) removes the device's serial number from SD-WAN Manager and generates a new token for the device.

- The Decommission WAN Edge feature applies only to cloud WAN edge devices and retains the cloud WAN Edge's UUID generated on the PnP Portal.
- Physical devices do not support the Decommission WAN Edge functionality.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.

Step 2 Click **WAN Edge List**, and select a cloud router.

Step 3 Click **…**, and click **Decommission WAN Edge**.

Step 4 To confirm the decommissioning of the router, click **OK**.

Note
From Cisco Catalyst SD-WAN Manager Release 20.15.1, the process to decommision a WAN edge router has been modified. The scenarios below highlight the updates.

Table 31: Updates to deleting a WAN edge router

Scenario	Action
Decommision a compromised device	Click **Delete WAN Edge**
Device is reachable	Perform a mandatory **configuration unlock** before proceeding with the decommissioning process.
Device is unreachable	The device will be unlocked after certain time when the device is unreachable. If you no longer have the device onboarded, with no Cisco SD-WAN Manager visibility, you can hold the power button for 5–10 seconds for a config reset, or 10-20 seconds for a software reset. If you have console/terminal access, you can run the **request config reset** command. Reuse of UUID is only possible after decommissioning a device. In this case, the **Decommission** option is not available since the device is offline.

View log of template activities

The template activity log records details about creating, editing, and deleting configuration templates, as well as the status of attaching templates to devices. This information helps in troubleshooting.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.

Step 2 Click **WAN Edge List** or **Controllers**, and select the device.

Step 3 Click **…**, and click **Template Log**.

View status of device bring up

You can view the status of operations that bring a router or controller online in the overlay network. This helps you monitor and track their progress effectively.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.

Step 2 Click **WAN Edge List** or **Controllers**, and select the device.

Step 3 Click **…**, and click **Device Bring Up**.

Add a Cisco SD-WAN Validator

A Cisco SD-WAN Validator automatically orchestrates connectivity between Cisco IOS XE Catalyst SD-WAN devices and Cisco SD-WAN Manager. If any Cisco IOS XE Catalyst SD-WAN device or SD-WAN Controller is behind a NAT, the SD-WAN Validator also serves as an initial NAT-traversal orchestrator.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.

Step 2 Click **Controllers**.

Step 3 Click **Add Validator**.

Step 4 In the **Add Validator** window:

a) Enter **Validator Management IP Address** of the SD-WAN Validator.

b) Enter the **Username** and **Password** to access the SD-WAN Validator.

c) To allow the certificate-generation process to occur automatically, check the **Generate CSR** check box.

d) Click **Add**.

Step 5 Repeat Steps 2, 3 and 4 to add additional SD-WAN Validators.

The new SD-WAN Validator is added to the list of controllers in the Controllers screen.

Configure Cisco SD-WAN Controllers

Add an SD-WAN Controller

After the SD-WAN Validator authenticates Cisco IOS XE Catalyst SD-WAN devices, the SD-WAN Validator provides Cisco IOS XE Catalyst SD-WAN device information that they need to connect to the SD-WAN Controller. A SD-WAN Controller controls the flow of data traffic throughout the network via data and app-route policies.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.

Step 2 Click **Controllers**.

Step 3 Click **Add Controller**.

Step 4 In the **Add Controller** window:

a) Enter the system IP address of the Cisco Catalyst SD-WAN Controller.
b) Enter the **username** and **password** to access the SD-WAN Controller.
c) Select the protocol to use for control-plane connections. The default is DTLS. The DTLS (Datagram Transport Layer Security) protocol is designed to provide security for UDP communications.
d) If you select TLS, enter the port number to use for TLS connections. The default is 23456.
e) The TLS (Transport Socket Layer) protocol that provides communications security over a network.
f) Check the **Generate CSR** check box to allow the certificate-generation process to occur automatically.
g) Click **Add**.

Step 5 Repeat Steps 2, 3 and 4 to add additional SD-WAN Controllers. Cisco SD-WAN Manager can support up to 20 SD-WAN Controllers in the network.

The new SD-WAN Controller is added to the list of controllers in the Controllers screen.

Edit SD-WAN Controller details

You can edit controller details to update the controller's IP address and login credentials.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.

Step 2 Click **Controllers**, and select the controller.

Step 3 Click **…**, and click **Edit**.

Step 4 In the **Edit** window, edit the IP address and the login credentials.

Step 5 Click **Save**.

Delete an SD-WAN Controller

Deleting a controller removes it from the overlay. Delete the controller when you replace it or no longer need it in your network.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.

Step 2 Click **Controllers**, and select the controller.

Step 3 Click **…**, and click **Invalidate**.

Step 4 To confirm the removal of the device and all its control connections, click **OK**.

Configure reverse proxy on SD-WAN Controllers

To configure reverse proxy on an individual SD-WAN Manager and SD-WAN Controller:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.

Step 2 Click **Controllers**, and select the controller.

Step 3 Click **…**, and click **Add Reverse Proxy**.

The **Add Reverse Proxy** dialog box is displayed.

Step 4 Configure the private IP address and port number for the device.

The private IP address is the IP address of the transport interface in VPN 0. The default port number is 12346. This is the port used to establish the connections that handle control and traffic in the overlay network.

Step 5 Configure the proxy IP address and port number for the device, to create the mapping between the private and public IP addresses and port numbers.

Step 6 If the SD-WAN Manager NMS or SD-WAN Controller has multiple cores, repeat Steps 5 and 6 for each core.

Step 7 Click **Add**.

To enable reverse proxy in the overlay network, from the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Proxy** > **Reverse Proxy**. Now enable **Reverse Proxy** and click **Save**.

Configure UCSE using a configuration group

Use these steps to configure UCSE using a configuration group.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure a UCSE feature in Other profile.

a) Configure parameter scope.

Table 32: Parameter

Parameter Scope	Scope Description
Global (Indicated by a globe icon)	Enter a value for the parameter and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.
Device Specific (Indicated by a host icon)	Use a device-specific value for the parameter. Choose **Device Specific** to provide a value for the key in the **Enter Key** field. The key is a unique string that helps identify the parameter. To change the default key, type a new string in the **Enter Key** field. Examples of device-specific parameters are system IP address, host name, GPS location, and site ID.
Default (indicated by a check mark)	The default value is shown for parameters that have a default setting.

b) Configure options for the UCSE feature.

Table 33: Settings

Field	Description
Type	Choose a feature from the drop-down list.
Feature Name*	Enter a name for the feature. The name can be up to 128 characters and can contain only alphanumeric characters.
Description	Enter a description of the feature. The description can be up to 2048 characters and can contain only alphanumeric characters.

c) Configure basic settings.

Table 34: Basic Configuration

Field	Description
Bay*	Specify the number for the SAS drive bays. The input value must be an integer.
Slot*	Specify the slot numbers for the mezzanine adapters. The input value must be an integer.

d) Configure IMC.

Table 35: IMC

Field	Description
Access Port	Configure the interface as an access port. You can configure only one VLAN on an access port, and the port can carry traffic for only one VLAN. Not all hardware models have a dedicated access port. See the release notes for your Cisco Catalyst SD-WAN release for the supported hardware. Available options: • **Dedicated** • **Shared** Configure the appropriate port (GE or TE) based on the hardware module.
IPv4 Address*	Provide the UCS-E management port address.
Default Gateway*	Gateway tracking determine, for static routes, whether the next hop is reachable before adding that route to the device's route table. Default: Enabled.
VLAN ID	Provide the VLAN number, which can be a value from 1 through 4094.
Assign Priority	Assign the priority.

e) Configure advanced settings.

Table 36: Advanced Configuration

Field	Description
Interface Name*	Specify the name of the interface.
Layer	Specify the layer details necessary for traffic exchange between different VLANs.
UCSE Interface VPN	Specify the details of the UCS-E interface VPN.
IPv4 Address	Provide the UCS-E management port address.

What to do next

Refer to Deploy a configuration group in the *Cisco Catalyst SD-WAN Configuration Groups Reference Guide*.

Create a UCS-E Template

For more information about the Cisco Unified Computing System (UCS) E-Series Servers, see the Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine Hardware Installation Guide.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** .

Step 2 Click **Feature Templates**.

In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

Step 3 Click **Add Template**.

Step 4 Select a Cisco IOS XE Catalyst SD-WAN device from the list.

Step 5 From the **Other Templates** section, click **UCSE**.

The UCSE Feature template opens. The top of the form contains fields for naming the template, and the bottom contains fields for configuring the Integrated Management Controller (IMC).

Step 6 In the **Template Name** field, enter a name for the template.

The name can be up to 128 characters and can contain only alphanumeric characters.

Step 7 In the **Description** field, enter a description of the template.

The description can be up to 2048 characters and can contain only alphanumeric characters.

Step 8 Configure bay and slot for template

Click the Basic Configuration tab to configure the bay and the slot for the template.

Parameter name	Description
Bay	Specify the number for the SAS drive bays.
Slot	Specify the slot numbers for the mezzanine adapters

Step 9 Configure IMC.

Click the **IMC** tab to configure the IMC parameters for the template.

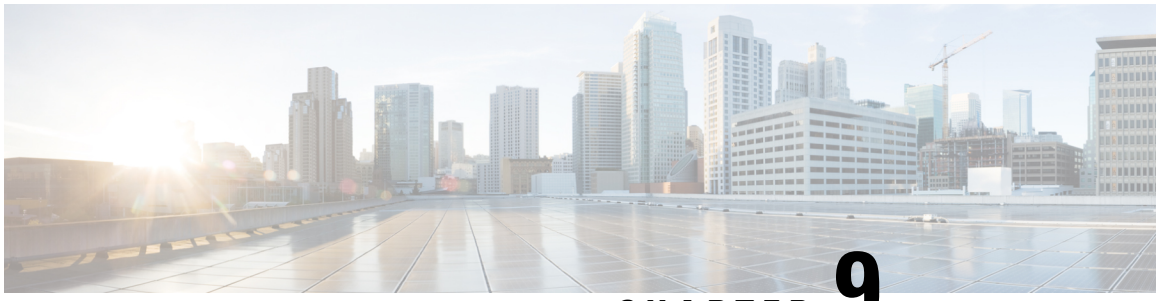
Parameter name	Description

Access port	Configure the interface as an access port. You can configure only one VLAN on an access port, and the port can carry traffic for only one VLAN.
	Not all hardware models have a dedicated access port. See the Release Notes for your Cisco Catalyst SD-WAN release for the supported hardware.
	Available options:
	• Dedicated
	• Shared
	The type of port, GE or TE, depends on the hardware model.
	For example:
	`Router(config-ucse)# imc access-port shared-lom ?`
	`GE1 GE1`
	`TE2 TE2`
	`TE3 TE3`
	`console Console`
	`failover Failover`
	Some hardware models have GE ports whereas some have TE ports.
	Depending on the hardware module, the appropriate port (GE or TE) needs to be configured. Otherwise you will get an error.
	• You can obtain the UCS-E module hardware model type by using the following commands:
	show inventory
	show platform
	• Failover - sub-option under Shared.
	For example:
	`Router(config)#ucse subslot 1/0`
	`Router(config-ucse)#imc access-port ?`
	`MGMT MGMT Interface`
	`shared-lom Shared LOMRouter(config-ucse)#imc access-port shared-lom ?`
	`GE1 GE1`
	`TE2 TE2`
	`TE3 TE3`
	`console Console`
	`failover Failover`

IPv4 address	Provide the UCS-E management port address.
Default gateway	Gateway tracking determine, for static routes, whether the next hop is reachable before adding that route to the device's route table. Default: Enabled.
VLAN ID	Provide the VLAN number, which can be a value from 1 through 4094.

Parameter name	Description
Assign priority	Assign the priority.

Parameter scope	Scope description
Global (indicated by a globe icon)	Enter a value for the parameter and apply that value to all devices.
Device specific (indicated by a host icon)	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Cisco Catalyst SD-WAN device to a device template. When you click **Device Specific**, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Cisco Catalyst SD-WAN device to a device template. To change the default key, type a new string and move the cursor out of the Enter Key box.
Default	When Default is selected, this field is not enabled.



CHAPTER 9

Basic Settings for Cisco SD-WAN Manager

- Basic system settings, on page 185
- Enforce a software version on devices, on page 192
- Configuring a login page banner, on page 193
- Configuring device basic settings, on page 195
- Configuring global system settings, on page 202
- Configuring NTP servers, on page 209
- Configuring a router as an NTP primary, on page 214
- Configure device time using CLI commands, on page 216
- Configuring GPS, on page 217
- Configuring automatic bandwidth detection, on page 219
- Proxy server for SD-WAN Manager HTTP and HTTPS traffic with external servers, on page 222
- Rate limit for bulk API requests, on page 224
- Configure device statistics collection, on page 226
- Configure the time interval for collecting device statistics, on page 226
- Configure the SD-WAN Manager server maintenance window, on page 227
- Configure system logging using CLI commands, on page 228
- Connect to a device by SSH terminal, on page 228
- View the rate limit for bulk API requests, on page 229
- Monitor NAT DIA endpoint trackers, on page 229

Basic system settings

Basic system settings are a set of parameters that enable the Cisco Catalyst SD-WAN fabric to function. They include

- device properties such as name and IP address
- network time configuration
- user access to devices
- system logging, and
- network interface parameters.

Device and SD-WAN Control Component properties

Device and SD-WAN Control Component properties, together called host properties, are the parameters that Cisco Catalyst SD-WAN uses to construct a view of the network topology. They include:

- Device system IP address:

  This provides a fixed location of the device in the overlay network. This address is independent of any of the interfaces and interface IP addresses on the device. The system IP address is one of the four components of the Transport Location (TLOC) property of each device.

- IP address of the SD-WAN Validator for the network domain, or a domain name system (DNS) name that resolves to one or more IP addresses for SD-WAN Validator:

  An SD-WAN Validator automatically orchestrates the process of bringing up the overlay network, admitting a new device into the overlay, and providing the introductions that allow the device and SD-WAN Controllers to locate each other.

- Domain identifier and the site identifier:

  These system-wide host properties are required on all devices, except for the SD-WAN Validators, to allow the Cisco Catalyst SD-WAN software to construct a view of the topology

Configure the host properties. Refer to the information about the overlay network bring-up process in the *Cisco Catalyst SD-WAN Getting Started Guide*.

Time and NTP

Network Time Protocol (NTP), is a networking protocol for synchronizing the clocks of devices throughout a network. It ensures that the time on all participating components of the network is accurate and synchronized.

Cisco Catalyst SD-WAN implements NTP to synchronize and coordinate time distribution across the fabric. NTP uses a intersection algorithm to select the applicable time servers and avoid issues caused due to network latency. The servers can also redistribute reference time using local routing algorithms and time daemons. NTP is defined in Network Time Protocol Version 4: Protocol and Algorithms Specification, RFC 5905.

User authentication and access with AAA, RADIUS, and TACACS+

Authentication, authorization, and accounting (AAA) is a framework for controlling access to resources. It includes:

- Authentication: Verifying the identity of a user or device seeking access.
- Authorization: Authorizing access to the resources a user is permitted to use, based on predefined policies and privileges.
- Accounting: Tracking and logging user activities within the network.

In Cisco Catalyst SD-WAN, AAA, in combination with RADIUS and Terminal Access Controller Access-Control System (TACACS+) user authentication, controls which users are allowed access to devices, and what operations they are authorized to perform after they are logged in or connected to the devices.

The Cisco Catalyst SD-WAN implementation of AAA includes:

- Authentication: Users log in with a username and a password. A local device can authenticate users or authentication can be performed by a remote device, either a RADIUS server or a TACACS+ server, or both in a sequence.
- Authorization: Authorization is implemented using role-based access. Access is based on groups that are configured on the devices. A user can be a member of one or more groups. User-defined groups are considered when performing authorization, that is, the Cisco Catalyst SD-WAN software uses group names received from RADIUS or TACACS+ servers to check the authorization level of a user. Each group is assigned privileges that authorize the group members to perform specific functions on the corresponding device. These privileges correspond to specific hierarchies of the configuration commands and the corresponding hierarchies of operational commands that members of the group are allowed to view or modify.
- Accounting: From Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, accounting generates a record of commands that a user executes on a device. Accounting is performed by a TACACS+ server.

Authentication for WANs and WLANs

Wide area networks (WAN) and wireless local area networks (WLAN) are two types of networks primarily differentiated by geographical reach and connectivity methods.

- Geographical reach: Extensive for WAN; limited for WLAN, such as a single building.
- Connectivity: Combination of wired and wireless technologies for WAN; wireless for WLAN.

Authentication methods differ for WAN and WLAN.

Authentication for wired networks

For wired networks (WANs), Cisco Catalyst SD-WAN devices can run IEEE 802.1X software to prevent unauthorized network devices from gaining access to the WAN. IEEE 802.1X is a port-based network access control (PNAC) protocol that uses a client–server mechanism to provide authentication for devices wishing to connect to the network.

IEEE 802.1X authentication requires three components:

- Requester: Client device, such as a laptop, that requests access to the Wide-Area Network (WAN). In the Cisco Catalyst SD-WAN overlay network, a supplicant is any service-side device that is running 802.1X-compliant software. These devices send network access requests to the router.
- Authenticator: A network device that provides a barrier to the WAN. In the overlay network, you can configure an interface device to act as an 802.1X authenticator. The device supports both controlled and uncontrolled ports. For controlled ports, the Cisco Catalyst SD-WAN device acts as an 802.1X port access entity (PAE), allowing authorized network traffic and preventing unauthorized network traffic ingressing to and egressing from the controlled port. For uncontrolled ports, Cisco Catalyst SD-WAN, acting as an 802.1X PAE, transmits and receives Extensible Authentication Protocol over IEEE 802 (EAP over LAN, or EAPOL) frames.
- Authentication server: Host that is running authentication software that validates and authenticates requesters that want to connect to the WAN. In the overlay network, this host is an external RADIUS server. This RADIUS server authenticates each client connected to the 802.1X port interface Cisco Catalyst SD-WAN device and assigns the interface to a virtual LAN (VLAN) before the client is allowed to access any of the services offered by the router or by the LAN.

Authentication for wireless networks

For wireless LANs (WLANs), routers can run IEEE 802.11i to prevent unauthorized network devices from gaining access to the WLANs. IEEE 802.11i implements Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) to provide authentication and encryption for devices that want to connect to a WLAN. WPA authenticates individual users on the WLAN using a username and a password. WPA uses the Temporal Key Integrity Protocol (TKIP), which is based on the RC4 cipher. WPA2 implements the NIST FIPS 140-2–compliant AES encryption algorithm along with IEEE 802.1X-based authentication, to enhance user access security over WPA. WPA2 uses the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP), which is based on the AES cipher. Authentication is done by either using preshared keys or through RADIUS authentication.

Network segmentation

Network segmentation is the division of a network into smaller, isolated logical segments.

Segmentation is a fundamental part of enhancing security, improving network performance, and simplifying manageability. The core idea is to restrict communication between different parts of the network.

The Layer 3 network segmentation in Cisco Catalyst SD-WAN is achieved through VRFs on devices. When you configure the network segmentation on a device using SD-WAN Manager, the system automatically maps the VPN configurations to VRF configurations.

Network interface properties

A network interface is the component that enables a device in a network to connect to other devices, to send and receive data. There are numerous interface properties relevant to a Cisco Catalyst SD-WAN fabric.

VPN

In the SD-WAN fabric, interfaces are associated with VPNs that translate to VRFs. The interfaces that participate in a VPN are configured and enabled in that VPN. Each interface can be present only in a single VPN.

Devices use VRFs in place of VPNs. When you configure a device in SD-WAN Manager, the system automatically maps the VPN configurations to VRF configurations.

The fabric has these types of VPNs and VRFs:

- VPN 0: Transport VPN:

  Carries control traffic using the configured WAN transport interfaces. Initially, VPN 0 contains all the interfaces on a device except for the management interface, and all the interfaces are disabled. This is the global VRF in Cisco IOS XE Catalyst SD-WAN software.

- VPN 512: Management VPN:

  Carries out-of-band network management traffic among the devices in the fabric. The interface used for management traffic is in VPN 512.

  - On devices, VPN 512 is configured by default and enabled. On devices, the management VPN is converted to VRF Mgmt-Intf.
  - On SD-WAN Control Components, VPN 512 is not configured by default.

Other properties

For each network interface, you can configure a number of interface-specific properties, such as

- DHCP clients and servers
- VRRP
- interface MTU and speed, and
- Point-to-Point Protocol over Ethernet (PPPoE).

Note If the network path only supports an MTU smaller than 1500 bytes and Path MTU discovery is enabled, ICMP responses blocked by the firewall may prevent SD-WAN Manager from dynamically adjusting the MTU. In such cases, either configure the SD-WAN Manager interface MTU to match the network MTU or ensure ICMP traffic is allowed through the firewall.

At a high level, for an interface to be operational, you must configure an IP address for the interface and mark it as operational (no shutdown). In practice, you always configure additional parameters for each interface.

Management and monitoring options

Management interfaces enable you to manage and monitor devices in the Cisco Catalyst SD-WAN fabric, allowing you to collect information from the devices in an out-of-band fashion and to perform operations on the devices, such as configuring and rebooting them.

These are the available management interfaces:

- CLI
- IP Flow Information Export (IPFIX)
- REST API
- SNMP
- System logging (syslog) messages
- Cisco SD-WAN Manager

CLI through SSH

You can access a CLI on each device, and from the CLI, you configure overlay network features on the local device and gather operational status and information regarding that device. Using an available CLI, we strongly recommend that you configure and monitor all the Cisco Catalyst SD-WAN network devices from Cisco SD-WAN Manager, which provides views of network-wide operations and device status, including detailed operational and status data. In addition, Cisco SD-WAN Manager provides straightforward tools for bringing up and configuring overlay network devices, including bulk operations for setting up multiple devices simultaneously.

You can access the CLI by establishing an SSH session to a Cisco Catalyst SD-WAN device.

For a Cisco Catalyst SD-WAN device that is being managed by Cisco SD-WAN Manager, if you create or modify the configuration from the CLI, the changes are overwritten by the configuration that is stored in the Cisco SD-WAN Manager configuration database.

IPFIX

The IP Flow Information Export (IPFIX) protocol, also called cflowd, is a tool for

- monitoring the traffic flowing through devices in the Cisco Catalyst SD-WAN fabric, and
- exporting information about the traffic to a flow collector.

cflowd version

Cisco Catalyst SD-WAN implements cflowd Version 10, as specified in RFC 7011 and RFC 7012.

Aggregating information

Cisco Catalyst SD-WAN Cflowd performs 1:1 traffic sampling. Information about all the flows is aggregated in the cflowd records. Flows are not sampled.

Devices do not cache any of the records that are exported to a collector.

For a list of elements exported by IPFIX, refer to the information about traffic flow monitoring with Cflowd in the *Cisco Catalyst SD-WAN Policies Configuration Guide*.

Enabling the collection of traffic flow information

To enable the collection of traffic flow information, you must create data policies that identify the traffic of interest, and then direct that traffic to a Cflowd collector. Refer to the information about traffic flow monitoring with Cflowd in the *Cisco Catalyst SD-WAN Policies Configuration Guide*.

You can also enable cflowd visibility directly on devices without configuring a data policy, so that you can perform traffic flow monitoring on the traffic coming to the device from all the VPNs in the LAN. You can then monitor the traffic from Cisco SD-WAN Manager or from the device's CLI.

REST API

The Cisco Catalyst SD-WAN representational state transfer (REST) application programming interface (API) is a programmatic interface for controlling, configuring, and monitoring the devices in the network.

You can access the REST API through Cisco SD-WAN Manager.

The REST API calls expose the functionality of the Cisco Catalyst SD-WAN software and hardware to an application program. Such functionality includes the normal operations you perform to maintain the devices and the overlay network itself.

SNMP

The Simple Network Management Protocol (SNMP) is an internet standard protocol that allows you to manage all the devices in the Cisco Catalyst SD-WAN network.

SNMP version

Cisco Catalyst SD-WAN supports supports SNMP v2c.

For SNMPv3, the PDU type for notifications is either SNMPv2c inform (InformRequest-PDU) or trap (Trapv2-PDU).

Configuring SNMP

You can configure:

- Properties for a device, such as device name, location, contact, and community, to enable the device to be monitored by a network management system.
- SNMP servers to receive SNMP trap messages.
- SNMP traps and trap groups. SNMP traps are messages that devices send to indicate an event or problem.

SNMP management information base

The object identifier (OID) for the internet port of the SNMP management information base (MIB) is 1.3.6.1.

System log messages

System log (syslog) messages are records of events on a device that form a chronological log of the device status for auditing, debugging problems, and so on.

System logging operations use a mechanism similar to the UNIX **syslog** command to record system-wide, high-level operations that occur on the devices in the Cisco Catalyst SD-WAN network.

The log levels (priorities) of the messages are the same as those in standard UNIX commands. You can configure the priority of the syslog messages to log.

You can configure logging to store the syslog files locally on the device or to send them to a remote host.

Cisco SD-WAN Manager

Cisco SD-WAN Manager is a centralized network management system that

- allows configuration and management of the devices in the Cisco Catalyst SD-WAN fabric, and
- provides a dashboard displaying the operations of the entire network and of individual devices in the network.

Three or more Cisco SD-WAN Manager servers are consolidated into a Cisco SD-WAN Manager cluster to

- provide scalability and management support for up to 6,000 devices
- distribute Cisco SD-WAN Manager functions across multiple devices, and
- provide redundancy of network management operations.

Enforce a software version on devices

If you are using the Cisco Catalyst SD-WAN hosted service, you can enforce a version of the Cisco Catalyst SD-WAN software to run on a router when it first joins the overlay network.

To ensure that templates are in sync after an upgrade that enforces a software version, make sure of these before you perform the upgrade:

- The bootflash and flash on the router must have enough free space to support the upgrade
- The version of the SD-WAN image that is on the device before the upgrade must be a lower version than the enforced SD-WAN version you specify in the procedure in this section
- For ZTP enforcement feature to start, initial onboarding has to be done through PNP/ZTP workflow.

Before you begin

- Ensure that the bootflash and flash on the router have enough free space to support the upgrade.
- Ensure that the version of the SD-WAN image that is on the device before the upgrade is a lower version than the version of the software image you are enforcing with this procedure.
- For ZTP enforcement feature to start, initial onboarding has to be done through the Plug-and-Play/ZTP workflow.

Follow these steps to enforce a specific software version to run a device when it first joins the fabric.

Procedure

Step 1 Ensure that the software image for the desired device software version is present in the Cisco SD-WAN Manager software image repository:

a) From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.

The **Software Repository** page opens and displays a table of software images. If the desired software image is present in the repository, continue with Step 2.

b) If you need to add a software image, click **Add New Software**.

c) Select the location from which to download the software images, either Cisco SD-WAN Manager, Remote Server, or Remote Server - Cisco SD-WAN Manager.

d) Select an x86-based or a MIPS-based software image.

e) To place the image in the repository, click **Add**.

Step 2 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Step 3 Click **Enforce Software Version (ZTP)**.

If you are using Cisco Catalyst SD-WAN Manager Release 20.12.x or earlier, locate **Enforce Software Version (ZTP)** and click **Edit**.

Step 4 For a specific platform, enable enforcing the software version.

Step 5 Do one of these:

- Use an image on a local server:

a. In the **Image Location** field, choose **Local Server**.

b. In the **Version/Image Name** field, choose an image.

- Use an image on a remote server:

a. In the **Image Location** field, choose **Remote Server**.

b. In the **Remote Server Name** field, choose a server.

c. In the **Image Filename** field, choose an image.

Step 6 Click **Save**.

Configuring a login page banner

Describes methods for configuring a login page banner.

- Configure a login page banner using a configuration group, on page 193
- Configure a login page banner, using templates, on page 194
- Configure a login page banner, using CLI commands, on page 195

Configure a login page banner using a configuration group

You can configure the banner text for login pages.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Follow these steps to configure a login page banner.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure a Banner feature in a System profile.

Table 37: Banner Basic Settings

Field	Description
Type	Choose a feature from the drop-down list.
Feature Name*	Enter a name for the feature.
Description	Enter a description of the feature. The description can contain any characters and spaces.

Field	Description
Login	Enter the text to display before the login prompt. The string can be up to 2048 characters long. To insert a line break, type \n.
Message of the Day	On a Cisco IOS XE Catalyst SD-WAN device, enter the message-of-the-day text to display before the login banner. The string can be up to 2048 characters long. To insert a line break, type \n.

What to do next

Refer to Deploy a Configuration Group in the *Cisco Catalyst SD-WAN Configuration Groups Reference Guide*.

Configure a login page banner, using templates

Use the Banner template for Cisco Catalyst SD-WAN Validators, Cisco SD-WAN Managers, Cisco Catalyst SD-WAN Controllers and Cisco IOS XE Catalyst SD-WAN devices.

- To configure the banner text for login pages using Cisco SD-WAN Manager templates, create a Banner feature template to configure PIM parameters, as described in this topic.
- To configure a login banner for the Cisco SD-WAN Manager system, from the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Before you begin

Follow these steps to configure a login page banner.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**, click **Add Template**, and select an appropriate device model.

In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.

Step 3 Select **Cisco Banner** from the list of templates.

Step 4 Configure these parameters:

Table 38: Configuring a banner:

Field	Description
MOTD Banner	On a Cisco IOS XE Catalyst SD-WAN device enter message-of-the-day text to display prior to the login banner. The string can be up to 2048 characters long. To insert a line break, type **\n**.
Login Banner	Enter text to display before the login prompt. The string can be up to 2048 characters long. To insert a line break, type **\n**.

Step 5 To save the feature template, click **Save.**

Configure a login page banner, using CLI commands

Before you begin

Perform these steps to configure a login banner using CLI commands.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Use the **banner** command to configure a login page banner.

```
banner {login login-string | motd motd-string}
```

Create a custom banner

Before you begin

Follow these steps to create a custom banner that is displayed when you log in to Cisco SD-WAN Manager.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Step 2 Open **Banner**.

Step 3 Enable the **Configure a login banner for the Cisco Catalyst SD-WAN Manager system** control.

Step 4 In **Banner Info**, enter the text string for the login banner or click **Select a File** to download a file that contains the text string.

Step 5 Click **Save**.

Configuring device basic settings

Describes methods for configuring device basic settings.

- Configure device basic settings using a configuration group, on page 195
- Configure device basic system settings using templates, on page 198

Configure device basic settings using a configuration group

Before you begin

Perform these steps to configure basic parameters for devices.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure a Basic feature in a System profile.

a. Configure basic settings.

Table 39: Basic Settings

Field	Description
Time Zone	Choose the time zone to use on the device.
Device Groups	Enter the names of one or more groups to which the device belongs, separated by commas.
Location	Enter a description of the location of the device. It can be up to 128 characters.
Description	Enter any additional descriptive information about the device.
Transport Gateway	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) Enable transport gateway functionality for the device. A transport gateway connects routers that may or may not have direct connectivity. One common use case for transport gateways is to provide connectivity between routers in disjoint networks, such as between public and private WANs. Another use case for transport gateway functionality is to use a transport gateway as the hub in a hub-and-spoke topology.

b. Configure controller settings.

c. Configure GPS.

Table 40: GPS

Field	Description
GPS Latitude	Enter the latitude of the device, in the format decimal-degrees.
GPS Longitude	Enter the longitude of the device, in the format decimal-degrees.

d. Configure track settings.

Table 41: Track Settings

Field	Description
Track Transport	Enable this option to regularly check whether the DTLS connection between the device and a Cisco SD-WAN Validator is up. Default: Enabled

Field	Description
Track Default Gateway	Enable or disable tracking of default gateway. Gateway tracking determines, for static routes, whether the next hop is reachable before adding that route to the route table of the device. Default: Enabled
Track Interface Tag	Set the tag string to include in routes associated with a network that is connected to a non-operational interface. Range: 1 through 4294967295
Tracker DIA Stabilize Status	Enable this option to stabilize interface flaps by using the multiplier to update HTTP or ICMP tracker status from DOWN to UP.

e. Configure advanced settings.

Table 42: Advanced

Field	Description
Port Hopping	Enable or disable port hopping. When a Cisco Catalyst SD-WAN device is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other Cisco Catalyst SD-WAN devices when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. Default: Enabled
Port Offset	Enter a number by which to offset the base port number. Configure this option when multiple Cisco Catalyst SD-WAN devices are behind a single NAT device, to ensure that each device uses a unique base port for DTLS connections. Values: 0 through 19
On Demand Tunnel	Enable dynamic on-demand tunnels between any two Cisco Catalyst SD-WAN spoke devices.
On Demand Tunnel Idle Timeout (In Minute)	Enter the on-demand tunnel idle timeout time. After the configured time, the tunnel between the spoke devices is removed. Range: 1 to 65535 minutes Default: 10 minutes
Control Session PPS	Enter a maximum rate of DTLS control session traffic to police the flow of control traffic. Range: 1 through 65535 pps Default: 300 pps
Multi Tenant	Enable this option to specify the device as multitenant.

Field	Description
Admin Tech On Failure	Enable this option to collect admin-tech information when the device reboots. Default: Enabled

What to do next

Refer to Deploy a Configuration Group in the *Cisco Catalyst SD-WAN Configuration Groups Reference Guide*.

Configure device basic system settings using templates

Create a Cisco System feature template to configure device system settings.

You can create a Cisco System feature template directly or through a device template.

Before you begin

Follow these steps to create a Cisco System feature template.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Select **Feature Templates**.

Step 3 Click **Add Template**.

Step 4 Select a platform.

Step 5 Click **Cisco System**.

Step 6 According to your needs, configure one or more of these sections.

a) To configure system-wide functionality on a Cisco Catalyst SD-WAN device, select the **Basic Configuration** tab and configure these parameters.

Table 43:

Field	Description
Site ID (on routers, Cisco SD-WAN Manager instances, and Cisco SD-WAN Controller)	Identifier of the site in the SD-WAN fabric domain where the device resides, such as a branch, campus, or data center. The site ID must be the same for all devices at the same site. Range: 1 through 4,294,967,295 (2^{32} – 1, or hexadecimal 0x100000000 – 1)
System IP	System IP address for the Cisco Catalyst SD-WAN device, in decimal four-part dotted notation. The system IP address provides a fixed location of the device in the overlay network and is a component of the device's TLOC address. It is used as the device's loopback address in the transport VPN (VPN 0). You cannot use this same address for another interface in VPN 0.

Field	Description
Timezone	Timezone to use on the device.
Hostname	Name for the device. Maximum 32 characters.
Location	Description of the location of the device. Maximum 128 characters.
Device Groups	Names of one or more groups to which the device belongs, separated by commas.
Controller Groups	SD-WAN Controller groups to which the router belongs.
Description	Additional descriptive information about the device.
Console Baud Rate	Baud rate of the console connection on the router. Values: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 baud or bits per second (bps). Default: 9600 (from Cisco vManage Release 20.3.1)
Maximum OMP Sessions	Maximum number of OMP sessions that a router can establish to a Cisco Catalyst SD-WAN Controller. Range: 0 through 100 Default: 2

b) To configure a device location, select the **GPS** tab and configure these parameters. The location is used to place the device on the SD-WAN Manager network map. Setting the location also allows SD-WAN Manager to send a notification if the device is moved to another location.

Table 44:

Field	Description
Latitude	Latitude of the device, in the format *decimal-degrees*.
Longitude	Longitude of the device, in the format *decimal-degrees*.

c) To track the status of transport interfaces that connect to the internet (Network Address Translation Direct Internet Access (NAT DIA),

- click **Tracker** and **New Endpoint Tracker**, or
- click **Tracker Group** and **New Endpoint Tracker Group**.

Then configure these parameters.

Table 45:

Field	Description
Name	Name of the tracker. The name can be up to 128 alphanumeric characters. You can configure up to eight trackers.
Tracker Type	Choose an interface, static route.

Field	Description
Threshold	How long to wait for the probe to return a response before declaring that the transport interface is down. Range: 100 to 1000 milliseconds Default: 300 milliseconds
Interval	How often probes are sent to determine the status of the transport interface. Range: 10 to 600 seconds Default: 60 seconds (1 minute)
Multiplier	Number of times to resend probes before declaring that the transport interface is down. Range: 1 to 10 Default: 3
Tracker Type	Interface or static route.
Endpoint Type	IP address or DNS name.
Endpoint IP or Endpoint DNS Name	Endpoint IP. or DNS name of the end point of the tunnel interface. This is the destination in the internet to which the router sends probes to determine the status of the transport interface.

A DIA tracker helps determine if the internet or external network becomes unavailable. This feature is useful when NAT is enabled on a transport interface in VPN 0 to allow data traffic from the router to exit directly to the internet.

If the internet or external network becomes unavailable, the router continues to forward traffic based on the NAT route in the service VPN. Traffic that is forwarded to the internet gets dropped. To prevent the internet-bound traffic from being dropped, configure the DIA tracker on the edge router to track the status of the transport interface. The tracker periodically probes the interface IP address of the end point of the tunnel interface to determine the status of the transport interface. The tracker determines the status of the internet and returns the data to the attach points that are associated with the tracker.

When the tracker is configured on the transport interface, the interface IP address is used as a source IP address for probe packets.

IP SLA monitors the status of probes and measures the round trip time of these probe packets and compares the values with the configured latency in the probe. When the latency exceeds the configured threshold value, the tracker considers the network as unavailable.

If the tracker determines that the local internet is unavailable, the router withdraws the NAT route and reroutes the traffic based on the local routing configuration to overlay.

The local router continues to periodically check the status of the path to the interface. When it detects that the path is functioning again, the router reinstalls the NAT route to the internet.

For more information on NAT DIA tracker for Cisco IOS XE Catalyst SD-WAN devices, refer to NAT DIA Tracker in the *Cisco Catalyst SD-WAN NAT Configuration Guide*.

To apply a tracker to an interface, configure it in the **VPN Interface Cellular**, **VPN Interface Ethernet**, **VPN Interface NAT Pool**, or **VPN Interface PPP** configuration templates. You can apply only one tracker to an interface.

To monitor endpoint trackers, see Monitor NAT DIA endpoint trackers, on page 229.

d) To configure additional system parameters, click **Advanced** and configure these parameters:

Field	Description
Control Session Policer Rate	Maximum rate of DTLS control session traffic, to police the flow of control traffic. Range: 1 to 65535 pps Default: 300 pps
Port Hopping	Click **On** to enable port hopping, or click **Off** to disable it. When a device is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other devices when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. To disable port hopping on an individual TLOC (tunnel interface), use the VPN Interface Ethernet configuration template. Default: Enabled on routers. Disabled on Cisco SD-WAN Manager or Cisco Catalyst SD-WAN Controller hosts.
Port Offset	Number by which to offset the base port number. Configure this option when multiple devices are behind a single NAT device, to ensure that each device uses a unique base port for DTLS connections. Range: 0 to 19
Track Transport	**On** : Regularly check whether the DTLS connection between the device and a Cisco Catalyst SD-WAN Validator is up. **Off**: Disable checking. Default: Enabled
Track Interface	Tag string to include in routes associated with a network that is connected to a non-operational interface. Range: 1 to 4,294,967,295
Gateway Tracking	**On** : Enable tracking of default gateway. **Off**: Disable tracking. Gateway tracking determines, for static routes, whether the next hop is reachable before adding that route to the device's route table. Default: Enabled
Collect Admin Tech on Reboot	**On** : Collect admin-tech information when the device reboots. **Off**: Disable collection.

Field	Description
Idle CLI Timeout in minutes	How long to wait, when the CLI is inactive, to log out the user. If a user is connected to the device via an SSH connection, the SSH connection is closed after this time expires. Default: CLI session does not time out.

Configuring global system settings

Describes methods for configuring global system settings.

- Configure global system settings using a configuration group, on page 202
- Configure global system settings using templates, on page 204
- Configure global system settings using CLI commands, on page 207

Configure global system settings using a configuration group

Before you begin

Perform these steps to configure basic parameters for devices.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure a Global feature in a System profile.

a) Configure services.

Table 46: Services

Field	Description
HTTP Server	Enable or disable HTTP server.
HTTPS Server	Enable or disable secure HTTPS server.
FTP Passive	Enable or disable passive FTP.
Domain Lookup	Enable or disable Domain Name System (DNS) lookup.
ARP Proxy	Enable or disable proxy ARP.
RSH/RCP	Enable or disable remote shell (RSH) and remote copy (rcp) on the device.
Line Virtual Teletype (Configure Outbound Telnet)	Enable or disable outbound telnet.

Field	Description
Cisco Discovery Protocol (CDP)	Enable or disable Cisco Discovery Protocol (CDP).
Link Layer Discovery Protocol (LLDP)	Enable or disable Link Layer Discovery Protocol (LLDP).
Specify interface for source address	Enter the address of the source interface in all HTTPS client connections.

b) Configure NAT64.

Table 47: NAT 64

Field	Description
UDP Timeout	Specify the NAT64 translation timeout for UDP. Range: 1 to 536870 (seconds) Default: 300 seconds (5 minutes)
TCP Timeout	Specify the NAT64 translation timeout for TCP. Range: 1 to 536870 (seconds) Default: 3600 seconds (1 hour)

c) Configure authentication.

Table 48: Authentication

Field	Description
HTTP Authentication	Choose the HTTP authentication mode. Accepted values: Local, AAA Default: Local

d) Configure SSH.

Table 49: SSH Version

Field	Description
SSH Version	Choose the SSH version. Default: Disabled

e) Configure other settings.

Table 50: Other Settings

Field	Description
TCP Keepalives (In)	Enable or disable generation of keepalive timers when incoming network connections are idle.
TCP Keepalives (Out)	Enable or disable generation of keepalive timers when outgoing network connections are idle.
TCP Small Servers	Enable or disable small TCP servers (for example, ECHO).
UDP Small Servers	Enable or disable small UDP servers (for example, ECHO).
Console Logging	Enable or disable console logging. By default, the router sends all log messages to its console port.
IP Source Routing	Enable or disable IP source routing. IP source routing is a feature that enables the originator of a packet to specify the path for the packet to use to get to the destination.
VTY Line Logging	Enable or disable the device to display log messages to a vty session in real time.
SNMP IFINDEX Persist	Enable or disable SNMP IFINDEX persistence, which provides an interface index (ifIndex) value that is retained and used when the device reboots.
Ignore BOOTP	Enable or disable BOOTP server. When enabled, the device listens for the BOOTP packet that comes in sourced from 0.0.0.0. When disabled, the device ignores these packets.
(optional) **Interface statistics per minute**	Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 26.1.1 Choose the time interval for interface statistics data collection: • **1 minute** • **5 minutes** (default)

What to do next

Refer to Deploy a Configuration Group in the *Cisco Catalyst SD-WAN Configuration Groups Reference Guide*.

Configure global system settings using templates

Configure global system settings using templates.

From Cisco IOS XE Catalyst SD-WAN Release Amsterdam 17.2.x, you can use the Global Settings template to configure device global parameters such as:

- Services such as HTTP and Telnet

- NAT64 time-outs
- HTTP authentication mode
- TCP keepalive
- TCP and UDP small servers
- Console logging
- IP source routing
- VTY line logging
- SNMP IFINDEX persistence
- BOOTP server

Before you begin

Follow these steps to configure global system settings.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**.

In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

Step 3 Click **Add Template**.

Step 4 Select a device type.

Step 5 Create a Global Settings template.

Step 6 Enter a name and description.

Step 7 Configure these parameters according to your requirements.

a) Configure services.

Field	Description
HTTP Server	Enable or disable HTTP server.
HTTPS Server	Enable or disable secure HTTPS server.
Passive FTP	Enable or disable passive FTP.
IP Domain-Lookup	Enable or disable domain name server (DNS) lookup.
Arp Proxy	Enable or disable proxy ARP.
RSH/RCP	Enable or disable remote shell (RSH) and remote copy (RCP) on the device.
Telnet (Outbound)	Enable or disable outbound telnet.

Field	Description
CDP	Enable or disable Cisco Discovery Protocol (CDP). From Cisco IOS XE SD-WAN Release 17.3.1, CDP on interfaces is enabled when the **cdp run** command is executed globally on Cisco ASR 1000 series devices.

b) Configure NAT64.

Field	Description
UDP Timeout	NAT64 translation timeout for UDP Range: 1 to 65536 (seconds) Default: 300 seconds (5 minutes) **Note** From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1, the default UDP Timeout value for NAT64 has changed to 300 seconds (5 minutes).
TCP Timeout	NAT64 translation timeout for TCP Range: 1 to 65536 (seconds) Default: 3600 seconds (1 hour) **Note** From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1, the default TCP Timeout value for NAT64 has been changed to 3600 seconds (1 hour).

c) Configure authentication.

Field	Description
HTTP Authentication	HTTP authentication mode Accepted values: Local, AAA Default: Local

d) Configure SSH.

Field	Description
SSH version	Specify an SSH version. Default value: Version 2

e) Configure other settings.

Field	Description
TCP Keepalives (In)	Enable or disable generation of keepalive timers when incoming network connections are idle.

Field	Description
TCP Keepalives (Out)	Enable or disable generation of keepalive timers when outgoing network connections are idle.
TCP Small Servers	Enable or disable small TCP servers (for example, ECHO).
UDP Small Servers	Enable or disable small UDP servers (for example, ECHO).
Console Logging	Enable or disable console logging. By default, the router sends all log messages to its console port.
IP Source Routing	Enable or disable IP source routing. IP source routing is a feature that enables the originator of a packet to specify the path for the packet to use to get to the destination.
VTY Line Logging	Enable or disable the device to display log messages to a VTY session in real time.
SNMP IFINDEX Persist	Enable or disable SNMP IFINDEX persistence, which provides an interface index (ifIndex) value that is retained and used when the device reboots.
Ignore BOOTP	Enable or disable BOOTP server. When enabled, the device listens for the bootp packet that comes in sourced from 0.0.0.0. When disabled, the device ignores these packets.

Configure global system settings using CLI commands

Configure global system settings using CLI commands in a CLI add-on profile or CLI add-on template.

These CLI instructions are not comprehensive.

Before you begin

Perform these steps to configure global system settings using CLI commands.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Enable or disable services.

Enable services:

```
system
    ip http server
    ip http secure-server
    ip ftp passive
    ip domain lookup
    ip arp proxy disable
    ip rcmd rsh-enable
    ip rcmd rcp-enable
    cdp run enable
```

Note

From Cisco IOS XE SD-WAN Release 17.3.1, CDP on interfaces is enabled when the **cdp run** command is executed globally on Cisco ASR 1000 series devices.

Enable outbound Telnet:

```
system
    line vty 0 4
        transport input telnet ssh
```

Disable services:

```
system
    no ip http server
    no ip http secure-server
    no ip ftp passive
    no ip domain lookup
    no ip arp proxy disable
    no ip rcmd rsh-enable
    no ip rcmd rcp-enable
    no cdp run enable
```

Disable outbound Telnet:

```
system
    line vty 0 4
        transport input ssh
```

Step 3 Enable or disable other settings.

Enable:

```
system
    service tcp-keepalives-in
    service tcp-keepalives-out
    service tcp-small-servers
    service udp-small-server
    logging console
    ip source-route
    logging monitor
    snmp-server ifindex persist
    ip bootp server
```

Disable:

```
system
    no service tcp-keepalives-in
    no service tcp-keepalives-out
    no service tcp-small-servers
    no service udp-small-server
    no logging console
    no ip source-route
    no logging monitor
    no snmp-server ifindex persist
    no ip bootp server
```

Step 4 Configure NAT64.

```
system
    nat64 translation timeout udp timeout
    nat64 translation timeout tcp timeout
```

Step 5 Configure authentication.

```
system
    ip http authentication {local | aaa}
```

Configuring NTP servers

Describes methods for configuring NTP servers.

- Configure NTP servers using a configuration group, on page 209
- Configure NTP servers and parameters using templates, on page 211
- Configure NTP servers using CLI commands, on page 213

Configure NTP servers using a configuration group

Configuring network time for your network includes these tasks:

1. Configure NTP servers and parameters as described in this procedure.
2. Configure the timezone in a System profile, in a Basic feature.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Perform these steps to configure NTP servers and parameters.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure an NTP feature in a System profile.

a) Configure a server.

Table 51: Server

Field	Description
Add Server	
Hostname/IP address*	Enter the IP address of an NTP server, or a DNS server that knows how to reach the NTP server.
VPN to reach NTP Server*	Enter the number of the VPN that should be used to reach the NTP server, or the VPN in which the NTP server is located. If you have configured multiple NTP servers, they must all be located or be reachable in the same VPN. Range: 1 to 65525, excluding 512. For details see the VRF range behavior change described here.

Field	Description
Set authentication key for the server	Specify the MD5 key associated with the NTP server, to enable MD5 authentication. For the key to work, you must mark it as trusted in the **Trusted Key** field under **Authentication**.
Set NTP version*	Enter the version number of the NTP protocol software. Range: 1 to 4 Default: 4
Set interface to use to reach NTP server	Enter the name of a specific interface to use for outgoing NTP packets. The interface must be located in the same VPN as the NTP server. If it is not, the configuration is ignored.
Prefer this NTP server*	Enable this option if multiple NTP servers are at the same stratum level and you want one to be preferred. For servers at different stratum levels, Cisco Catalyst SD-WAN chooses the one at the highest stratum level.

b) Configure authentication.

Table 52: Authentication

Field	Description
Add Authentication Keys	
Key Id*	Enter an MD5 authentication key ID. Range: 1 to 65535
MD5 Value*	Enter an MD5 authentication key. Enter either a cleartext key or an AES-encrypted key.
Trusted Key	Enter the MD5 authentication key to designate the key as trustworthy. To associate this key with a server, enter the same value that you entered for the **Set authentication key for the server** field under **Server**.

c) Configure advanced parameters.

Table 53: Advanced

Field	Description
Authoritative NTP Server	Choose **Global** from the drop-down list, and enable this option if you want to configure one or more supported routers as a primary NTP router.
Stratum	Enter the stratum value for the primary NTP router. The stratum value defines the hierarchical distance of the router from its reference clock. Valid values: Integers 1 to 15. If you do not enter a value, the system uses the router internal clock default stratum value, which is 8.

Field	Description
Source Interface	Enter the name of the exit interface for NTP communication. If configured, the system sends NTP traffic to this interface. For example, enter **GigabitEthernet1** or **Loopback0**.

What to do next

Refer to Deploy a Configuration Group in the *Cisco Catalyst SD-WAN Configuration Groups Reference Guide*.

Configure NTP servers and parameters using templates

Configure network time protocol (NTP) servers using a Cisco NTP feature template.

You can create a Cisco NTP feature template directly or through a device template.

Configuring network time for your network includes these tasks:

1. Configure NTP servers and parameters as described in this procedure.
2. Configure the timezone in a System template.

Before you begin

Perform these steps to configure NTP servers and parameters.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Select **Feature Templates**.

Step 3 Click **Add Template**.

Step 4 Select a platform.

Step 5 Click **Cisco NTP**.

Step 6 To add an NTP server:

a) Click **Server**.

b) Click **New Server**, and configure these parameters.

Table 54: NTP server parameters

Field	Description
Hostname/IP Address*	IP address of an NTP server, or a DNS server that knows how to reach the NTP server.

Field	Description
Authentication Key ID*	Specify the MD5 authentication key associated with the NTP server, to enable authentication. For the key to work, you must mark it as trusted in the **Trusted Keys** field, under **Authentication**. **Note** From Cisco Catalyst SD-WAN Control Components Release 20.14.1, you can use CMAC-AES authentication when configuring NTP servers for Cisco SD-WAN Control Components. This requires configuration using a CLI template.
VPN ID*	Number of the VPN that should be used to reach the NTP server, or the VPN in which the NTP server is located. If you have configured multiple NTP servers, they must all be located or be reachable in the same VPN. The valid range is from 0 through 65530.
Version*	Version number of the NTP protocol software. The range is from 1 through 4. The default is 4.
Source Interface	Name of a specific interface to use for outgoing NTP packets. The interface must be located in the same VPN as the NTP server. If it is not, the configuration is ignored.
Prefer	Click **On** if multiple NTP servers are at the same stratum level and you want one to be preferred. For servers at different stratum levels, the software chooses the one at the highest stratum level.

c) You can click **Add** to add another server.
d) Click **Save**.

Step 7 To configure the authentication keys used to authenticate NTP servers:
a) Click **Authentication**.
b) Click the **Authentication Key** tab.
c) Click **New Authentication Key**, and configure these parameters.

Table 55: NTP authentication key parameters

Field	Description
Authentication Key ID*	• Authentication Key: Enter an authentication key ID. Range: 1 to 65535 • Authentication Value: Enter either a cleartext key or an AES-encrypted key.
Authentication Value*	Enter an authentication key. For this key to be used, you must designate it as trusted. To associate a key with a server, enter the same value that you entered in the **Authentication Key ID** field under **Server**.

d) Click **Add**.

Step 8 To configure the trusted keys used to authenticate NTP servers:
a) Click **Authentication**.

b) Click the **Trusted Key** tab.
c) Configure these parameters.

Table 56: Trusted key parameters

Field	Description
Trusted Keys*	Authentication key to designate the key as trustworthy. To associate this key with a server, enter the same value that you entered for the **Authentication Key ID** field under **Server**.

Configure NTP servers using CLI commands

Configure NTP servers using CLI commands in a CLI add-on profile or CLI add-on template.

Before you begin

Perform these steps to configure NTP servers.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Enter system configuration mode.

```
system
```

Step 3 Enter NTP configuration mode.

```
ntp
```

Step 4 Enter keys configuration mode.

```
keys
```

Step 5 Configure an authentication type to use for an NTP server. Assign a key for the authentication type, and assign one of these authentication methods: MD5, CMAC-AES-128. Using multiple instances of the **authentication** command, you can configure authentication for multiple NTP servers.

```
authentication authentication-key-id {md5 md5-authentication-key | cmac-aes-128 cmac-authentication-key}
```

Note
The CMAC-AES option is available from Cisco Catalyst SD-WAN Control Components Release 20.14.1.

Step 6 Designate an authentication type as trusted. Optionally, you can include multiple authentication key IDs.

```
trusted authentication-key-id {authentication-key-id}[authentication-key-id]
```

Step 7 Exit keys configuration mode.

```
exit
```

Step 8 Configure an NTP server, including the VPN and version, and optionally an authentication key. You can configure multiple NTP servers.

```
server {server-ip | fully-qualified-domain-name}
key authentication-key
vpn vpn-id
version version-id
exit
```

Here is an example for configuring two authentication types and three NTP servers. Two servers are trusted and use an authentication key, and one server is generic. Authentication key 1001 uses MD5 and key 1002 uses CMAC-AES-128.

```
system ntp
  keys
    authentication 1001 md5 password1
    authentication 1002 cmac-aes-128 password2
    trusted 1001 1002
  !
  server 192.168.10.1
    key 1001
    vpn 512
    version 4
  exit
  server 192.168.10.2
    key 1002
    vpn 512
    version 4
  server us.pool.ntp.org
    vpn 512
    version 4
  exit
  !
!
```

Note The passwords above are in plain text. When using a CLI template, you can encrypt passwords.

Configuring a router as an NTP primary

Describes methods for configuring a router as an NTP primary.

- Configure a router as an NTP primary using templates, on page 214
- Configure a router as an NTP primary using CLI commands, on page 215

Configure a router as an NTP primary using templates

Configure a router to operate as an NTP primary using templates.

You can configure one or more supported routers as an NTP primary router in a Cisco Catalyst SD-WAN deployment. A router that is configured in this way acts as the NTP server to which other nodes in the deployment synchronize their clocks.

Configuring a router as an NTP primary router is useful if you do not have an NTP server in your deployment.

To configure a router as an NTP primary router, create a template that includes configured parameters for the NTP primary router.

Before you begin

Follow these steps to configure a router to operate as an NTP primary.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Create a new Cisco NTP feature template or edit an existing one.

- To create a new Cisco NTP feature template, click **Feature Templates**, click **Add Template**, select the type of device to be the NTP primary router, and then select the **Cisco NTP** template in the **Basic Information** section.
- To update an existing Cisco NTP feature template, click **Feature Templates**, click **...** adjacent to a template, and select **Edit**.

Step 3 For a new template, enter a name and description.

Step 4 In the **Master** tab, perform these steps:

a) For the **Master** option, choose **Global** from the drop-down list, and then select **On**.

b) (Optional) In the **Stratum** field, enter the stratum value for the NTP primary router, which is the hierarchical distance of the router from its reference clock.

Range: 1 to 15

Default: 8

c) (Optional) In the **Source** field, enter the name of the exit interface for NTP communication.

If configured, the system sends NTP traffic to this interface.

Examples: **GigabitEthernet1**, **Loopback0**

Step 5 Click **Save** for a new template, or **Update** if updating an existing template.

Configure a router as an NTP primary using CLI commands

Configure NTP using CLI commands in a CLI add-on profile or CLI add-on template.

These CLI instructions are not comprehensive.

You can configure one or more supported routers as an NTP primary router in a Cisco Catalyst SD-WAN deployment. A router that is configured in this way acts as the NTP server to which other nodes in the deployment synchronize their clocks.

Configuring a router as an NTP primary router is useful if you do not have an NTP server in your deployment.

Before you begin

Perform these steps to configure NTP settings using CLI commands.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Use **ntp master** to configure a device as primary.

Optionally, include a stratum value for the NTP primary router. The stratum value defines the hierarchical distance of the router from its reference clock. For *stratum-number*:

- Range: 1 to 15
- Default: 8

```
ntp master [stratum-number]
```

Step 3 (Optional) Use **ntp source** to configure an NTP source, which is an exit interface for NTP communication.

If configured, the system sends NTP traffic to this interface.

Examples for *source-interface*: **GigabitEthernet1**, **Loopback0**

```
ntp source source-interface
```

Configure device time using CLI commands

You can set the time locally on a device without using NTP if you do not need to ensure that time is synchronized across an entire network of devices. You can also set the time locally on any device as it is joining the network, in addition to configuring an NTP server. The local time gets overwritten by the official NTP time once the device contacts the NTP server.

Configure the time using CLI commands in a CLI add-on profile or CLI add-on template.

Before you begin

Perform these steps to configure the time on a device using CLI commands.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Use **clock set** to set the time.

```
clock set hh:mm:ss dd month yyyy
```

```
clock set 12:00:00 31 May 2019
```

Configuring GPS

Describes methods for configuring GPS.

- Configure GPS using a configuration group, on page 217
- Configure GPS using templates, on page 218

Configure GPS using a configuration group

Before you begin

Perform these steps to configure GPS for devices.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure a GPS feature in a Transport and Management profile.

Step 3 Configure GPS.

Table 57: GPS

Field	Description
Type	Choose a feature from the drop-down list.
Feature Name*	Enter a name for the feature. The name can be up to 128 characters and can contain only alphanumeric characters.
Description	Enter a description of the feature. The description can be up to 2,048 characters and can contain only alphanumeric characters.
GPS	Click **On** to enable the GPS feature on the router.
GPS Mode	Select the GPS mode: • **MS-based**: Use mobile station–based assistance, also called assisted GPS mode, when determining position. In this mode, cell tower data is used to enhance the quality and precision in determining location, which is useful when satellite signals are poor. • **Standalone**: Use satellite information when determining position.
NMEA	Click **On** to enable the use of NMEA streams to help with determining position. NMEA streams data from the router's cellular module to any marine device, such as a Windows-based PC, that is running a commercially available GPS-based application.
Source Address*	Enter the IP address of the router's interface that connects to the external device reading the NMEA.

Field	Description
Destination Address*	Enter the IP address of the external device's interface that's connected to router.
Destination Port*	Enter the number of the port to use to send NMEA data to the external device's interface.

What to do next

Refer to Deploy a Configuration Group in the *Cisco Catalyst SD-WAN Configuration Groups Reference Guide*.

Configure GPS using templates

Configure GPS using templates.

Note You can configure GPS using Cisco SD-WAN Manager from Cisco vManage Release 20.6.1, with devices running Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and later.

Configuring GPS is a prerequisite for geofencing. Refer to Geofencing in the *Cisco Catalyst SD-WAN Location Services Configuration Guide*.

Before you begin

Follow these steps to configure GPS.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Create a new GPS feature template or edit an existing one.

- To create a new GPS feature template, click **Feature Templates**, click **Add Template**, select a device type, and select the **GPS** template.
- To update an existing GPS feature template, click **Feature Templates**, click **...** adjacent to a template, and select **Edit**.

Step 3 For a new template, enter a name and description.

Step 4 Configure the GPS parameters.

Parameter Name	Description
GPS	Click **On** to enable the GPS feature on the router.

Parameter Name	Description
GPS Mode	Select the GPS mode: • **MS-based**: Use mobile station–based assistance, also called assisted GPS mode, when determining position. In this mode, a network data session is used to obtain the GPS satellite locations, resulting in a faster fix of location coordinates. • **Standalone**: Use satellite information when determining position. **Note** Standalone mode is currently not supported for geofencing.
NMEA	Click **On** to enable the use of NMEA streams to help in determining position. NMEA streams data from the router's 4G LTE Pluggable Interface Module (PIM) to any device, such as a Windows-based PC, that is running a commercially available GPS-based application.
Source Address	(Optional) Enter the IP address of the interface that connects to the router's PIM. **Note** This option is not used for configuring geofencing.
Destination Address	(Optional) Enter the IP address of the NMEA server. The NMEA server can be local or remote. **Note** This option is not used for configuring geofencing.
Destination Port	(Optional) Enter the number of the port to use to send NMEA data to the server. **Note** This option is not used for configuring geofencing.

Step 5 Click **Save** for a new template, or **Update** if updating an existing template.

Configuring automatic bandwidth detection

Describes methods for configuring automatic bandwidth detection.

• Configure automatic bandwidth detection using templates, on page 219
• Configure automatic bandwidth detection using CLI commands, on page 221

Configure automatic bandwidth detection using templates

Configure automatic bandwidth detection using templates.

Also see Configure automatic bandwidth detection using CLI commands, on page 221.

You can configure the Cisco VPN Interface Ethernet template to cause a device to automatically detect the bandwidth for WAN interfaces in VPN0 during its day 0 onboarding. If you configure a template in this way,

a Cisco IOS XE Catalyst SD-WAN device attempts to determine the bandwidth for WAN interfaces in VPN0 after completing the PnP process.

Automated bandwidth detection can provide more accurate day 0 bandwidth configuration than manual configuration because there is limited user traffic that can affect results.

A device determines the bandwidth by performing a speed test using an iPerf3 server. iPerf3 is a third-party tool that provides active measurements of bandwidth on IP networks. For more information, see the Iperf.fr website.

If a device has a connection to the internet, the device uses a public iPerf3 server for automatic bandwidth detection, unless you specify a private iPerf3 server. If a device has a connection to a private circuit and no internet connection, you must specify a private iPerf3 server for automatic bandwidth detection.

We recommend that you specify a private iPerf3 server. If a private iPerf3 server is not specified, the device pings a system defined set of public iPerf3 servers and selects for the speed test the public server with the minimum hops value or, if all servers have the same minimum hops value, the server with the minimum latency value. If the speed test fails, the device selects another public server from the list. The device continues to select other public iPerf3 servers until the speed test is successful or until it has tried all servers. Therefore, a speed test on a public iPerf3 server can use a server that is far away, resulting in a larger latency than the minimum.

The set of system defined public iPerf3 servers includes:

- iperf.scottlinux.com
- iperf.he.net
- bouygues.iperf.fr
- ping.online.net
- iperf.biznetnetworks.com

Before you begin

Configure automatic bandwidth detection.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Create a new Cisco VPN Interface Ethernet feature template or edit an existing one.

- To create a new Cisco VPN Interface Ethernet feature template, click **Feature Templates**, click **Add Template**, select a device type, and select the **Cisco VPN Interface Ethernet** template.
- To update an existing Cisco VPN Interface Ethernet feature template, click **Feature Templates**, click **...** adjacent to a template, and select **Edit**.

Step 3 For a new template, enter a name and description.

Step 4 Configure bandwidth detection.

Field	Description
Auto Detect Bandwidth	When enabled, the device detects the bandwidth.

Field	Description
Iperf Server	To use a private iPerf3 server for automatic bandwidth detection, enter the IPv4 address of the private server. To use a public iPerf3 server for automatic bandwidth detection, leave this field blank. The private iPerf3 server should run on port 5201, which is the default iPerf3 port.

Step 5 Ensure that the **allow-service all** command is configured for the tunnel interface.

The device writes the results of a speed test to the auto_speedtest.json file in its bootflash directory. It also displays the results in the **Auto Upstream Bandwidth (bps)** and **Auto Downstream Bandwidth (Mbps)** areas on the **Monitor** > **Devices** > **Interface** page of Cisco SD-WAN Manager.

If a device does not receive a response from an iPerf3 server, an error is recorded in the auto_speedtest.json file and displays on the **Monitor** > **Devices** > **Interface** page of Cisco SD-WAN Manager.

Configure automatic bandwidth detection using CLI commands

Configure automatic bandwidth detection using CLI commands.

Also see Configure automatic bandwidth detection using templates, on page 219.

To disable auto-bandwidth-detect, use the no form of the command: **no auto-bandwidth-detect**.

Before you begin

Perform these steps to configure automatic bandwidth detection.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Use the **auto-bandwidth-detect** command to enable automatic bandwidth detection.

```
auto-bandwidth-detect
iperf-server ipv4-address
```

Step 3 Ensure that the **allow-service all** command is configured for the tunnel interface.

The example includes the **auto-bandwidth-detect**, **iperf-server**, and **allow-service all** commands.

```
sdwan
 interface GigabitEthernet0/0/0
  tunnel-interface
   encapsulation gre
   allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   allow-service sshd
```

```
  allow-service netconf
  no allow-service ntp
  no allow-service ospf
  no allow-service stun
  allow-service https
  no allow-service snmp
  no allow-service bfd
 exit
 auto-bandwidth-detect
 iperf-server 192.0.2.255
exit
appqoe
 no tcpopt enable
 no dreopt enable
```

Proxy server for SD-WAN Manager HTTP and HTTPS traffic with external servers

You can configure a proxy server to handle HTTP and HTTPS traffic between Cisco SD-WAN Manager and external servers.

Traffic

Here's some of the HTTP and HTTPS traffic SD-WAN Manager directs through a proxy, if configured:

- HTTPS connection for Symantec or Cisco automated certificate request or renewal
- REST API calls to URLs of these domains:
  - cisco.com
  - amazonaws.com
  - microsoft.com
  - office.com
  - microsoftonline.com

Each 24 hours, SD-WAN Manager checks whether the proxy server is reachable. If the proxy server is unreachable, SD-WAN Manager raises an alarm: `HTTPS proxy server {IP} not reachable`

Benefits

Cisco SD-WAN Manager uses an HTTP or HTTPS connection to an external server for certain traffic, including:

- Certificate request or renewal
- Cisco Plug and Play integration
- Smart Licensing Using Policy
- Cloud OnRamp
- Software image download

- Data upload to Cisco SD-WAN Analytics

In releases earlier than Cisco vManage Release 20.5.1, you must permit this HTTP and HTTPS traffic in the firewall configured on your on-premises Cisco SD-WAN Manager instance. From Cisco vManage Release 20.5.1, you can channel HTTP and HTTPS traffic through a proxy server. With the proxy server configured, you can restrict HTTP and HTTPS communication with external servers while configuring the firewall and secure the system further.

Restrictions for a proxy server for HTTP and HTTPS traffic

These restrictions apply to using a proxy server for HTTP and HTTPS traffic between Cisco SD-WAN Manager and external servers.

Domain name resolution

When configured to communicate with external servers via an HTTP/HTTPS proxy server, SD-WAN Manager resolves fully qualified domain names (FQDNs) locally or through configured DNS servers, bypassing the proxy server.

SD-WAN Manager then sends the HTTP or HTTPS connections resulting from the resolution to the proxy server. DNS queries for the resolution of external server FQDNs must be successful before SD-WAN Manager can send the resulting connections to the proxy server for HTTP and HTTPS traffic.

SD-AVC container

There is no support for using the proxy server for traffic between the SD-AVC container, which operates as part of SD-WAN Manager, and external services.

Configure a proxy server for HTTP and HTTPS traffic

Configure a proxy server for HTTP and HTTPS traffic between Cisco SD-WAN Manager and external servers.

SD-WAN Manager verifies that the proxy server for HTTP and HTTPS traffic is reachable, and saves the server details in the configuration database. SD-WAN Manager then directs HTTP and HTTPS connections and REST API calls to external servers through the proxy server.

If the HTTP/HTTPS proxy server is not reachable, Cisco SD-WAN Manager displays an error message on the GUI indicating the reason for failure.

Before you begin

- SD-WAN Manager uses HTTPs connection to *www.cisco.com* (previously, TCP port 7 echo request was used) to validate reachability of the proxy server. Ensure that you configure your firewall and proxy server to allow the echo requests to make the destination host ports accessible.
- Enable out of band interface on single node using **Administration** > **Cluster Management** before configuring proxy server.

Perform these steps to configure a proxy server for HTTP and HTTPS traffic.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Step 2 Open **HTTP/HTTPS Proxy**.

Step 3 For the **Enable HTTP/HTTPS Proxy** setting, click **Enabled**.

Step 4 Enter the **HTTP/HTTPS Proxy IP Address** and **Port** number.

For releases before Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 address. For releases from Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 or IPv6 address.

Step 5 Enter a **Non Proxy Host/IP List** of IP addresses or hostnames to exclude from use with the proxy server.

Use the pipe (|) character to separate items in the list.

Step 6 Click **Save**.

Rate limit for bulk API requests

Describes the rate limit that applies to bulk API requests.

In Cisco vManage Release 20.9.x and earlier releases, you send bulk API requests to a specific node in an SD-WAN Manager cluster. The bulk API throughput is constrained by the rate-limit per node. Increasing the throughput requires sending separate bulk API requests to each node in the cluster and collating the API responses.

From Cisco vManage Release 20.10.1, the method is to send bulk API requests to the SD-WAN Manager cluster. SD-WAN Manager distributes the API requests among the clusters in the node. This distribution increases the rate limit to:

(rate-limit per node) * (number of nodes in the cluster)

This allows you to retrieve more data in a shorter duration compared to a bulk API request addressed to a single node. With the distribution, you need not send separate bulk API requests to two or more nodes in the cluster or collate the API responses.

Configure the rate limit for bulk API requests, using CLI commands

Configure the rate limit for bulk API requests.

Before you begin

Follow these steps to configure the rate limit for bulk API requests.

Procedure

Step 1 Log in to one of the Cisco SD-WAN Manager nodes in the SD-WAN Manager cluster and execute the **request nms server-proxy set ratelimit** command.

```
sdwan-manager# request nms server-proxy set ratelimit
```

Step 2 When prompted with this:

```
Do you want to reconfigure rate limit for URL non bulk api [y/n] :
```

Enter **n**.

Step 3 When prompted with this:

```
Do you want to reconfigure rate limit for URL bulk api /dataservice/data/device/statistics [y/n] :
```

Enter **y**.

Step 4 Enter the per-node rate limit in response to a prompt similar to this:

```
Enter the PER NODE rate limit for URL bulk api /dataservice/data/device/statistics [144 load balanced
 across all nodes at present] :
```

In this example, there is a three-node SD-WAN Manager cluster, with the bulk API rate limit configured to the default value of 48 requests per node. Across all the three nodes, the bulk API rate limit is (rate-limit/node) * 3, which is 144 requests.

Before you enter the rate limit, consider its effect on SD-WAN Manager resources.

Step 5 Enter the unit time for which the rate limit applies in response to a prompt similar to this:

```
Enter the rate limit unit (second, minute, hour, day) for URL bulk api
/dataservice/data/device/statistics [minute] :
```

You can apply a rate limit per second, minute, hour, or day. The default unit is minute.

While SD-WAN Manager applies the rate limit to all the SD-WAN Manager instances in the cluster, the command line displays this message:

```
Propagating rate limit update across all nodes. Please wait.
```

After the rate limit is applied, SD-WAN Manager prompts you to restart the server-proxy on all nodes and the command line returns to the privileged EXEC mode:

```
Done. Please restart server-proxy on all nodes using "request nms server-proxy restart" command.
```

Step 6 Restart the server-proxy using the **request nms server-proxy restart** command.

```
sdwan-manager# request nms server-proxy restart
```

Step 7 Log in to the other SD-WAN Manager nodes in the cluster and restart the server-proxy using the **request nms server-proxy restart** command.

In this example, the bulk API rate limit per node is set to 50 requests per minute.

```
sdwan-manager# request nms server-proxy set ratelimit
Do you want to reconfigure rate limit for URL non bulk api [y/n] : n
Do you want to reconfigure rate limit for URL bulk api /dataservice/data/device/statistics
 [y/n] : y
Enter the PER NODE rate limit for URL bulk api /dataservice/data/device/statistics [144
load balanced across all nodes at present] : 50
Enter the rate limit unit (second, minute, hour, day) for URL bulk api
/dataservice/data/device/statistics [minute] : minute
Propagating rate limit update across all nodes. Please wait.
Done. Please restart server-proxy on all nodes using "request nms server-proxy restart"
command.
vManage# request nms server-proxy restart
```

Configure device statistics collection

Enable or disable the collection of statistics for devices in the fabric. By default, the collection of statistics is enabled for all the devices in the overlay network.

An update in Cisco Catalyst SD-WAN Manager Release 20.16.1 improves the performance of statistics processing, with faster performance and better scalability.

By default, devices enable collecting statistics groups such as Aggregated SAIE and AppHosting.

To delete previously collected data from the statistics database, use the REST API provided in the Cisco Developer Documentation.

Before you begin

Perform these steps to configure device statistics.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Step 2 Open **Statistics Database Configuration**.

For Cisco Catalyst SD-WAN Manager Release 20.12.x or earlier, click **Statistics Setting** and **Edit**.

Step 3 For each statistics group, enable or disable as desired.

To collect statistics exclusively for Cisco SD-WAN Analytics, select the **Analytics only** option for the group.

To enable or disable for specific devices in the network, select the **Custom** option for the group and specify the devices.

Step 4 To apply the modified settings, click **Save**.

Configure the time interval for collecting device statistics

Enable or disable the collection of statistics for devices in the fabric. By default, the collection of statistics is enabled for all the devices in the overlay network.

Before you begin

Perform these steps to configure device statistics.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Step 2 To modify the time interval at which device statistics are collected, click **Statistics Configuration**.

Step 3 Enter the required **Collection Interval** in minutes.

Range: 5 to 180 minutes

Default: 30 minutes

From Cisco Catalyst SD-WAN Manager Release 20.9.6, SD-WAN Manager collects device statistics files at a higher frequency, independent of the configured collection intervals.

Step 4 To apply the modified settings, click **Save**.

Configure the SD-WAN Manager server maintenance window

Before you begin

Perform these steps to set or cancel the start and end times and the duration of the maintenance window for the Cisco SD-WAN Manager server.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Step 2 Click **Maintenance Window**.

If you are using Cisco IOS XE Catalyst SD-WAN Release 17.12.x or earlier, click **Maintenance Window** and then click **Edit**.

To cancel the maintenance window, click **Cancel**.

Step 3 Click the **Start Date** and **Start Time** drop-down list. Select the date and time when the **Maintenance Window** will start.

a) From Cisco Catalyst SD-WAN Manager Release 20.18.x, you can **Select timezone** for the **start time** and **end time**.

The default selected timezone is UTC.

b) Click the **Start Date** and **Start Time** drop-down list. Select the date and time when the **Maintenance Window** will start.

The default start time is 7 days from the configuration date at 00:00.

c) Click the **End Date** and **EndTime** drop-down list. Select the date and time when the **Maintenance Window** will end.

The default end time 6 hours after the start time.

Step 4 From Cisco Catalyst SD-WAN Manager Release 20.18.x, you can set the **Lead Time** (in days) for when the **Pre-Maintenance Alert** message should pop up.

The default **Lead Time** is 2 days.

Step 5 From Cisco Catalyst SD-WAN Manager Release 20.18.x, you can enter banner information text of maximum 256 characters for the **Pre-Maintenance Alert**, which is displayed prior to the maintenance time period.

Step 6 From Cisco Catalyst SD-WAN Manager Release 20.18.x, you can enable the **Active-Maintenance Alert**. Enter banner information text here of maximum 256 characters, which is displayed during the specified maintenance window.

The **Active-Maintenance Alert** is disabled by default.

Note

The banners support HTML hyperlinks including URL-based links and mailto-based email links.

Step 7 Click **Save**. The start and end times and the duration of the maintenance window are displayed in the **Maintenance Window** bar.

Two days before the start of the window, the Cisco SD-WAN Manager Dashboard displays a maintenance window alert notification.

Configure system logging using CLI commands

Configure system logging using CLI commands in a CLI add-on profile or CLI add-on template.

Before you begin

Perform these steps to configure system logging using CLI commands.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Configure system logging.

```
config-transaction [IP address | description | alarm | buffered | buginf | console | discriminator
 esm | event | facility | file | history | host | origin-id | persistent | rate-limit | snmp-authfail
 | snmp-trap | source-interface
 trap | userinfo]
```

Connect to a device by SSH terminal

Establish an SSH session with a device.

Before you begin

Perform these steps to establish an SSH session with a device.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Tools** > **SSH Terminal**.

Step 2 Select a device.

Step 3 Enter credentials to log in to the device.

You can execute CLI commands to monitor or configure the device.

View the rate limit for bulk API requests

View the rate limit for bulk API requests.

Procedure

To view the bulk API rate limit, log in to any node in the Cisco SD-WAN Manager cluster and use the **show nms server-proxy ratelimit** command.

This sample output is from three-node SD-WAN Manager cluster with the bulk API rate limit per node configured to 50 requests per minute. Therefore, the bulk API rate limit for the cluster is 50*3 = 150 requests per minute.

```
sdwan-manager# show nms server-proxy ratelimit
Non Bulk API: 100/second (per node)
Bulk API: 150/minute (across cluster)
```

Monitor NAT DIA endpoint trackers

Describes how to monitor the NAT DIA endpoint tracker configuration.

Configure NAT DIA endpoint trackers using Configure device basic settings using a configuration group, on page 195 or Configure device basic system settings using templates, on page 198.

Before you begin

Follow these steps to monitor the NAT DIA endpoint tracker configuration.

Procedure

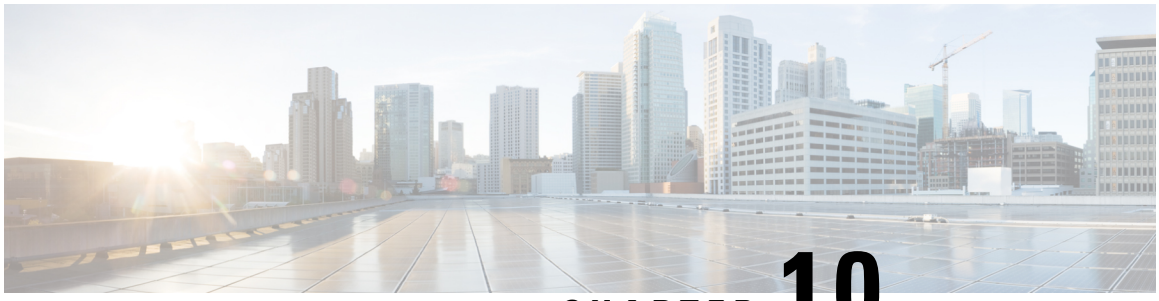
Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

Step 2 Select a device from the list of devices.

Step 3 Click **Real Time**.

Step 4 From the **Device Options** drop-down list, choose **Endpoint Tracker Info**.



CHAPTER 10

VPN

- VPN, on page 231
- Configure VPN, on page 233
- Verify the VPN configuration, on page 252

VPN

A VPN template in Cisco Catalyst SD-WAN is a configuration template that

- enables the creation of separate feature templates for each VPN, and
- supports configuration of VPN 0 and VPN 512 on all device types, with additional VPN templates for segmenting service-side user networks on Cisco IOS XE Catalyst SD-WAN devices.

Types of VPNs

The types of VPNs in Cisco Catalyst SD-WAN include:

- **VPN 0—Transport VPN**, which carries control traffic via the configured WAN transport interfaces. Initially, VPN 0 contains all of a device's interfaces except for the management interface, and all interfaces are disabled.
- **VPN 512—Management VPN**, which carries out-of-band network management traffic among the Cisco IOS XE Catalyst SD-WAN devices in the overlay network. The interface used for management traffic resides in VPN 512. By default, VPN 512 is configured and enabled on all Cisco IOS XE Catalyst SD-WAN devices. For controller devices, by default, VPN 512 is not configured.
- **VPNs 1–511, 513–65530—Service VPNs**, for service-side data traffic on Cisco IOS XE Catalyst SD-WAN devices.

You create a separate VPN feature template for each VPN. For example, create one feature template for VPN 0, a second for VPN 1, and a third for VPN 512.

Interfaces in the WAN Transport VPN

A VPN 0 is a WAN transport VPN that

- handles all control plane traffic carried over OMP sessions in the overlay network,

- requires at least one interface configured in VPN 0 for a Cisco IOS XE Catalyst SD-WAN device to participate in the overlay network, and
- mandates that at least one interface connects to a WAN transport network, such as the Internet or an MPLS or a metro Ethernet network.

Tunnel interface configurations

The WAN transport interface, known as a tunnel interface, is configured in VPN 0.

To configure a tunnel interface on a Cisco SD-WAN Controller or a Cisco SD-WAN Manager, you must create an interface in VPN 0, assign an IP address (static or via DHCP), enable the interface with the **no shutdown** command, and mark it as a tunnel interface.

The IP address can be either IPv4 or IPv6. To enable dual stack, configure both address types. Optionally, you can associate a color with the tunnel.



Note You can configure IPv6 addresses only on transport interfaces in VPN 0. Configuring IPv6 addresses is not supported in VPN 512.

On Cisco IOS XE Catalyst SD-WAN devices, tunnel interfaces must have an IP address, a color, and an encapsulation type. For releases before Cisco IOS XE Catalyst SD-WAN Release 17.3.2, dual stack is enabled by configuring both IPv4 and IPv6 addresses. Starting from Release 17.3.2, only one address type is supported per TLOC or interface. Using a second address type requires a second TLOC or interface on which it can be provisioned.

On Cisco Catalyst SD-WAN Controllers and Controller NMSs, interface names can be either ethnumber or loopbacknumber, and only VPN 0 and VPN 512 are supported for interface configuration.

On Cisco SD-WAN Controller and Cisco SD-WAN Manager, *interface-name* can be either **eth** *number* or **loopback** *number*, and only VPN 0 and VPN 512 are supported for interface configuration. Hence, all interfaces are present only on these VPNs.

Dual stack configuration

To use dual stack with Cisco IOS XE Catalyst SD-WAN devices from Cisco IOS XE Catalyst SD-WAN Release 17.3.2, configure all controllers with both IPv4 and IPv6 addresses. In addition, configure DNS for the Cisco SD-WAN Validator interface to resolve IPv4 and IPv6 address types so that controllers can reach the Cisco SD-WAN Validator through either IP address type.

Starting from Cisco vManage Release 20.6.1, in case of a dual-stack configuration, if an IPv4 address or the fully qualified domain name (FQDN) is not available, but an IPv6 address is available, then the IPv6 address is used to connect to the Cisco SD-WAN Validator.

Interfaces in the Management

VPN 512 is a default out-of-band management VPN that

- is included as part of the factory-default configuration for out-of-band management, and
- is converted to VRF Mgmt-Intf on Cisco IOS XE Catalyst SD-WAN devices, which use VRFs in place of VPNs.

VPN 512 is local to the device and not advertised in the overlay. If you need a management VPN that is reachable through the overlay, create a VPN with a number other than 512.

Configure VPN

Use one of these methods to configure VPN parameters:

- Configuration group
- Feature template
- CLI commands

Configure VPN using configuration groups

Configure transport VPN using a configuration group

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure a Transport VPN feature in Transport and Management profile.

a) Enter the basic configuration information.

Table 58: Basic Configuration

Field	Description
VPN	Enter the numeric identifier of the VPN.
Enhance ECMP Keying	Enable the use in the ECMP hash key of Layer 4 source and destination ports, in addition to the combination of the source IP address, destination IP address, protocol, and DSCP field, as the ECMP hash key. Default: Disabled

b) Enter DNS information.

Table 59: DNS

Field	Description
Add DNS	
Primary DNS Address (IPv4)	Enter the IP address of the primary IPv4 DNS server in this VPN.
Secondary DNS Address (IPv4)	Enter the IP address of a secondary IPv4 DNS server in this VPN.

Field	Description
Add DNS IPv6	
Primary DNS Address (IPv6)	Enter the IP address of the primary IPv6 DNS server in this VPN.
Secondary DNS Address (IPv6)	Enter the IP address of a secondary IPv6 DNS server in this VPN.

c) Enter host happing information.

Table 60: Host Mapping

Field	Description
Add New Host Mapping	
Hostname*	Enter the hostname of the DNS server. The name can be up to 128 characters.
List of IP*	Enter up to 14 IP addresses to associate with the hostname. Separate the entries with commas.

Step 3 Configure the following parameters based on the features you choose to configure on your network.

a) Enter the route details.

Table 61: Route

Field	Description
Add IPv4 Static Route	
Network address*	Enter the IPv4 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv4 static route to configure in the VPN.
Subnet Mask*	Enter the subnet mask.
Gateway*	Choose one of the following options to configure the next hop to reach the static route: • **nextHop**: When you choose this option and click **Add Next Hop**, the following fields appear: • **Address***: Enter the next-hop IPv4 address. • **Administrative distance***: Enter the administrative distance for the route. • **dhcp** • **null0**: When you choose this option, the following field appears: • **Administrative distance**: Enter the administrative distance for the route.
Add IPv6 Static Route	

Field	Description
Prefix*	Enter the IPv6 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv6 static route to configure in the VPN.
Next Hop/Null 0/NAT	Choose one of the following options to configure the next hop to reach the static route: • **Next Hop**: When you choose this option and click **Add Next Hop**, the following fields appear: • **Address***: Enter the next-hop IPv6 address. **Administrative distance***: Enter the administrative distance for the route. • **Null 0**: When you choose this option, the following field appears: • **IPv6 Route Null 0***: Enable this option to set the next hop to be the null interface. All packets sent to this interface are dropped without sending any ICMP messages. • **NAT**: When you choose this option, the following field appears: • **IPv6 NAT***: Choose NAT64 or NAT66.
Add BGP Routing	Choose a BGP route.

b) Enter the NAT details

Table 62: NAT

Field	Description
Add NAT64 v4 Pool	
NAT64 v4 Pool Name*	Enter a NAT pool number configured in the centralized data policy. The NAT pool name must be unique across VPNs and VRFs. You can configure up to 31 (1–32) NAT pools per router.
NAT64 Pool Range Start*	Enter a starting IP address for the NAT pool.
NAT64 Pool Range End*	Enter a closing IP address for the NAT pool.
NAT64 Overload	Enable this option to configure per-port translation. If this option is disabled, only dynamic NAT is configured on the end device. Per-port NAT is not configured. Default: Disabled

c) Enter the service information.

Table 63: Service

Field	Description
Add Service	
Service Type	Choose the service available in the VPN. Value: **TE**

What to do next

Also see Deploy a Configuration Group.

Configure management VPN using a configuration group

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure a Management VPN feature in Transport and Management profile.

a) Enter the basic configuration information.

Table 64: Basic Configuration

Field	Description
VPN	Management VPN carries out-of-band network management traffic among the Cisco IOS XE Catalyst SD-WAN devices in the overlay network. The interface used for management traffic resides in VPN 512. By default, VPN 512 is configured and enabled on all Cisco IOS XE Catalyst SD-WAN devices.
Name	Enter a name for the interface.

b) Enter DNS information.

Table 65: DNS

Field	Description
Add DNS	
Primary DNS Address (IPv4)	Enter the IPv4 address of the primary DNS server in this VPN.
Secondary DNS Address (IPv4)	Enter the IPv4 address of a secondary DNS server in this VPN.
Add DNS IPv6	

Field	Description
Primary DNS Address (IPv6)	Enter the IPv6 address of the primary DNS server in this VPN.
Secondary DNS Address (IPv6)	Enter the IPv6 address of a secondary DNS server in this VPN.

c) Enter host happing information.

Table 66: Host Mapping

Field	Description
Add New Host Mapping	
Hostname*	Enter the hostname of the DNS server. The name can be up to 128 characters.
List of IP Address*	Enter IP addresses to associate with the hostname. Separate the entries with commas.

d) Enter the IPv4/IPv6 static route information.

Table 67: IPv4/IPv6 Static Route

Field	Description
Add IPv4 Static Route	
IP Address*	Enter the IPv4 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv4 static route to configure in the VPN.
Subnet Mask*	Enter the subnet mask.
Gateway*	Choose one of the following options to configure the next hop to reach the static route: • **nextHop**: When you choose this option and click **Add Next Hop**, the following fields appear: • **Address***: Enter the next-hop IPv4 address. • **Administrative distance***: Enter the administrative distance for the route. • **dhcp** • **null0**: When you choose this option, the following field appears: • **Administrative distance**: Enter the administrative distance for the route.
Add IPv6 Static Route	
Prefix*	Enter the IPv6 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv6 static route to configure in the VPN.

Field	Description
Next Hop/Null 0/NAT	Choose one of the following options to configure the next hop to reach the static route: • **Next Hop**: When you choose this option and click **Add Next Hop**, the following fields appear: • **Address***: Enter the next-hop IPv6 address. **Administrative distance***: Enter the administrative distance for the route. • **Null 0**: When you choose this option, the following field appears: • **NULL0***: Enable this option to set the next hop to be the null interface. All packets sent to this interface are dropped without sending any ICMP messages. • **NAT**: When you choose this option, the following field appears: • **IPv6 NAT**: Choose NAT64 or NAT66.

What to do next

Also see Deploy a Configuration Group.

Configure service VPN using a configuration group

This section helps you configure a service VPN (range 1 – 65527, except 512) or the LAN VPN.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure Service VPN in a Service profile.

a) Enter the basic configuration information.

Table 68: Basic Configuration

Field	Description
VPN*	Enter the numeric identifier of the VPN.
Name*	Enter a name for the VPN.

Field	Description
OMP Admin Distance IPv4	Administrative distance for OMP routes. The Cisco SD-WAN Controllers learn the topology of the overlay network and the services available in the network using OMP routes. The distance can be a value between 1–255.
OMP Admin Distance IPv6	Administrative distance for OMP routes. The Cisco SD-WAN Controllers learn the topology of the overlay network and the services available in the network using OMP routes. The distance can be a value between 1–255.

b) Enter DNS information.

Table 69: DNS

Field	Description
Add DNS IPv4	
Primary DNS Address (IPv4)	Enter the IP address of the primary IPv4 DNS server in this VPN.
Secondary DNS Address (IPv4)	Enter the IP address of a secondary IPv4 DNS server in this VPN.
Add DNS IPv6	
Primary DNS Address (IPv6)	Enter the IP address of the primary IPv6 DNS server in this VPN.
Secondary DNS Address (IPv6)	Enter the IP address of a secondary IPv6 DNS server in this VPN.

c) Enter host happing information.

Table 70: Host Mapping

Field	Description
Add New Host Mapping	
Hostname*	Enter the hostname of the DNS server. The name can be up to 128 characters.
List of IP*	Enter up to eight IP addresses to associate with the hostname. Separate the entries with commas.

Step 3 Configure the following parameters based on the features you choose to configure on your network.

a) Enter advertise OMP information.

Table 71: Advertise OMP

Field	Description
Add OMP Advertise IPv4	

Field	Description
Protocol	Choose a protocol to configure route advertisements to OMP, for this VPN: • **bgp** • **ospf** • **ospfv3** • **connected** • **static** • **network** • **aggregate** **Applied to Region**: (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) In a Multi-Region Fabric scenario, route aggregation is a method for reducing the number of entries that routers in a network must maintain in routing tables, for better scaling. Choose **core**, **access**, or **core-and-access**, to apply route aggregation only to access regions, the core region, or both. This option is applicable only to a Multi-Region Fabric border router, not an edge router or a transport gateway. • **eigrp** • **lisp** • **isis**
Select Route Policy	Enter the name of the route policy. Route policy is not supported in Cisco vManage Release 20.9.1.
Add OMP Advertise IPv6	

Field	Description
Protocol	**Note** Advertising IPv6 OMP routes as network statements is not supported. This applies when using the Service VPN feature in a configuration group, and applies also when using a Cisco VPN feature template. You can configure to advertise: • IPv6 routes by BGP and OSPF protocols • Connected routes, static routes, and aggregate routes The reason for the lack of support is that the Service VPN feature and the Cisco VPN feature template both use the **advertise network** *prefix* command, which does not fully support IPv6 addresses. Choose a protocol to configure route advertisements to OMP, for this VPN: • **BGP** • **OSPF** • **Connected** • **Static** • **Network** • **Aggregate** **Applied to Region**: (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) In a Multi-Region Fabric scenario, route aggregation is a method for reducing the number of entries that routers in a network must maintain in routing tables, for better scaling. Choose **core**, **access**, or **core-and-access**, to apply route aggregation only to access regions, the core region, or both. This option is applicable only to a Multi-Region Fabric border router, not an edge router or a transport gateway.
Select Route Policy	Enter the name of the route policy. Route policy is not supported in Cisco vManage Release 20.9.1.
Protocol Sub Type	When you choose the OSPF protocol, specify the sub type as external.

b) Enter route information.

Table 72: Route

Field	Description
Add IPv4 Static Route	
Network Address*	Enter the IPv4 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv4 static route to configure in the VPN.

Field	Description
Subnet Mask*	Enter the subnet mask.
Next Hop/Null 0/VPN/DHCP	Choose one of the following options to configure the next hop to reach the static route: • **Next Hop**: When you choose this option, the **IPv4 Route Gateway Next Hop** field appears. Enable this option to add the next hop. You can add a hop with and without a tracker. When you click **Add Next Hop**, the following fields appear: • **Address***: Enter the next-hop IPv4 address. • **Administrative Distance***: Enter the administrative distance for the route. When you click **Add Next Hop with Tracker**, the following fields appear: • **Address***: Enter the next-hop IPv4 address. • **Administrative Distance***: Enter the administrative distance for the route. • **Tracker***: Enter the name of the gateway tracker to determine whether the next hop is reachable before adding that route to the route table of the device. • **Null 0**: When you choose this option, the following field appears: • **IPv4 Route Null 0***: Enable this option to set the next hop to be the null interface. All packets sent to this interface are dropped without sending any ICMP messages. • **VPN**: When you choose this option, the following field appears: • **IPv4 Route VPN***: Selects VPN as the gateway to direct packets to the transport VPN. • **DHCP**: When you choose this option, the following field appears: • **IPv4 Route Gateway DHCP***: Assigns a static route for the default next-hop router when the DHCP server is accessed for an IP address.
Add BGP Routing	Choose a BGP route.
Add OSPF Routing	Choose an OSPF route.
Add IPv6 Static Route	
Prefix*	Enter the IPv6 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv6 static route to configure in the VPN.

Field	Description
Next Hop/Null 0/NAT	Choose one of the following options to configure the next hop to reach the static route: • **Next Hop**: When you choose this option and click **Add Next Hop**, the following fields appear: • **Address***: Enter the next-hop IPv6 address. • **Administrative distance***: Enter the administrative distance for the route. • **Null 0**: When you choose this option, the following field appears: • **IPv6 Route Null 0***: Enable this option to set the next hop to be the null interface. All packets sent to this interface are dropped without sending any ICMP messages. • **NAT**: When you choose this option, the following field appears: • **IPv6 NAT***: Choose NAT64 or NAT66. • **Interface**: When you choose this option, the following fields appear: • **Interface Name**: Choose IPv6 interface name for the IPsec tunnel. • **Next Hop**: Enter the IPv6 address and the administrative distance for the next hop.

c) Enter service information.

Table 73: Service

Field	Description
Add Service	
Service Type	Choose a service available at the local site and in the VPN. Values: **FW**, **IDS**, **IDP**, **netsvc1**, **netsvc2**, **netsvc3**, **netsvc4**, **TE**, **SIG**
IPv4 Addresses (Maximum: 4)*	Enter up to four IP address, separated by commas. The service is advertised to the Cisco SD-WAN Controller only if one of the addresses can be resolved locally, at the local site, not via routes learned through OMP. You can configure up to four IP addresses.
Tracking*	Cisco Catalyst SD-WAN tests each service device periodically to check whether it is operational. Tracking saves the results of the periodic tests in a service log. Tracking is enabled by default.

d) Enter service route information.

Table 74: Service Route

Field	Description
Add Service Route	
Prefix*	Enter the IP address or prefix. For Umbrella SIG, use any RFC 1918 subnet for Service IP addresses.
Service*	Configure routes pointing to any service. Values: **FW**, **IDS**, **IDP**, **netsvc1**, **netsvc2**, **netsvc3**, **netsvc4**.
VPN*	Destination VPN to resolve the prefix.

e) Enter GRE route information.

Table 75: GRE Route

Field	Description
Add GRE Route	
Prefix*	Enter the IP address or prefix, in decimal four-part-dotted notation, and prefix length of the GRE-specific static route.
Interface*	Enter the name of one or two GRE tunnels to use to reach the service.
VPN*	Enter the number of the VPN to reach the service. This must be VPN 0.

f) Enter IPSEC route information.

Table 76: IPSEC Route

Field	Description
Add ipSec Route	
Prefix*	Enter the IP address or prefix, in decimal four-part-dotted notation, and prefix length of the IPsec-specific static route.
Interface*	Enter the name of one or two IPsec tunnel interfaces. If you configure two interfaces, the first is the primary IPsec tunnel, and the second is the backup. All packets are sent only to the primary tunnel. If that tunnel fails, all packets are then sent to the secondary tunnel. If the primary tunnel comes back up, all traffic is moved back to the primary IPsec tunnel.

g) Enter NAT information.

Table 77: NAT

Field	Description
Nat Pool	

Field	Description
NatPool Name*	Enter a NAT pool number configured in the centralized data policy. The NAT pool name must be unique across VPNs and VRFs. You can configure up to 31 (1–32) NAT pools per router.
Prefix Length*	Enter the NAT pool prefix length.
Range Start*	Enter a starting IP address for the NAT pool.
Range End*	Enter a closing IP address for the NAT pool.
Overload*	Enable this option to configure per-port translation. If this option is disabled, only dynamic NAT is configured on the end device. Per-port NAT is not configured. Default: Enabled
Direction*	Choose the NAT direction.
Nat64 V4 Pool	
Nat64 V4 Pool Name*	Enter a NAT pool number configured in the centralized data policy. The NAT pool name must be unique across VPNs and VRFs. You can configure up to 31 (1–32) NAT pools per router.
Nat 64 V4 Pool Range Start*	Enter a starting IP address for the NAT pool.
Nat 64 V4 Pool Range End*	Enter a closing IP address for the NAT pool.
Overload*	Enable this option to configure per-port translation. If this option is disabled, only dynamic NAT is configured on the end device. Per-port NAT is not configured. Default: Disabled

h) Enter route leak information.

Table 78: Route leak from Global VPN

Field	Description
Route Protocol*	Choose a protocol to configure leak routes from global VPN to the service VPN that you are configuring: • **static** • **connected** • **bgp** • **ospf**
Select Route Policy	Choose a route policy from the drop-down list.
Redistribution (in service VPN)	

Field	Description
Protocol*	Choose a protocol from the available options to redistribute the leaked routes: • **bgp** • **ospf** • (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1) **eigrp**
Select Route Policy	Choose a route policy from the drop-down list.

Table 79: Route leak to Global VPN

Field	Description
Route Protocol*	Choose a protocol to leak routes from the service VPN that you are configuring to the global VPN: • **static** • **connected** • **bgp** • **ospf** • (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1) **eigrp**
Select Route Policy	Choose a route policy from the drop-down list.
Redistribution (in global VPN)	
Protocol*	Choose a protocol from the available options to redistribute the leaked routes: • **bgp** • **ospf**
Select Route Policy	Enter the name of the route policy.
Select Route Policy	Choose a route policy from the drop-down list.

Table 80: Route leak between services

Field	Description
Source VPN	Enter a value of the source VPN.

Field	Description
Route Protocol*	Choose a protocol from the available options to leak routes from the source service VPN to the service VPN that you are configuring: • **static** • **connected** • **bgp** • **ospf** • (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1) **eigrp**
Select Route Policy	Choose a route policy from the drop-down list.
Redistribution (in Service VPN)	
Protocol*	Choose a protocol from the available options to redistribute the leaked routes: • **bgp** • **ospf** • (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1) **eigrp**
Select Route Policy	Choose a route policy from the drop-down list.

i) Enter route target information.

Table 81: Route Target

Field	Description
IPv4 Settings	
Import Route Target List: Route Target*	Configure a route target for IPv4 interfaces. It imports routing information from the target VPN extended community.
Export Route Target List: Route Target*	Configure a route target for IPv4 interfaces. It exports routing information to the target VPN extended community.
IPv6 Settings	
Import Route Target List: Route Target*	Configure a route target for IPv6 interfaces. It imports routing information from the target VPN extended community.

Field	Description
Export Route Target List: Route Target*	Configure a route target for IPv6 interfaces. It exports routing information to the target VPN extended community.

What to do next

Also see Deploy a Configuration Group.

Configure VPN using templates

Cisco IOS XE Catalyst SD-WAN devices use VRFs for segmentation and network isolation. However, the following steps still apply if you are configuring segmentation for Cisco IOS XE Catalyst SD-WAN devices through Cisco SD-WAN Manager. When you complete the configuration, the system automatically converts the VPNs to VRFs for Cisco IOS XE Catalyst SD-WAN devices.

You can configure a static route through the VPN template.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Device Templates**, and click **Create Template**.

In Cisco vManage Release 20.7.x and earlier releases **Device Templates** is called **Device**.

Step 3 From the **Create Template** drop-down list, choose **From Feature Template**.

Step 4 From the **Device Model** drop-down list, choose the type of device for which you wish to create the template.

Step 5 To create a template for VPN 0 or VPN 512:

a) Click **Transport & Management VPN**, or scroll to the **Transport & Management VPN** section.

b) From the VPN 0 or VPN 512 drop-down list, click **Create Template**. The VPN template form appears.

The form contains fields for naming the template, and fields for defining VPN parameters.

Step 6 To create a template for VPNs 1 through 511, and 513 through 65527:

a) Click **Service VPN**, or scroll to the **Service VPN** section.

b) Click the **Service VPN** drop-down list.

c) From the **VPN** drop-down list, click **Create Template**. The VPN template form displays.

The form contains fields for naming the template, and fields for defining VPN parameters.

Step 7 In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

Step 8 In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

Step 9 Configure the VPN template parameters.

a) Configure basic VPN parameters.

Parameter Name	Description
VPN	Enter the numeric identifier of the VPN. Range for Cisco IOS XE Catalyst SD-WAN devices: 0 through 65527 Values for Cisco SD-WAN Controller and Cisco SD-WAN Manager devices: 0, 512
Name	Enter a name for the VPN. **Note** For Cisco IOS XE Catalyst SD-WAN devices, you can't enter a device-specific name for the VPN.
Enhance ECMP keying	Click **On** to enable the use in the ECMP hash key of Layer 4 source and destination ports, in addition to the combination of the source, and destination IP addresses, as the ECMP hash key. ECMP keying is **Off** by default.
OMP Admin Distance (IPv4)	To configure a site to prefer the OMP route over the leaked route path, configure the IPv4 address with a lower administrative distance than the leaked route. You can apply the configuration at the global level or at the specific VRF level by choosing **Global** or **Device Specific** respectively. Range: 1-251
OMP Admin Distance (IPv6)	To configure a site to prefer the OMP route over the leaked route path, configure the IPv6 address with a lower administrative distance than the leaked route. You can apply the configuration at the global level or at the specific VRF level by choosing **Global** or **Device Specific** respectively. Range: 1-251

Note
To complete the configuration of the transport VPN on a router, you must configure at least one interface in VPN 0.

b) Configure DNS addresses and static hostname mapping.

Parameter Name	Options	Description
Primary DNS Address	Click either **IPv4** or **IPv6**, and enter the IP address of the primary DNS server in this VPN.	

Parameter Name	Options	Description
New DNS Address	Click **New DNS Address** and enter the IP address of a secondary DNS server in this VPN. This field appears only if you have specified a primary DNS address.	
	Mark as Optional Row	Check the **Mark as Optional Row** check box to mark this configuration as device-specific. To include this configuration for a device, enter the requested variable values when you attach a device template to a device, or create a template variables spreadsheet to apply the variables.
	Hostname	Enter the hostname of the DNS server. The name can be up to 128 characters.
	List of IP Addresses	Enter up to eight IP addresses to associate with the hostname. Separate the entries with commas.
To save the DNS server configuration, click **Add**.		

Configure VPN parameters using CLI commands

Configure load-balancing algorithm using CLI commands

From Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, you need CLI template to configure the **src-only** load-sharing algorithm for IPv4 and IPv6 Cisco Catalyst SD-WAN and non Cisco Catalyst SD-WAN traffic. For complete details on the load-sharing algorithm CLI, see IP Commands list.

Follow these steps to configure load-balancing algorithm using CLI commands:

Procedure

Step 1 Select a Cisco Express Forwarding load-balancing algorithm for non Cisco Catalyst SD-WAN IPv4 and IPv6 traffic.

Example:

```
Device# config-transaction
Device(config)# ip cef load-sharing algorithm {universal [id] | include-ports [ source [id] |
destination [id]] |
src-only [id]}

Device# config-transaction
Device(config)# ipv6 cef load-sharing algorithm {universal [id] | include-ports [ source [id] |
destination [id]] |
src-only [id]}
```

Step 2 Enable load balancing algorithm on an interface for Cisco Catalyst SD-WAN IPv4 and IPv6 traffic.

Example:

```
Device# config-transaction
Device(config)# sdwan
Device(config-sdwan)# ip load-sharing algorithm {ip-and-ports | src-dst-ip | src-ip-only}
```

```
Device# config-transaction
Device(config)# sdwan
Device(config-sdwan)# ipv6 load-sharing algorithm {ip-and-ports | src-dst-ip | src-ip-only}
```

Map host names to IP addresses using CLI commands

Perform this task to associate host names with IP addresses.

A name server is used to keep track of information associated with domain names. A name server can maintain a database of host name-to-address mappings. Each name can map to one or more IP addresses. In order to use this service to map domain names to IP addresses, you must specify a name server.

Procedure

Step 1 Define a static host name-to-address mapping in the host name cache.

Example:

```
Device(config)# ip host cisco-rtp 192.168.0.148
```

Step 2 Define a default domain name that Cisco Catalyst SD-WAN can use to complete unqualified host names.

Example:

```
Device(config)# ip domain name cisco.com
```

Step 3 Specify one or more hosts that supply name information.

Example:

```
Device(config)# ip name-server 172.16.1.111 172.16.1.2
```

Step 4 Enable DNS-based address translation.

DNS is enabled by default. Use this command if DNS has been disabled.

Example:

```
Device(config)# ip domain lookup
```

The following example configures the host-name-to-address mapping process. IP DNS-based translation is specified, the addresses of the name servers are specified, and the default domain name is given.

```
! IP DNS-based host name-to-address translation is enabled
  ip domain lookup
! Specifies hosts 192.168.1.111 and 192.168.1.2 as name servers
  ip name-server 192.168.1.111 192.168.1.2
! Defines cisco.com as the default domain name the device uses to complete
! Set the name for unqualified host names
  ip domain name cisco.com
```

Verify the VPN configuration

This section provides examples for VPN configurations.

Use the **show sdwan running-config | sec vrf definition Mgmt-intf** command to verify the management interface configurations.

```
Device# show sdwan running-config | sec vrf definition Mgmt-intf

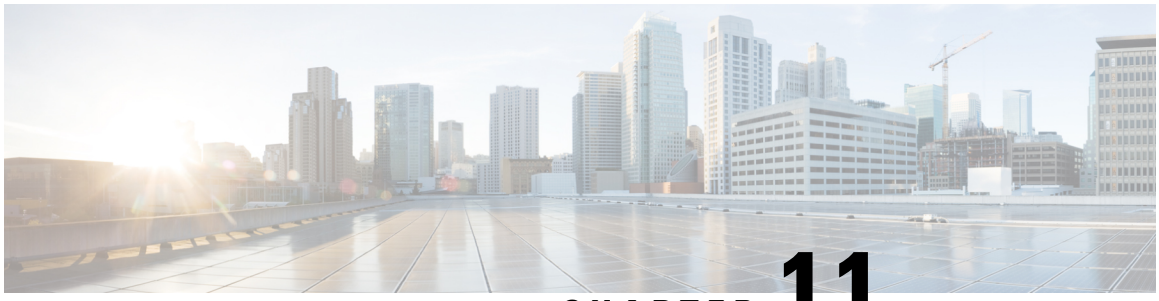
vrf definition Mgmt-intf
 address-family ipv4
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
============
interface GigabitEthernet0
 no shutdown
 vrf forwarding Mgmt-intf
 negotiation auto
exit
============
config-t
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0

vrf definition Mgmt-intf
 rd 1:512
 !
 address-family ipv4
  route-target export 1:512
  route-target import 1:512
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
!
interface GigabitEthernet1
 vrf forwarding Mgmt-intf
 ip address 192.168.20.11 255.255.255.0
!
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0
!
```

To display information about the configured management interfaces, use the **show interface** command.

```
Device# show interface gigabitEthernet0
GigabitEthernet0 is up, line protocol is up
  Hardware is RP management port, address is d478.9bfe.9f7f (bia d478.9bfe.9f7f)
  Internet address is 10.34.9.177/16
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 1000Mbps, link type is auto, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
```

```
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 8000 bits/sec, 12 packets/sec
5 minute output rate 1000 bits/sec, 2 packets/sec
   4839793 packets input, 415574814 bytes, 0 no buffer
   Received 3060073 broadcasts (0 IP multicasts)
   0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   0 watchdog, 0 multicast, 0 pause input
   82246 packets output, 41970224 bytes, 0 underruns
   Output 0 broadcasts (0 IP multicasts)
   0 output errors, 0 collisions, 0 interface resets
   0 unknown protocol drops
   0 babbles, 0 late collision, 0 deferred
   0 lost carrier, 0 no carrier, 0 pause output
   0 output buffer failures, 0 output buffers swapped out
```



CHAPTER 11

TLOC

- TLOC, on page 255
- System IP address, on page 256
- Color, on page 257
- Encapsulation, on page 257

TLOC

A TLOC (Transport Locator) is a unique identifier in Cisco Catalyst SD-WAN that

- represents a WAN Edge device's connection to a WAN transport, and
- is defined by the combination of its system IP address, a color indicating the type of transport, and an encapsulation type.

Components of TLOC

A TLOC is made up of three components:

- System IP address: The unique IP address of the SD-WAN device.
- Color: A Cisco Catalyst SD-WAN software construct that identifies the transport tunnel.
- Encapsulation: The method used to encapsulate the overlay tunnel data.

Tunnel interface

A tunnel interface in Cisco Catalyst SD-WAN is a network connection that you configure for secure data transport. On a Cisco SD-WAN Controller or Cisco SD-WAN Manager, you can configure one tunnel interface. On a Cisco IOS XE Catalyst SD-WAN device, you can configure up to eight tunnel interfaces.

To limit the remote TLOCs that the local TLOC can establish BFD sessions with, mark the TLOC with the **restrict** option. When a TLOC is marked as restricted, a TLOC on the local router establishes tunnel connections with a remote TLOC only if the remote TLOC has the same color.

When a WAN edge device is configured with two IPv6 TLOCs, one with static default route and the other one with IPv6 address autoconfig default which is the IPv6 neighbor discovery default route, the IPv6 neighbor discovery default route is not installed in the routing table. In this case, the IPv6 TLOC with IPv6 neighbor discovery default route does not work.

For IPv6 TLOC with IPv6 neighbor discovery default route to work, you can configure the static route for TLOC with IPv6 neighbor discovery to overwrite the IPv6 neighbor discovery default route and ensure that both the static routes are installed into the routing table. You can also use the IPv6 neighbor discovery default route on all interfaces.

A tunnel interface allows only DTLS, TLS, and, for Cisco IOS XE Catalyst SD-WAN devices, IPsec traffic to pass through the tunnel. To allow additional traffic to pass without having to create explicit policies or access lists, enable them by including one **allow-service** command for each service. You can also explicitly disallow services by including the **no allow-service** command. Note that services affect only physical interfaces.

STUN server

In Cisco Catalyst SD-WAN, Session Traversal Utilities for NAT (STUN) is a protocol used by Cisco IOS XE Catalyst SD-WAN devices to discover their public IP address and port assigned by a Network Address Translator (NAT).

Use the **allow-service stun** command to enable or disable a Cisco IOS XE Catalyst SD-WAN device from sending requests to a generic STUN server. This allows the device to determine if it is behind a NAT, identify the NAT type, and discover its public IP address and port number. On a Cisco IOS XE Catalyst SD-WAN device that is behind a NAT, you can also configure a tunnel interface to obtain its public IP address and port number from the Cisco SD-WAN Validator.

When you configure the Cisco IOS XE Catalyst SD-WAN device to use the Cisco SD-WAN Validator as a STUN server, the device determines its public IP address and public port number, which enables it to establish TLOC connections and form the overlay fabric over various public transports like broadband or cellular networks. However, the device cannot identify the type of NAT it is behind in this setup. The tunnel interface configured for the Cisco SD-WAN Validator does not carry overlay network control traffic or exchange encryption keys, but BFD establishes connectivity and allows data traffic. Because this tunnel does not support control traffic, you must configure at least one additional tunnel interface to ensure the device can exchange control traffic with the Cisco SD-WAN Controller and Cisco SD-WAN Manager.

You can log the headers of all packets that the system drops because they do not match a service configured with an **allow-service** command. You can use these logs for security purposes, for example, to monitor the flows that are being directed to a WAN interface and to determine, in the case of a DDoS attack, which IP addresses to block.

System IP address

A system interface IP address is a persistent address that

- identifies the Cisco IOS XE Catalyst SD-WAN device,
- is similar to a router ID on a regular router, and
- is used to identify the router from which packets originated.

System IP address configuration

You configure a system interface for each Cisco IOS XE Catalyst SD-WAN device using the **system system-ip** command. Specify the system IP address as an IPv4 address in decimal four-part dotted notation, without including the prefix length; the /32 prefix is implicit. The system IP address must not be within the following ranges: 0.0.0.0/8, 127.0.0.0/8, 224.0.0.0/4, or 240.0.0.0/4 and later. Assign a unique system IP address to each device in the overlay network. You cannot assign this address to another interface in VPN 0.

The system interface is placed in VPN 0 as a loopback interface named **system**. This loopback is not the same as a loopback address that you configure for a specific interface. To display information about the system interface, use the **show interface** command.

Role in OMP TLOC identification

The system IP address is used as one of the attributes of the OMP TLOC (Overlay Management Protocol Transport Locator). Each TLOC is uniquely identified by a 3-tuple: the system IP address, a color, and an encapsulation. Use the **show omp tlocs** command to display TLOC information.

Device management

For device management, configure the same system IP address on a loopback interface located in a service-side VPN appropriate for management purposes. Use a loopback interface because it remains reachable whenever the router is operational and the overlay network is up. Avoid configuring the system IP address on a physical interface, since both the router and the interface must be up for reachability in that case.

Assign the loopback interface to a service-side VPN, which is any VPN other than VPN 0 (the WAN transport VPN) or VPN 512 (the management VPN). Service-side VPNs are used to route data traffic and remain reachable from the data center.

Color

A color is a Cisco Catalyst SD-WAN software construct that

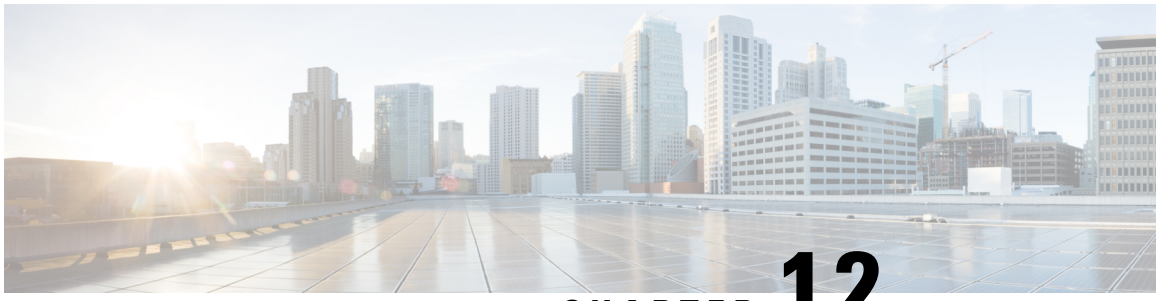
- identifies the transport tunnel,
- includes options such as **3g**, **biz-internet**, **blue**, **bronze**, **custom1**, **custom2**, **custom3**, **default**, **gold**, **green**, **lte**, **metro-ethernet**, **mpls**, **private1** through **private6**, **public-internet**, **red**, and **silver**, and
- designates **metro-ethernet**, **mpls**, and **private1** through **private6** as private colors that use private addresses for private networks, which can be used on public networks only if there is no NAT device between the local and remote Cisco IOS XE Catalyst SD-WAN devices.

Encapsulation

An encapsulation is a required configuration on Cisco IOS XE Catalyst SD-WAN devices that

- specifies the tunnel encapsulation type as either IPsec or GRE, and
- sets the default MTU to 1442 bytes for IPsec and 1468 bytes for GRE, which is enabled by default on all TLOCs, based on BFD path MTU discovery.

You can configure both IPsec and GRE encapsulation by including two **encapsulation** commands under the same **tunnel-interface** command. On the remote Cisco IOS XE Catalyst SD-WAN device, you must configure the same tunnel encapsulation type or types so that the two routers can exchange data traffic. Data transmitted out of an IPsec tunnel can be received only by an IPsec tunnel, and data sent on a GRE tunnel can be received only by a GRE tunnel. The Cisco Catalyst SD-WAN software automatically selects the correct tunnel on the destination Cisco IOS XE Catalyst SD-WAN device.



CHAPTER 12

TLOC Extension

- Feature history for TLOC extension, on page 259
- TLOC extension, on page 259
- How TLOC extension over IPv6 works, on page 261
- Configure TLOC extension using CLI commands, on page 262
- Verify TLOC extension, on page 263

Feature history for TLOC extension

Table 82: Feature History

Feature Name	Release Information	Description
TLOC Extension Over IPv6	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature enables the support of TLOC extension for IPv6. In the previous releases, TLOC extension was supported only for IPv4.

TLOC extension

A TLOC Extension is a Cisco Catalyst SD-WAN feature that

- enables a device to access the opposite WAN transport connected to a neighboring device using a TLOC extension interface, and
- addresses scenarios where devices cannot connect directly to a single transport and only one device can connect to each transport.

Benefits of TLOC extension

There are scenarios when Cisco IOS XE Catalyst SD-WAN devices cannot connect to a single transport directly and only one device can connect to a single transport. A switch is connected to each transport and the devices connect to each transport through the switches. TLOC extension provides the following benefits:

- Eliminates the need for additional switches at branch locations.
- Reduces overall solution costs and simplifies network management.

TLOC extension over IPv6

From Cisco IOS XE Catalyst SD-WAN Release 17.11.1a TLOC extension over IPv6 works only if the underlay supports IPv6 addressing on both the Cisco IOS XE Catalyst SD-WAN devices connecting each other.

In the earlier releases, TLOC extension was supported only over IPv4 interfaces.

Supported configurations

This feature supports the following requirements:

- Implicit IPv6 ACL on TLOC tunnel interface.
- Private and public color TLOC interfaces.
- Dual stack support. When both IPv4 and IPv6 are configured, the tunnel is built on top of either IPv4 or IPv6, based on the configuration.
- NAT66 support. The limitations of NAT66 also applies to the TLOC extended interface.
- Only the Layer 2 setup supports IPv6 TLOC extension. The following interface types supports IPv6 TLOC extension:
  - Physical interface
  - Physical sub-interface
  - Loopback interface
- Loopback TLOC interface that is bound to either:
  - The WAN transport circuit.
  - An extended WAN interface between two Cisco IOS XE Catalyst SD-WAN devices.

Limitations for TLOC extension over IPv6

SIG

Secure Internet Gateway (SIG) is not supported on TLOC extension over IPv6.

NAT64

NAT64 is not supported for TLOC extension over IPv6.

Layer 3 Connectivity

TLOC extension over IPv6 is not supported for Layer 3 connections.

Control connection persistence

When a TLOC configuration is extended to a peer interface and then to the internet service provider, the extended control connections remain active on the peer interface even after the TLOC extension configuration is removed.

Extender interface configuration

In TLOC extension, the extender interface is part of the Cisco Catalyst SD-WAN. However, configuring a tunnel-interface under the extender interface is optional.

How TLOC extension over IPv6 works

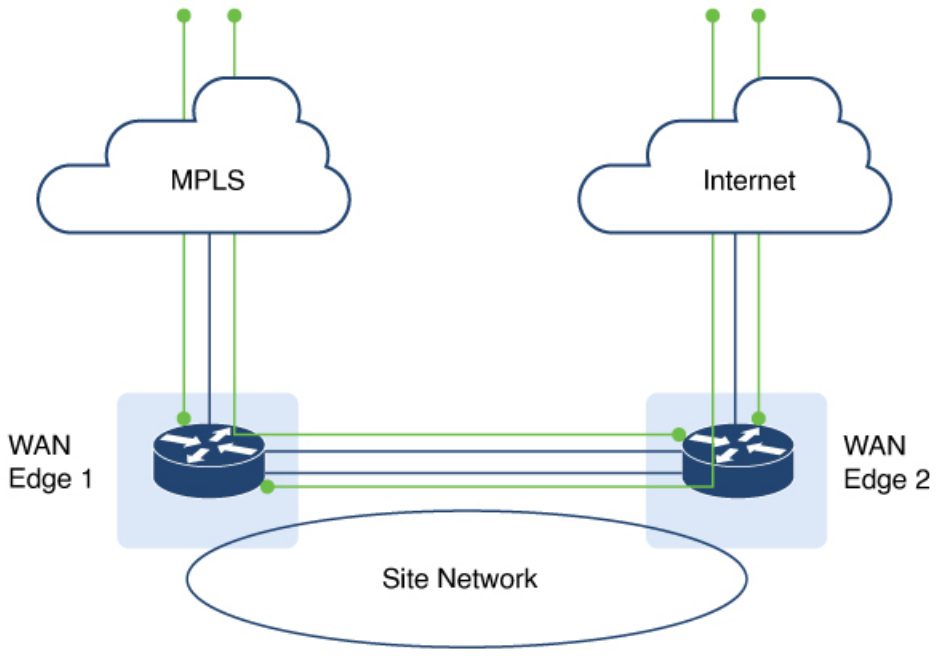
Summary

The key components involved in TLOC extension over IPv6 are:

- Establish TLOC extension interfaces: Each Cisco IOS XE Catalyst SD-WAN device configures a TLOC-extension interface to enable access to the transport network of its neighboring SD-WAN device.
- Access opposite transport via neighbor.

Workflow

Figure 1: TLOC extension



This process outlines how TLOC extension interfaces facilitate transport access and redundancy between two Cisco IOS XE Catalyst SD-WAN devices.

1. SD-WAN device 1 accesses the internet transport through the TLOC-extension interface on SD-WAN device 2, in addition to its direct MPLS connection.

2. SD-WAN device 2 accesses the MPLS transport through the TLOC-extension interface on SD-WAN device 1, in addition to its direct internet connection.

Result

TLOC extension over IPv6 achieves redundancy in a dual-device deployment scenario with only one circuit connection on each device.

Configure TLOC extension using CLI commands

Follow these steps to configure TLOC extension using CLI commands:

Procedure

Step 1 Enter global configuration mode, and configure an interface.

Example:

```
Device# config-transaction
```

Step 2 Enter SD-WAN configuration mode.

Example:

```
Device(config)# sdwan
```

Step 3 in the SD-WAN configuration mode, configure an interface type such as, Gigabit Ethernet.

Example:

```
Device(config-sdwan)# interface GigabitEthernet3
```

Step 4 Configure tunnel interface.

Example:

```
Device(config-interface-GigabitEthernet3)# tunnel-interface
```

Step 5 Configure encapsulation, color, allowed services for TLOC.

Example:

```
Device(config-interface-GigabitEthernet3)# tunnel-interface
Device(config-interface-GigabitEthernet3)# encapsulation ipsec
Device(config-interface-GigabitEthernet3)# color color
Device(config-interface-GigabitEthernet3)# exit
```

Step 6 In the global configuration mode, configure an interface.

Example:

```
Device# config-transaction
Device(config)# ip route 0.0.0.0 0.0.0.0 ip-address
```

Step 7 On device 2, the LTE WAN connection is on GigabitEthernet1 and this transport is extended to device 1 GigabitEthernet3 TLOC interface.

Example:

```
Device(config-sdwan)# tloc-extension GigabitEthernet1
```

Step 8 Configure NAT routes on GigabitEthernet1 for data traffic to reach back to device 1 through device 2 for GigabitEthernet3 subnet.

The following example describes how TLOC extension is configured on a network interface.

```
On Device1,
Configure TLOC interface on VPN 0
sdwan
interface GigabitEthernet3
  tunnel-interface
   encapsulation ipsec
   color custom1
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   no allow-service snmp
   no allow-service bfd
  exit

  Configure default route via this TLOC interface with nexthop
  to L2 connected interface of the peer (ED2 Gig3).

  ip route 0.0.0.0 0.0.0.0 10.1.19.16

 On Device2,
LTE WAN connection is on Gig1 and this transport is extended to ED1 Gig3 TLOC
interface(custom1).
 sdwan
 int GigabitEthernet3
 tloc-extension GigabitEthernet1
Configure NAT routes on Gig1 or appropriate routes for data traffic to reach back to ED1
via ED2 for Gig3 subnet.
```

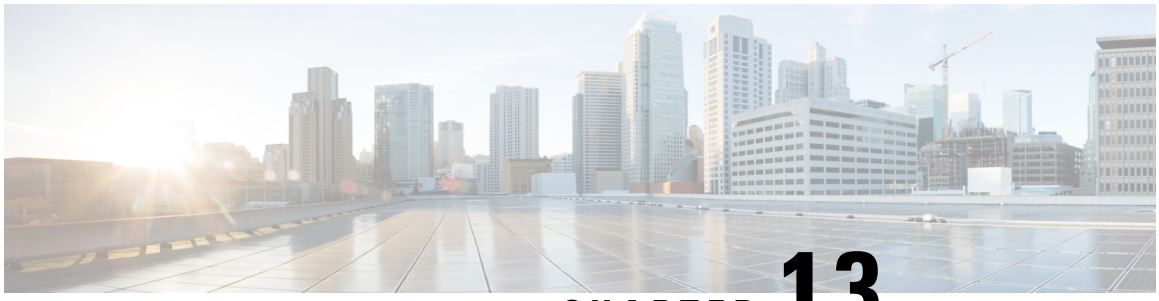
Verify TLOC extension

The following is a sample output of the commands to verify if TLOC extension is configured on a network interface.

```
Device# show sdwan control connections
PEER                                            PEER
  CONTROLLER
PEER    PEER PEER            SITE       DOMAIN PEER                                    PRIV
  PEER
PUB                                             GROUP
TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP                              PORT
```

```
  PUBLIC IP
PORT  ORGANIZATION            LOCAL COLOR     PROXY STATE UPTIME      ID
-------------------------------------------------------------------------------------------------------
vsmart  dtls 172.16.255.19   100        1      2001:a0:5::13
12455 2001:a0:5::13                          12455 vIPtela Inc Regression  custom1
      No    up
0:01:23:06 0
vsmart  dtls 172.16.255.20   200        1      2001:a0:c::14                           12456
2001:a0:c::14                            12456 vIPtela Inc Regression  custom1
No    up
0:01:23:06 0


Device# show sdwan bfd sessions
                                       SOURCE TLOC      REMOTE TLOC
DST PUBLIC                        DST PUBLIC         DETECT      TX
  SYSTEM IP        SITE ID     STATE       COLOR            COLOR            SOURCE IP
IP                                          PORT        ENCAP  MULTIPLIER  INTERVAL(msec
  UPTIME
TRANSITIONS
-------------------------------------------------------------------------------------------------------
172.16.255.14    400         up          custom1            lte             2001:a0:15::10
2001:a1:e::e                               12346       ipsec  7           1000
0:00:05:50  3
```



CHAPTER 13

Network Hierarchy Management

- Feature history for network hierarchy management, on page 265
- Network hierarchy management, on page 266
- Benefits of network hierarchy, on page 267
- Supported devices for network hierarchy, on page 267
- Restrictions for network hierarchy, on page 267
- Manage a network hierarchy, on page 268

Feature history for network hierarchy management

Table 83: Feature History

Feature Name	Release Information	Description
Network Hierarchy	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	This feature enables you to create a network hierarchy in Cisco SD-WAN Manager to represent the geographical locations of your network. The network hierarchy and the associated resource IDs, including region IDs and site IDs, help you apply configuration settings to a device. In addition, the introduction of the resource manager in Cisco SD-WAN Manager automatically manages these resource IDs, thereby simplifying the overall user experience of Cisco Catalyst SD-WAN. Note that you can create a region only if you enable the **Multi-Region Fabric** option in Cisco SD-WAN Manager. You can create a network hierarchy in Cisco SD-WAN Manager to represent the geographical locations of your network. You can create a region, an area, and a site in a network hierarchy. In addition, you can assign a site ID and a region ID to a device.

Feature Name	Release Information	Description
Network Hierarchy Enhancement	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco vManage Release 20.10.1	The following enhancements are introduced in the Network Hierarchy and Resource Management feature. • Creation of a system IP pool on the **Configuration** > **Network Hierarchy** page • Automatic assignment of site ID, system IP, and hostname to a device in the Quick Connect workflow • Display of detailed information on the **Configuration** > **Network Hierarchy** page, including site ID pool, region ID pool, and the list of devices associated with a site You can create a system IP pool on the **Configuration** > **Network Hierarchy** page.
Support for Software Defined Remote Access Pools	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	Remote access refers to enabling secure access to an organization's network from devices at remote locations. The resource pool manager manages the IPv4 and IPv6 private IP address pools for Cisco Catalyst SD-WAN remote access devices. You can create a software defined remote access pool using the **Configuration** > **Network Hierarchy** page.
Support for Traffic Flow Collectors	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	This feature enables you to configure traffic flow collectors such as the Cflowd server and security logging server. Cflowd monitors service side traffic flowing through devices in the overlay network and exports flow information to the collector. Enable security logging and configure servers for high-speed logging (HSL) and collecting external syslogs. You can configure the traffic flow collectors by navigating to **Configuration** > **Network Hierarchy** > **Collectors**.
End of Support for Secondary Regions and Subregions	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	This release ends support for secondary regions and subregions.

Network hierarchy management

A network hierarchy is a logical framework in Cisco SD-WAN Manager that

- organizes network nodes into geographical or logical groupings,
- assigns resource IDs to each node to assist with configuration management, and

- establishes a predetermined multi-level structure supporting regions, areas, and sites.

By default, there is one node called global in the network hierarchy. The network hierarchy has a predetermined hierarchy with three types of nodes.

- A region is a top-level node in a multiregion fabric-based Cisco Catalyst SD-WAN deployment. Regions segment the SD-WAN overlay into distinct networks and require the Multi-Region Fabric feature to be enabled.

  You can create a region only if you enable the **Multi-Region Fabric** option in Cisco SD-WAN Manager. For complete information about the Multi-Region Fabric feature, see the *Cisco Catalyst SD-WAN Multi-Region Fabric (also Hierarchical SD-WAN) Configuration Guide*.

- Group (Area): An area, also called a group, is a logical grouping of nodes such as sites, regions, or other areas. Areas allow flexible organization of network locations within the hierarchy.
- Site: A site is the lowest-level node in the hierarchy. Sites represent specific network locations and can be associated with network devices. Child nodes cannot be created under a site.
- By default, the hierarchy includes a single global node.
- Resource IDs assigned to nodes help determine where to apply configuration settings in Cisco SD-WAN Manager.
- To create or manage nodes in a network hierarchy, see "Manage a Network Hierarchy" in the product documentation.

Benefits of network hierarchy

These are the benefits of network hierarchy.

- Automates the management of regions and sites.
- Saves the manual effort in an upgrade scenario when Cisco SD-WAN Manager discovers all your existing sites and displays them in the network hierarchy.
- Simplifies the onboarding and configuration of devices.
- Monitors and collects information about traffic flow.

Supported devices for network hierarchy

This feature is supported on Cisco IOS XE Catalyst SD-WAN devices.

Restrictions for network hierarchy

These are the restrictions for network hierarchy.

- You can delete a node only if it does not have any child node. For example, you can delete a site only if no devices are associated with it.

- A site is the lowest level of a node or the leaf node in a network hierarchy. You cannot create a child node under a site.
- You cannot create more than one region node between the global node and a site node.
- You cannot create a region in a multitenant deployment.
- The maximum combined number of regions and secondary regions is 63 (region ID numbers 1 through 63).

Manage a network hierarchy

Create a region in a network hierarchy

Use these steps to create a Region for Cisco Catalyst SD-WAN Manager Release 20.12.1 and earlier.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
2. Click **…** adjacent to a node (global or area) in the left pane and choose **Add MRF Region**.

Note You can also use the **Add Node** option to add a region.

3. In the **Name** field, enter a name for the region. The name must be unique and can contain only letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.).
4. In the **Description** field, enter a description of the region.
5. From the **Parent** drop-down list, choose a parent node.
6. Click **Add**.

(For Cisco Catalyst SD-WAN Manager Release 20.12.1 or earlier) Ensure that the **Multi-Region Fabric** option in Cisco SD-WAN Manager is enabled. See Enable Multi-Region Fabric in the *Cisco Catalyst SD-WAN Multi-Region Fabric Configuration Guide*.

From Cisco Catalyst SD-WAN Manager Release 20.13.1, configuring regions is enabled by default. It does not require enabling Multi-Region Fabric. Use these steps to create a Region for Cisco Catalyst SD-WAN Manager Release 20.13.1 and later.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.

Step 2 Click **…** adjacent to **Global** in the left pane and choose **Add Node**.

Step 3 Do one of the following:

- If Multi-Region Fabric is not enabled:

  In the **Add Node** pop-up window, check the **Behave as SDWAN Region** checkbox.

If you do not check this checkbox, this procedure creates a new group within the network hierarchy instead of a region.

- If Multi-Region Fabric is enabled:

  In the **Add Node** pop-up window, choose **Region**.

Step 4 Configure the following:

Field	Description
Name	Name for the region. The name must be unique and can contain only letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.).
Description	Description of the region.
Parent drop-down list	Choose a parent node.

Step 5 Click **Add**.

The new region appears in the left pane.

Step 6 (Optional) You can click a region name or a secondary region name in the left pane to display the automatically assigned region ID number. The region ID number appears above the table in the right pane. The maximum combined number of regions and secondary regions is 63 (region ID numbers 1 through 63).

Create a subregion in a network hierarchy

From Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Control Components Release 20.15.1, configuration of this feature is supported only through API.

Before you begin

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1

- From Cisco Catalyst SD-WAN Manager Release 20.13.1, configuring subregions is enabled by default. It does not require enabling Multi-Region Fabric.
- Create a region before creating a subregion. See Create a Region in a Network Hierarchy section.
- For the maximum combined number of regions and secondary regions, see Restrictions for Network Hierarchy and Resource Management.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.

Step 2 Click **…** adjacent to a region in the left pane and choose **Add MRF Sub Region**.

Step 3 In the **Add Sub-Region** pop-up window, configure the following:

Field	Description
Name	Name for the region. The name must be unique and can contain only letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.).
Description	Description of the region.
Parent	This field is automatically populated with the region to which you are adding the subregion, and is not configurable.

Step 4 Click **Add**. The new subregion appears in the left pane..

Create a secondary region in a network hierarchy



Note From Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Control Components Release 20.15.1 and , configuration of this feature is supported only through API.

Before you begin

- Create a region before creating a subregion.
- For the maximum combined number of regions and secondary regions.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.

Step 2 Click **…** adjacent to **Global** in the left pane and choose **Add Node**.

Step 3 In the **Add Node** pop-up window, click **Secondary Region**.

Step 4 Configure the following:

Field	Description
Name	Name for the region. The name must be unique and can contain only letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.).
Description	Description of the region.
Parent	This field shows **Secondary Regions**, and is not configurable.

Step 5 Click **Add**.

The new secondary region appears in the left pane, in the **Secondary Regions** section.

Step 6 (Optional) You can click a region name or a secondary region name in the left pane to display the automatically assigned region ID number. The region ID number appears above the table in the right pane. The maximum combined number of regions and secondary regions is 63 (region ID numbers 1 through 63).

Create a group in a network hierarchy

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.

Step 2 Click **…** adjacent to a node (global, region, or group) in the left pane and choose **Add Node.**

Step 3 In the **Add Node** pop-up window, in the **Type** field, choose **Group**.

Step 4 In the **Name** field, enter a name for the group. The name must be unique and can contain only letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.).

Step 5 In the **Description** field, enter a description of the group.

Step 6 From the **Parent** drop-down list, choose a parent node.

Step 7 Click **Add**.

Create a site in a network hierarchy

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.

Step 2 Click **…** adjacent to a node (global, region, or area) in the left pane and choose **Add Site**.

Step 3 In the **Name** field, enter a name for the site. The name must be unique and can contain only letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.).

Step 4 In the **Description** field, enter a description of the site.

Step 5 From the **Parent** drop-down list, choose a parent node.

Step 6 In the **Site ID** field, enter a site ID.

If you do not enter the site ID, Cisco SD-WAN Manager generates a site ID for the site.

Step 7 In the **Address** field, enter the address.

When you enter an address, latitude and longitude fields are auto populated.

Step 8 n the **Latitude** and **Longitude** fields, enter the latitude longitude values of the site.

Step 9 Click **Add**.

Use the following table to enter the fields.

Field	Description
Name	Enter a name for the site. The name must be unique and can contain only letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.).
Description	Enter a description of the site.
Parent	From the drop-down list, choose a parent node.
Site ID	Enter a site ID. If you do not enter the site ID, Cisco SD-WAN Manager generates a site ID for the site.
Address	Enter the address. When you enter an address, latitude and longitude fields are auto populated.
Latitude	Specifies latitude of the site. When you enter the latitude of the site, the address field is auto populated if the location of the site is found.
Longitude	Specifies longitude of the site. When you enter the longitude of the site, the address field is auto populated if the location of the site is found.

Note
The **Address** , **Latitude**, and **Longitude** fields are included starting from Cisco IOS XE Catalyst SD-WAN Release 17.18.1a. When you type in the address, the latitude and longitude fields are auto-populated.

Conversely, you can also enter your own latitude and longitude. If a corresponding location is found, then the address field will be auto-populated. If you do not want to provide address data for your site, then you can check the **Undisclosed Address** check box.

Edit a WAN region

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
Step 2 Click **…** adjacent to the region name and choose **Edit WAN Region**.
Step 3 Edit the options as needed. You can edit the name, description, and parent of the region.
Step 4 Click **Save**.

Delete a WAN region

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
Step 2 Click **…** adjacent to the region name and choose **Delete WAN Region**.
Step 3 In the confirmation dialog box, click **Yes**.

Edit a group

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
Step 2 Click **…** adjacent to the group name and choose **Edit Group**.
Step 3 Edit the options as needed. You can edit the name, description, and parent of the group.
Step 4 Click **Save**.

Delete a group

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
Step 2 Click **…** adjacent to the group name and choose **Delete Group**.
Step 3 In the confirmation dialog box, click **Yes**.

Edit a site

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
Step 2 Click **…** adjacent to the site name and choose **Edit Site**.
Step 3 Edit the options as needed. You can edit only the name, description, and parent of the site.

Step 4 Click **Save**.

What to do next

Note After reassigning a site to a different region in the **Network Hierarchy Manager**, follow the procedures in **Assign a site ID to a device** and **Assign a region ID to a device** sections in the Resource Management section to ensure configuration updates are properly applied to the affected device.

Delete a site

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
Step 2 Click **…** adjacent to the site name and choose **Delete Site**.
Step 3 In the confirmation dialog box, click **Yes**.

Create a system IP pool

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.

The page displays the site pool and region pool for the Global node.

Step 2 Click **Pools**.
Step 3 Click **Add Pool**.
Step 4 In the **Pool Name** field, enter a name for the pool.
Step 5 In the **Pool Description** field, enter a description of the pool.
Step 6 From the **Pool Type** drop-down list, choose **System IP**.
Step 7 In the **IP Subnet*** field, enter an IP address.
Step 8 In the **Prefix Length*** field, enter the prefix length of the system IP pool.
Step 9 Click **Add**.

Note
You can create only one system IP pool. If you want to make any changes to the pool, you must edit the existing pool.

Edit a system IP pool

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.

The page displays the site pool and region pool for the Global node. The system IP pool is also displayed if you have already created it.

Step 2 Click **…** adjacent to the system IP name and choose **Edit**.

Step 3 Edit the options as needed.

Note
You can only expand the pool range and cannot enter a lower IP address than the already specified IP address.

Step 4 Click **Save**.

Create a remote access pool

The resource pool manager supports creation of IPv4 and IPv6 private IP pools for Cisco Catalyst SD-WAN remote access devices. In the remote access configuration you can select the remote access private IP Pool by defining the number of IP addresses.

For more information on Software Defined Remote Access, see Cisco Catalyst SD-WAN Remote Access.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.

The page displays the site pool and region pool for the Global node.

Step 2 Click **Add Pool**.

Step 3 In the **Pool Name** field, enter a name for the pool.

Step 4 In the **Pool Description** field, enter a description of the pool.

Step 5 From the **Pool Type** drop-down list, choose **Remote Access**.

Step 6 Choose the **IP Type** by clicking the radio button next to **IPv4** or **IPv6**.

Step 7 In the **IP Subnet** field, enter an IP subnet.

Step 8 In the **Prefix Length** field, enter the prefix length of the remote access pool.

Step 9 Click **Add**.

Edit a remote access pool

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**

The page displays the site pool and region pool for the Global node. The remote access pool is also displayed if you have already created it.

Step 2 Click **…** adjacent to the remote access pool name and choose **Edit**.

Step 3 Edit the options as needed.

Note
When you edit a remote access pool, the new pool range cannot be less than the existing pool range

Step 4 Click **Save**.

Create an IP pool for ThousandEyes

Procedure

Step 1 From the menu, choose **Configuration** > **Network Hierarchy**. The page displays the site pool and region pool for the Global node.

Step 2 Examine the audit logs to determine if the ThousandEyes test has been posted or failed.

Step 3 Click **Pools** and click **Add Pool**.

Step 4 In the **Pool Name** field, enter a name for the pool.

Step 5 In the **Pool Description** field, enter a description of the pool.

Step 6 From the **Pool Type** drop-down list, choose **ThousadEyes**.

Step 7 In the **IP Subnet*** field, enter an IP address.

Step 8 In the **Prefix Length*** field, enter the prefix length of the system IP pool.

Step 9 Click **Add**.

Delete a pool

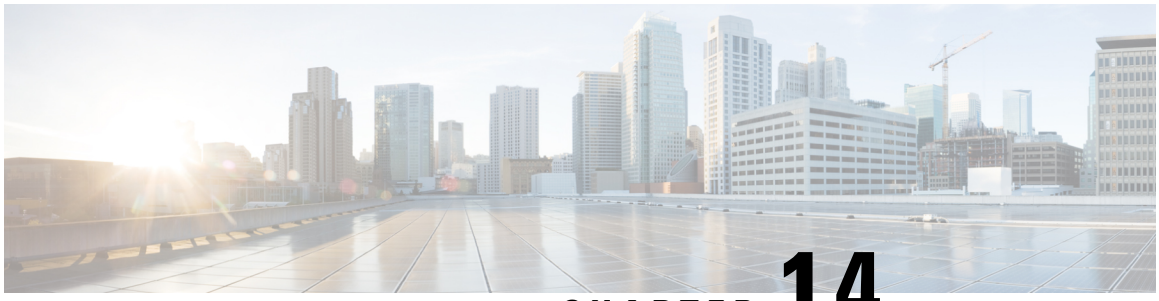
Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.

Step 2 In the Global page, click **…** adjacent to the pool name and choose **Delete**.

Step 3 In the confirmation dialog box, click **Yes**.

Note
You can delete a pool only when the pool resources are not in use.



CHAPTER 14

Resource Management and Collectors in a Network Hierarchy

- Feature history of resource management and collectors, on page 279
- Resource management and collectors, on page 280
- Assign resource IDs to devices, on page 281
- Assign a region ID to a device, on page 282
- Assign a system IP to a device, on page 283
- Assign a hostname to a device, on page 283
- Configure cflowd, on page 284
- Configure security logging, on page 285

Feature history of resource management and collectors

Table 84: Feature History

Feature Name	Release Information	Description
Resource Management	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	This feature enables you to create a network hierarchy in Cisco SD-WAN Manager to represent the geographical locations of your network. The network hierarchy and the associated resource IDs, including region IDs and site IDs, help you apply configuration settings to a device. In addition, the introduction of the resource manager in Cisco SD-WAN Manager automatically manages these resource IDs, thereby simplifying the overall user experience of Cisco Catalyst SD-WAN. You can create a network hierarchy in Cisco SD-WAN Manager to represent the geographical locations of your network. You can create a region, an area, and a site in a network hierarchy. In addition, you can assign a site ID and a region ID to a device.

Feature Name	Release Information	Description
Resource Management Enhancement	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	The following enhancements are introduced in the Resource Management feature. • Creation of a system IP pool on the **Configuration** > **Network Hierarchy** page • Automatic assignment of site ID, system IP, and hostname to a device in the Quick Connect workflow • Display of detailed information on the **Configuration** > **Network Hierarchy** page, including site ID pool, region ID pool, and the list of devices associated with a site
Support for Traffic Flow Collectors	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	This feature enables you to configure traffic flow collectors such as the Cflowd server and security logging server. Cflowd monitors service side traffic flowing through devices in the overlay network and exports flow information to the collector. Enable security logging and configure servers for high-speed logging (HSL) and collecting external syslogs. You can configure the traffic flow collectors by navigating to **Configuration** > **Network Hierarchy** > **Collectors**.

Resource management and collectors

The resource manager in Cisco SD-WAN Manager manages resource IDs, which include region IDs and site IDs. The resource manager automatically generates a region ID when you create a region on the **Configuration** > **Network Hierarchy** page. Similarly, it generates a site ID for a site if you do not specify it. You can assign a site ID and a region ID to a device.

When you upgrade from an earlier version of Cisco SD-WAN Manager to Cisco vManage Release 20.9.1, the resource manager automatically creates sites based on the site IDs of your devices. Each site is named SITE_. The sites appear under the global node on the **Configuration** > **Network Hierarchy** page, and Cisco SD-WAN Manager associates each device with its site in the network hierarchy.

Collectors

Collectors process traffic that flows through routers in the overlay network and export flow information to a server. They maintain flow data extracted from the IP headers of packets within the traffic.

You can configure the location of cflowd collectors and set how frequently sampled flows are sent to the collectors. The samples are sent to the collectors at specific intervals. You can configure a maximum of four cflowd collectors per Cisco IOS XE Catalyst SD-WAN device. To have a cflowd configuration take effect, apply it with the appropriate data policy.

Assign resource IDs to devices

The resource management feature enables you to assign site ID, region ID, system IP, and host names to a device.

Assign a site ID to a device using the quick connect workflow

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.

Step 2 Start the **Quick Connect** workflow.

Step 3 Follow the instructions provided in the workflow.

Step 4 On the **Add and Review Device Configuration** page, enter the site ID of the device.

Note

- You can use any of the existing site IDs that are available in the network hierarchy or enter a new site ID. If you enter a new site ID without creating a node in the network hierarchy, the site is automatically created and listed on the **Configuration** > **Network Hierarchy** page.
- If you want Cisco SD-WAN Manager to automatically generate a site ID for the device, do not make any change to the default value, **AUTO**.

Assign a site ID to a device using a template

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **WAN Edge List**.

Step 2 Check if a device is attached to a device template.

Step 3 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Feature Templates**.

Step 4 Click **…** adjacent to the System feature template and choose **Edit**.

Step 5 Click the **Basic Configuration** tab and set the scope of the **Site ID** field to **Global** and enter the site ID.

If you set the scope of the **Site ID** field to **Device Specific**, do the following:

a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Device Templates**.

b. Click **…** adjacent to the device template and choose **Edit Device Template**.

c. In the **Site ID** field, enter the site ID.

You can use any of the existing site IDs that are available in the network hierarchy or enter a new site ID. If you enter a new site ID without creating a node in the network hierarchy, the site is automatically created and listed on the **Configuration** > **Network Hierarchy** page.

d. Click **Update**.

e. Click **Configure Devices** to push the configuration to the device.

Step 6 Click **Update**.

Step 7 Click **Configure Devices** to push the configuration to the device.

Assign a site ID to a device using a configuration group

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Configuration Groups**.

Step 2 Click **…** adjacent to the configuration group name and choose **Edit**.

Step 3 Click **Associated Devices**.

Step 4 Choose a device that is associated with the configuration group and click **Deploy**.

The **Deploy Configuration Group** workflow starts.

Step 5 Follow the instructions provided in the workflow.

Step 6 On the **Add and Review Device Configuration** page, enter the site ID of the device.

You can use any of the existing site IDs that are available in the network hierarchy or enter a new site ID. If you enter a new site ID without creating a node in the network hierarchy, the site is automatically created and listed on the **Configuration** > **Network Hierarchy** page.

Assign a region ID to a device

Before you begin

- Have access to the **Multi-Region Fabric** feature.
- Ensure that the region is available in the network hierarchy.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **WAN Edge List**.

Step 2 Check if the corresponding device is attached to a device template.

Step 3 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Feature Templates**.

Step 4 Click **…** adjacent to the System feature template and choose **Edit**.

Step 5 Click the **Basic Configuration** tab and set the scope of the **Region ID** field to **Global** and enter the region ID.

You can use any of the existing region IDs that are available in the network hierarchy. If the specified region ID is not available in the network hierarchy, the template push operation to the devices fails.

If you set the scope of the **Region ID** field to **Device Specific**, do the following:

a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Device Templates**.

b. Click **…** adjacent to the device template and choose **Edit Device Template**.

c. In the **Region ID** field, enter the region ID.

d. Click **Update**.

e. Click **Configure Devices** to push the configuration to the device.

Step 6 Click **Update**.

Step 7 Click **Configure Devices** to push the configuration to the device.

Assign a system IP to a device

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.

Step 2 Start the **Quick Connect** workflow.

Step 3 Follow the instructions provided in the workflow.

Step 4 On the **Add and Review Device Configuration** page, enter the system IP of the device. If you want Cisco SD-WAN Manager to automatically generate a system IP for the device, do not make any change to the default value, **AUTO**.

Assign a hostname to a device

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.

Step 2 Start the **Quick Connect** workflow.

Step 3 Follow the instructions provided in the workflow.

Step 4 On the **Add and Review Device Configuration** page, enter the hostname of the device. If you want Cisco SD-WAN Manager to automatically generate a hostname for the device, do not make any change to the default value, **AUTO**.

Configure cflowd

Before you begin

You can configure the location of cflowd collectors, how often sets of sampled flows are sent to the collectors, and how often the samples are sent to the collectors (on Cisco SD-WAN Controllers only). You can configure a maximum of four cflowd collectors per Cisco IOS XE Catalyst SD-WAN device. To have a cflowd configuration take effect, apply it with the appropriate data policy.

Ensure that you specify the granular role-based access control (RBAC) for Cflowd and policy groups. With specific permissions to the user group, ensure that you are able to access policy groups from **Configuration** > **Policy Groups**. For more information about configuring RBAC for policy groups, see Configure RBAC for policy groups in Prerequisites for Policy Groups.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Users and Access** > **Roles**.
2. Click **Edit** next to existing roles or click **Add Role** to create a new role.
3. Choose the desired permission for the **Cflowd** feature under **Network Settings** and click **Update**.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy** > **Collectors**.

Step 2 Enable Cflowd and configure the values in the following table for the collector server:

Field	Description
Add Collector Server	
VPN ID	VPN ID of the server. Range: 0 through 65536
IPv4/IPv6 Address	IPv4 or IPv6 address of the collector server.
UDP Port	UDP port number of the collector server. Range: 1024 through 65535
Export Spreading	Toggle to enable or disable the export spreading configuration.
BFD Metrics Exporting	Toggle to enable or disable Bidirectional Forwarding Detection (BFD) metrics.
Exporting Interval	Interval in seconds for sending BFD metrics. **Exporting Interval** appears if you have enabled **BFD Metrics Exporting**. The default BFD export interval is 600 seconds.
Advanced Settings	

Field	Description
Active Flow Timeout (Seconds)	Active flow timeout value. Range: 30 through 3600 Default: 600 seconds.
Inactive Flow Timeout (Seconds)	Inactive flow timeout value. Range: 1 through 3600 Default: 60 seconds.
Flow Refresh Time (Seconds)	Flow refresh time in seconds. Range: 60 through 86400 seconds. Default: 600 seconds.
Sampling Rate	Sample duration in seconds. Range: 1 through 65536. Default: 1 second.
Collect TLOC Loopback	Enable to collect information about the TLOC loopback.
Protocol	Traffic protocol type to apply the collector to. The options are: **IPv4**, **IPv6**, or **both**. The default protocol is **IPv4**.
TOS	Type of field in the IPv4 header.
Re-marked DSCP	Traffic output of the router's data policy.

You can configure up to four collector servers.

Step 3 Click **Save**.

The Cflowd settings that you configure are applied to the application priority and SLA policy when the policy is deployed to Cisco IOS XE Catalyst SD-WAN devices. You can monitor application traffic flow over IPv4, IPv6, or both network addresses. For more information about configuring additional settings, see **Monitor traffic flow** in Application Priority and SLA.

Configure security logging

You can set up security logging for Cisco IOS XE Catalyst SD-WAN devices by configuring the location of the destination IP address of the log server. You can configure up to four destination servers along with the source interface to collect the syslogs for High Speed Logging (HSL). The IP address for the destination server can be IPv4, IPv6, or both. For more information about configuring HSL, see Configure Firewall High-Speed Logging Using the CLI Template. You can configure the external syslog server to export UTD logs. For more information about UTD logging, see Create Unified Security Policy Summary page.

Before you begin

Ensure that you specify the granular role-based access control (RBAC) for security logging. Ensure that you are able to access policy groups from **Configuration** > **Policy Groups** by configuring specific permissions to the user group. For more information about configuring RBAC for policy groups, see "Configure RBAC for policy groups" in Prerequisites for Policy Groups.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Users and Access** > **Roles**.
2. Click **Edit** adjacent to existing roles or click **Add Role** to create a new role.
3. Choose the permission you wish to configure for the **Security Logging** feature under **Network Settings** and click **Update**.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy** > **Collectors**.

Step 2 Enable **Security Logging** and configure the values in the following table for the high-speed logging and external syslog servers:

Field	Description
High Speed Logging	Configure the following values for the high-speed logging server: • **VPN**: VPN name of the high-speed logging server. The VPNs available in the drop-down list are ones that are previously configured in the configuration groups in Cisco SD-WAN Manager. • **Server IP**: IPv4 or IPv6 address of the log collector server. • **Port**: Port number on which the log collector server is listening for incoming packets.
External Syslog Server	Configure the following values for the external syslog server: • **VPN**: VPN name of the external syslog server. The VPNs available in the drop-down list are ones that are previously configured in the configuration groups in Cisco SD-WAN Manager. • **Server IP**: IPv4 or IPv6 address of the external syslog server.

You can configure up to four high-speed logging servers.

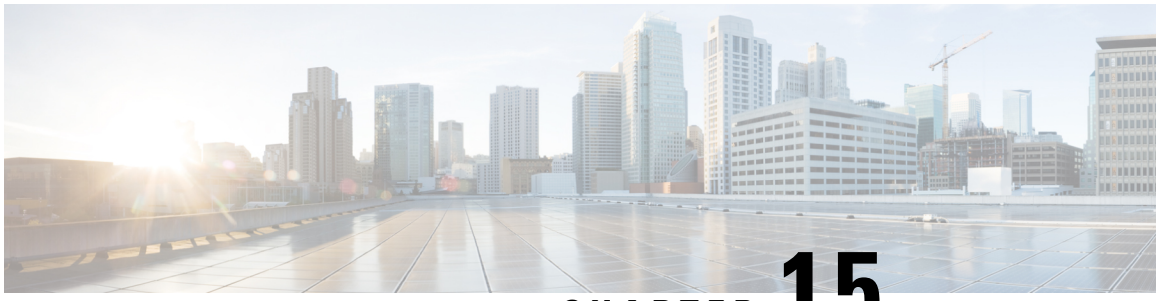
Note
Starting from Cisco IOS XE Catalyst SD-WAN Release 17.16.1a and Cisco Catalyst SD-WAN Manager Release 20.16.1, server labels (**Server 1**, **Server 2**, **Server 3**, and **Server 4**) are added to the high-speed logging server and the syslog server.

For device-specific server settings, add the associated source interface in the **Additional Settings** of the NGFW policy. For more information about configuring additional settings in the policy groups, see Configure NGFW Additional Settings section.

For Global server settings, define the global NHM values. For more information about defining global values on NHM, see Network Hierarchy and Resource Management.

Step 3 Click **Save**.

The security logging settings that you configure are applied along with the embedded security policy when the policy is deployed to Cisco IOS XE Catalyst SD-WAN devices. For more information about configuring the embedded security policy, see Configure Embedded Security.



CHAPTER 15

Wireless Management

- Feature history for wireless management, on page 289
- Wireless management on ISR 1000 series routers, on page 290
- Configuring wireless management, on page 292
- Monitor wireless configuration on Cisco ISR 1000 series routers, on page 300
- Troubleshooting wireless configuration on Cisco ISR 1000 series routers, on page 301

Feature history for wireless management

Developments in wireless management, release by release.

Table 85: Feature history

Feature Name	Release Information	Description
Wireless Management for ISR 1000 Series Routers with WiFi 5	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature enables you to configure wireless LAN settings on WiFi 5-capable Cisco 1000 Series Integrated Services Routers using Cisco SD-WAN Manager. With Cisco SD-WAN Manager, you can automate the wireless LAN controller configuration and provide wireless connectivity without the need for another external controller to configure and manage the wireless settings on the routers.
Wireless Management for ISR 1000 Series Routers with WiFi 6	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	This feature enables you to configure wireless LAN settings on WiFi 6-capable Cisco 1000 Series Integrated Services Routers using Cisco SD-WAN Manager. The Embedded Wireless Controller on these routers facilitates wireless connectivity management without the need for an external controller.

Wireless management on ISR 1000 series routers

Wireless Management on Cisco ISR 1000 Series Routers is a capability that enables the configuration and management of wireless LAN settings, provisioned through a Wireless LAN (WLAN) module, and utilizing an embedded virtual wireless LAN controller. This feature provides wireless connectivity without the need for an external controller to manage the router's wireless settings.

This capability is implemented through:

- WLAN Module Provisioning: A WLAN module is provisioned on the Cisco ISR 1000 Series Routers to provide wireless connectivity
- Embedded Virtual Controllers (EWC): The WLAN module hosts a virtual wireless LAN controller.
- Cisco SD-WAN Manager Integration: Wireless settings are configured and managed using SD-WAN Manager.

Cisco Mobility Express

Cisco Mobility Express is a virtual wireless LAN controller installed in the WLAN module of WiFi 5-capable Cisco ISR 1000 Series Routers. It provides the interface where wireless settings for LAN access are available.

Embedded wireless controller

The Embedded Wireless Controller is a virtual wireless controller installed on the WLAN module of WiFi 6-capable C1131 Cisco IOS XE Catalyst SD-WAN devices. Similar to Cisco Mobility Express, the EWC provides the interface for wireless LAN access settings.

Supported devices for wireless management

This section identifies Cisco device models that are compatible with wireless LAN management capabilities. It details the specific device models and the minimum software release versions required for wireless management on the Cisco ISR 1000 Series, assisting users in verifying their hardware for wireless deployments.

The following table displays a list of Cisco ISR 1000 Series routers that include the WLAN module.

Table 86: Cisco ISR 1000 Series Routers

Device Family	Device Name	Release Version
Cisco ISR 1000 Series Routers with WLAN module supporting WiFi 5	• C1101-4PLTEPW • C1109-4PLTE2PW • C1111-4PW • C1111-8PLTEEAW • C1111-8PW • C1112-8PLTEEAW • C1112-8PW • C1113-8PLTEEAW • C1113-8PMW • C1113-8PW • C1116-4PLTEEAW • C1116-4PW • C1117-4PLTEEAW • C1117-4PLTELAW • C1117-4PMLTEEAW • C1117-4PMW • C1117-4PW • C1121-8PLTEPW • C1121X-8PLTEPW	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco SD-WAN Release 20.6.1
Cisco ISR 1000 Series Routers with WLAN module supporting WiFi 6	• C1131X-8PLTEPW • C1131-8PLTEPW • C1131X-8PW • C1131-8PW	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1

Prerequisites for wireless management on Cisco ISR 1000 series routers

WLAN module VLAN association

Add the management interface of the Wireless LAN (WLAN) module to a specific VLAN in order to access servers such as DHCP and RADIUS.

DHCP server

Configure a DHCP server to assign the IP address for the access point.

SVI for WLAN controller

Configure a switch virtual interface (SVI) on the Cisco ISR 1000 Services Router for virtual WLAN controller management.

Restrictions for wireless management on Cisco ISR 1000 series routers

Single Cisco mobility express access point

Configure only one access point on the LAN side of the router when using Cisco Mobility Express. However, you can connect other external access points to the router that are not configured with Cisco Mobility Express.

Absence of other wireless controllers

Ensure that no other wireless controllers are accessible on the LAN side of the router.

Configuring wireless management

Describes methods for configuring wireless management.

Configure wireless management on Cisco ISR 1000 series routers using a configuration group

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure a Wireless LAN feature in Service profile.

a) Configure the basic details for the wireless LAN.

Field	Description
Enable 2.4G*	Disable this option to shut down the radio type of 2.4 GHz. Default: Enabled
Enable 5G*	Disable this option to shut down the radio type of 5 GHz. Default: Enabled
Country*	Choose the country where the router is installed.
Username*	Specify the username of Cisco Mobility Express.

Field	Description
Password*	Specify the password of Cisco Mobility Express.

b) Configure ME IP address.

Field	Description
ME Dynamic IP*	Enable this option so that the interface receives its IP address dynamically from a DHCP server.
ME IP Address	Specify the IP address of Cisco Mobility Express.
Subnet Mask	Specify the subnet mask of Cisco Mobility Express.
Default Gateway	Specify the default gateway address of Cisco Mobility Express.

c) Configure the Wi-Fi SSID details for setting up a wireless LAN.

Field	Description
Add SSID	
SSID Name*	Enter a name for the wireless SSID. It can be a string from 4 to 32 characters. The SSID must be unique.
Admin State*	Enable this option to indicate that the interface has been configured.
Broadcast SSID*	Enable this option if you want to broadcast the SSID. Disable this option if you do not want the SSID to be visible to all the wireless clients.
VLAN (Range 1-4094)*	Enter a VLAN ID for the wireless LAN traffic.
Radio Type	Choose one of the following radio types: • **2.4GHz** • **5GHz** • **All**
Security Type*	Choose a security type: • **WPA2 Enterprise**: Choose this option for an enterprise where you authenticate and authorize network users with a remote RADIUS server. • **WPA2 Personal**: Choose this option to authenticate users who want to access the wireless network using a passphrase. • **Open**: Choose this option to allow access to the wireless network without authentication.
Passphrase*	This field is available if you choose **WPA2 Personal** as the security type. Set a pass phrase. This pass phrase provides users access to the wireless network.

Field	Description
QoS Profile	Choose a QoS profile.

What to do next

Refer to Deploy a Configuration Group in the *Cisco Catalyst SD-WAN Configuration Groups Reference Guide*.

Configure wireless management on ISR 1000 series routers

Use this procedure to configure and manage wireless settings on your Cisco ISR 1000 Series Routers using Cisco SD-WAN Manager. This task allows you to enable wireless LAN functionality directly on the router, leveraging its embedded wireless controller capabilities.

Wireless management on ISR 1000 Series Routers enables you to set up wireless LANs (WLANs) directly on the router, utilizing its embedded wireless controller. This eliminates the need for an external wireless LAN controller, simplifying network architecture and management.

Before you begin

- Ensure your Cisco ISR 1000 Series Router is a supported model with a WLAN module (WiFi 5 or WiFi 6 capable).
- Confirm that necessary network prerequisites, such as DHCP server availability and proper VLAN configuration for the WLAN module's management interface, are in place.

Follow these steps to configure wireless management using feature templates in Cisco SD-WAN Manager:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**.

In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled as **Feature**.

Step 3 Click **Add Template** to select an appropriate device model.

Step 4 In the left pane, from **Select Devices**, choose a Cisco ISR 1000 Series Router for which you are creating a template.

Step 5 Under **OTHER TEMPLATES**, click **ISR1K Wireless** to select it as the feature template.

Step 6 In the **Template Name** field, enter a name for the feature template.

This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 to 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

Step 7 In the **Description** field, enter a description for the feature template.

This field is mandatory, and it can contain all characters and spaces.

Step 8 Enter the Wi-Fi SSID details for setting up a wireless LAN:

Parameter Name	Description
Wireless Network Name (SSID)	Enter a name for the wireless SSID. It can be a string from 4 to 32 characters. The SSID must be unique.
VLAN (Range 1-4094)	Enter a VLAN ID for the wireless LAN traffic.
Security Type	Choose a security type: • **WPA2 Enterprise**: Choose this option for an enterprise where you authenticate and authorize network users with a remote RADIUS server. • **WPA2 Personal**: Choose this option to authenticate users who want to access the wireless network using a passphrase. • **Open**: Choose this option to allow access to the wireless network without authentication.
RADIUS Server IP	(Optional) This field is available if you choose the **WPA2 Enterprise** option as the security type. Enter the IP address of the RADIUS server.
Authentication Port	(Optional) This field is available if you choose the **WPA2 Enterprise** option as the security type. Enter the authentication port number of the RADIUS server.
Shared Secret	(Optional) This field is available if you choose the **WPA2 Enterprise** option as the security type. Enter the shared secret key of the RADIUS server.
Passphrase	(Optional) This field is available if you choose the **WPA2 Personal** option as the security type. Set a pass phrase. This pass phrase provides users with access to the wireless network.
Admin State	Choose an admin state.
Radio Type	Choose one of the following radio types: • **2.4GHz** • **5GHz** • **Both**
Broadcast SSID	Choose **On** to broadcast the SSID. Choose **Off** if you do not want the SSID to be visible to all the wireless clients.
QoS Profile	Choose a QoS profile.

Step 9 Enter the **General** details for the wireless LAN:

Parameter Name	Description
Country	Choose the country where the ISR is installed.
Username	Specify the username of Cisco Mobility Express. If you are using a C1131 Cisco IOS XE Catalyst SD-WAN device specify the username for the EWC.
Password	Specify the password for Cisco Mobility Express or the EWC.

Step 10 Enter the **Advanced** details for the wireless LAN:

Parameter Name	Description
Controller IP Address	**Note** For Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, and Cisco vManage Release 20.6.1 and earlier releases, this field is displayed as **ME IP Address.** Specify the Management IP address of Cisco Mobility Express or EWC.
Subnet Mask	Specify the subnet mask for the Management IP address.
Default Gateway	Specify the default gateway address of Cisco Mobility Express or EWC.
2.4GHz Shutdown	Click **Yes** to shut down the 2.4 GHz radio type. Click **No** to not shut down this radio type.
5GHz Shutdown	Click **Yes** to shut down the 5 GHz radio type. Click **No** to not shut down this radio type.

Step 11 Click **Save** to save your wireless configuration.

After completing these steps, the wireless LAN settings are configured on your Cisco ISR 1000 Series Router via the feature template, enabling wireless connectivity.

What to do next

Deploy the configured feature template to the desired devices. For more information, see Deploy a Configuration Group.

Configure wireless management on Cisco ISR 1000 series routers using CLI commands

Use this procedure to apply Command Line Interface (CLI) templates to configure wireless LAN settings on your Cisco ISR 1000 series routers. This method allows for direct configuration using pre-defined command sets.

CLI templates are pre-configured sets of commands that simplify the deployment of wireless settings. They allow for precise control over radio profiles, WLAN SSIDs, and general wireless LAN parameters. By default, these commands are executed in global configuration mode.

Before you begin

Ensure you have console or SSH access to the Cisco ISR 1000 series router.

Follow these steps to configure wireless management settings using CLI templates:

Configure a WLAN profile using a CLI template

Note By default, CLI templates execute commands in global config mode.

```
wlan-profile wlan-profile-sample-1
vlan-id 100
ssid sample-ssid-1
data-security personal
passphrase 0 Pass-Phrase-Sample123#
qos-type silver
wlan-profile wlan-profile-sample-2
vlan-id 200
ssid sample-ssid-2
data-security enterprise
aaa radius-server 10.2.3.4 auth-port 1812 shared-secret 0 EsrdT_23sss

qos-type gold
nobroadcast-ssid
```

Configure general WLAN settings using a CLI template

Note By default, CLI templates execute commands in global config mode.

Here is the complete configuration example that shows that show how to configure and manage wireless settings on Cisco ISR 1000 Series Routers.

```
wlan-profile TEST-Enterprise
radio-band all
vlan-id 300
ssid TEST-Enterprise
data-security enterprise
aaa radius-server 192.168.100.20 auth-port 1812 shared-secret 6 EsrdT_23sss
qos-type silver


wlan-profile TEST-Personal
radio-band all
ssid TEST-Personal
data-security personal
passphrase 0 IdSvs23452#
qos-type silver
```

```
radio-profile 24ghz
channel auto
channel-bandwidth auto


radio-profile 5ghz
channel auto
channel-bandwidth auto


wireless-lan mgmt ip address 192.168.1.11 255.255.255.0 default-gateway 192.168.1.1
wireless-lan mgmt credential username admin password 6 sRe32dfst#asd
wireless-lan country US
```

Procedure

Step 1 Access the router's command-line interface.

Log in to your Cisco ISR 1000 series router.

Step 2 Enter global configuration mode.

From privileged EXEC mode, enter configure terminal.

```
Router# configure
Router(config)#
```

Step 3 Configure the radio profiles.

Apply the necessary CLI commands to define the 2.4GHz and 5GHz radio settings, such as shutdown status, channel, and bandwidth.

```
radio-profile 24ghz
shutdown
exit
radio-profile 5ghz
no shutdown
```

Step 4 Configure the WLAN profiles.

Apply the CLI commands to define your wireless SSIDs, including VLAN IDs, security types (WPA2 Personal, WPA2 Enterprise, Open), passphrases, RADIUS server details, and QoS profiles.

```
wlan-profile wlan-profile-sample-1
vlan-id 100
ssid sample-ssid-1
data-security personal
passphrase 0 Pass-Phrase-Sample123#
qos-type silver
wlan-profile wlan-profile-sample-2
vlan-id 200
ssid sample-ssid-2
data-security enterprise
aaa radius-server 10.2.3.4 auth-port 1812 shared-secret 0 EsrdT_23sss

qos-type gold
nobroadcast-ssid
```

Step 5 Configure general wireless LAN settings.

Apply the CLI commands to set the country code, management IP address, default gateway, and management credentials for Cisco Mobility Express or the Embedded Wireless Controller (EWC).

```
wireless-lan country US
wireless-lan mgmt ip address10.16.1.100 255.255.255.0 default-gateway 192.168.1.1
wireless-lan mgmt credential username admin password 0 sRe32dfst#asd
```

Step 6 Commit the configuration changes.

Here is the complete configuration example that shows that show how to configure and manage wireless settings on Cisco ISR 1000 Series Routers.

```
wlan-profile TEST-Enterprise
radio-band all
vlan-id 300
ssid TEST-Enterprise
data-security enterprise
aaa radius-server 192.168.100.20 auth-port 1812 shared-secret 6 EsrdT_23sss
qos-type silver


wlan-profile TEST-Personal
radio-band all
ssid TEST-Personal
data-security personal
passphrase 0 IdSvs23452#
qos-type silver


radio-profile 24ghz
channel auto
channel-bandwidth auto


radio-profile 5ghz
channel auto
channel-bandwidth auto


wireless-lan mgmt ip address 192.168.1.11 255.255.255.0 default-gateway 192.168.1.1
wireless-lan mgmt credential username admin password 6 sRe32dfst#asd
wireless-lan country US
```

The wireless management settings are applied to your Cisco ISR 1000 series router using the specified CLI templates. The router's wireless module will now operate according to the configured radio and WLAN profiles.

This section provides a sample Command Line Interface (CLI) configuration for wireless management on Cisco ISR 1000 Series Routers. This example illustrates a complete setup, including WLAN profiles, radio settings, and general wireless LAN management parameters, serving as a factual representation for reference and implementation. Refer to Configuration example for wireless configuration on Cisco ISR 1000 series routers, on page 300.

What to do next

Monitor the wireless configuration to verify that the settings are active and functioning as expected. For verfication steps, refer to Monitor wireless configuration on Cisco ISR 1000 series routers, on page 300.

Configuration example for wireless configuration on Cisco ISR 1000 series routers

This section provides a sample CLI configuration for wireless management on Cisco ISR 1000 series routers. This example illustrates a complete setup, including WLAN profiles, radio settings, and general wireless LAN management parameters, serving as a factual representation for reference and implementation.

Wireless configuration example

```
wlan-profile TEST-Enterprise
radio-band all
vlan-id 300
ssid TEST-Enterprise
data-security enterprise
aaa radius-server 192.168.100.20 auth-port 1812 shared-secret 6 EsrdT_23sss
qos-type silver


wlan-profile TEST-Personal
radio-band all
ssid TEST-Personal
data-security personal
passphrase 0 IdSvs23452#
qos-type silver


radio-profile 24ghz
channel auto
channel-bandwidth auto


radio-profile 5ghz
channel auto
channel-bandwidth auto


wireless-lan mgmt ip address 192.168.1.11 255.255.255.0 default-gateway 192.168.1.1
wireless-lan mgmt credential username admin password 6 sRe32dfst#asd
wireless-lan country US
```

Monitor wireless configuration on Cisco ISR 1000 series routers

Use this procedure to monitor the wireless settings configured on your Cisco ISR 1000 series routers using Cisco SD-WAN Manager. This allows you to verify the operational status of your wireless LAN, including radio parameters, SSID information, and connected clients.

After configuring wireless management, it is essential to monitor the operational status to ensure that the settings have been applied correctly and the wireless network is functioning as expected. Cisco SD-WAN Manager provides real-time monitoring capabilities for this purpose.

Before you begin

- Wireless management must be configured and deployed on the Cisco ISR 1000 Series Router.
- You must have access to Cisco SD-WAN Manager with appropriate monitoring permissions.

Follow these steps to monitor the wireless configuration using Cisco SD-WAN Manager:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, navigate to **Monitor** > **Network**.

Step 2 Choose a router from the list of the routers.

Step 3 Click **Real Time** in the left pane.

Step 4 From the **Device Options** drop-down list, choose one of the following options:

Device Option	Description
Wireless Radio	Displays the radio parameters of the wireless LAN.
Wireless SSID	Displays information about the wireless SSID.
Wireless Clients	Displays information about the wireless clients in the wireless LAN.

Upon selecting a device option, the real-time data for the chosen wireless aspect (Radio, SSID, or Clients) is displayed, providing insight into the current state of the wireless configuration on the selected Cisco ISR 1000 Series Router.

Troubleshooting wireless configuration on Cisco ISR 1000 series routers

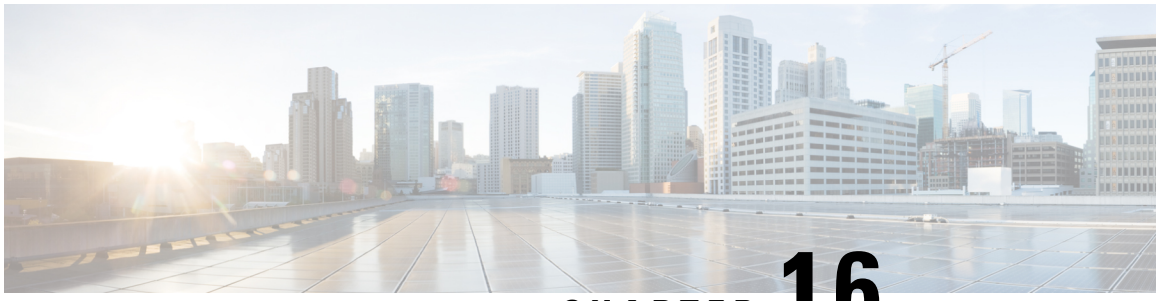
To ensure successful connection of an access point to the Cisco Mobility Express virtual controller or the Embedded Wireless Controller (EWC).

This guidance applies when a Cisco Mobility Express-enabled or EWC-enabled access point fails to establish a connection to the Cisco ISR 1000 Series Router's wireless controller.

The primary reason for this connectivity failure is the absence of an active DHCP server within the management VLAN that is assigned to the Wlan-GigabitEthernet interface. Without an IP address dynamically assigned by a DHCP server, the access point cannot communicate with the controller.

If a DHCP server is not configured in the appropriate VLAN, the access point will remain unable to connect to the wireless controller, thereby preventing wireless client connectivity through that access point.

- Configure a DHCP Server: Ensure a DHCP server is configured and active within the native VLAN of the WiFi module. This server must be capable of assigning IP addresses to the access points.
- Verify WLAN Module VLAN Configuration: Confirm that the management interface of the WLAN module is correctly assigned to a specific VLAN that has access to the DHCP server and other necessary network services (e.g., RADIUS).



CHAPTER 16

Cellular Gateway

- Feature history for Cellular Gateway configuration, on page 303
- Cellular gateways, on page 303
- Configuring cellular gateways, on page 304

Feature history for Cellular Gateway configuration

Developments in cellular gateway configuration, release by release.

Table 87: Feature history

Feature Name	Release Information	Feature Description
Cellular Gateway Configuration	Cisco vManage Release 20.4.1 Cisco IOS XE Catalyst SD-WAN Release 17.4.1a (on devices)	This feature provides templates for configuring a supported cellular gateway as an IP pass-through device. This release supports the Cisco Cellular Gateway CG418-E and CG522-E.
Cellular Gateway Configuration Using a Configuration Group	Cisco Catalyst SD-WAN Manager Release 20.13.1 Cisco IOS CG Release 17.13.1	Added support for configuring cellular gateways using configuration groups. A new Create Cellular Gateway Group workflow creates a configuration group specifically for cellular gateways.

Cellular gateways

A cellular gateway is a network device that

- provides wireless connectivity to a wide area network (WAN),
- functions as a bridge between cellular networks and enterprise LANs, and
- supports secure remote management and monitoring.

Secure communication with devices through a vmanage-admin account

SD-WAN Manager communicates with devices, such as Cisco Catalyst Cellular Gateways, using a secure channel—either a datagram transport layer security (DTLS) tunnel or transport layer security (TLS) tunnel. Within this secure channel, it communicates with the devices or controllers using the NETCONF protocol, within an SSH session. It uses an internal-use-only passwordless "vmanage-admin" user account on the device or controller. The vmanage-admin account is created during the initial device setup. Cisco SD-WAN Manager uses this secure channel for monitoring, configuring, and managing devices.

As noted, the vmanage-admin user accounts do not have any password associated with them, so SD-WAN Manager uses a passwordless procedure to log in to the account. To accomplish this, SD-WAN Manager generates an asymmetric encryption public-private key pair. During deployment of a device, SD-WAN Manager copies the public key that it has generated to the device. It sends the public key using a proprietary protocol, within a secure channel—a DTLS or TLS tunnel.

The activity that SD-WAN Manager performs using the vmanage-admin account appears in syslog messages and in the output of certain show commands. The syslog messages are logged with the same level of detail as activities performed through any other user account. The level of syslog detail depends on the syslog configuration of the device.

Note SD-WAN Manager requires the vmanage-admin account on devices in order to monitor, configure, and manage the devices. Removing, disabling, or altering this account on a device would prevent Cisco SD-WAN Manager from performing these activities, and is not supported.

Supported Cellular Gateway devices

This sections provides information about the supported Cisco Catalyst Cellular Gateway models.

- CG418-E
- CG522-E

Configuring cellular gateways

Describes methods for configuring a cellular gateway.

- Configure a cellular gateway using a configuration group, on page 304
- Configure a cellular gateway with a feature template, on page 309

Configure a cellular gateway using a configuration group

Configure and manage cellular gateways using a configuration group in SD-WAN Manager.

Before you begin

Create a configuration group for Cisco Catalyst Cellular Gateways using **Workflows** > **Create Cellular Gateway Group**. On the **Configuration Groups** page, the resulting configuration group is labelled cellulargateway in the **Device Solution** column.

Follow these steps to configure a Cellular Gateway using a Configuration Group in SD-WAN Manager.

Procedure

Step 1 From the SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Click **…** adjacent to a configuration group for a Cellular Gateway and choose **Edit**.

- **AAA** feature:

Table 88: Local

Parameter Name	Description
Name	The account name is preset to **admin** and cannot be changed.
Password	Enter a password for login.

Table 89: TACACS

Parameter Name	Description
TACACS Configuration	Enable TACACS configuration. Click **Add TACACS** to add one or more TACACS servers.
Authentication	TACACS authentication option: • **tacacs_ascii**: Send authentication information in ASCII format. • **tacacs_pap**: Send authentication information using the password authentication protocol (PAP).
Timeout	Timeout for TACACS authentication. Range: 1 through 1000 seconds
TACACS	
IP Address	IP address of the TACACS server.
Auth Port	TCP port number to connect to the TACACS server. Default: 49
Secret Key	Encryption key for encrypting and decrypting traffic between the cellular gateway and the TACACS server. Configure the same key on the TACACS server.
Source Interface	Preconfigured as Cellular1/0, and cannot be changed. This is the only interface that the cellular gateway can use for communication with the TACACS server.

Parameter Name	Description
Priority	Priority level of the TACACS server. Zero is a default priority value and indicates the highest priority. If a cellular gateway is unable to establish a connection with the highest priority server, it attempts to connect to the server of the next highest priority. Range: 0 through 7

- **Cellular** feature:

Table 90: Cellular Settings

Parameter Name	Description
Primary Slot	Choose a SIM slot to designate it as primary. Range: 0, 1 Default: 0
SIM SLOT 0 Cellular Profile	
Profile Id	Profile ID. You can click **Add** to add multiple profiles.
Access Point Name	Access point name, from your service provider.
Authentication Method	Authentication method (**none**, **pap**, **chap**, **pap_or_chap**) indicated by your service provider.
Username	Username for authentication, as indicated by your service provider.
Password	Password for authentication, as indicated by your service provider.
Packet Data Network Type	Packet data network type (**IPv4**, **IPv6**, **IPv4v6**), as indicated by your service provider.
Attach Profile	Choose the attach profile from the defined profiles.
Data Profile	Choose the data profile from the defined profiles. You can use the same profile for the attach profile and data profile.
SIM SLOT 1 Cellular Profile	
See the fields described for SIM slot 0.	

- **Logging** feature:

Table 91: Disk

Parameter Name	Description
Disk File Rotate	Maximum number of log files to store locally. The device collects diagnostic monitor log files, which have a maximum size of 20 MB each, until the number of files reaches the rotate value. Then the device deletes the oldest file to make room for a new file. Range: 1 through 10
Disk File Size	Maximum file size for each log file that the device stores locally. After reaching the maximum size, the device creates a new log file, with a numerically sequenced filename. Range: 1 through 20 megabytes

Table 92: Servers

Parameter Name	Description
Server Name Type	Choose **ipv4** or **ipv6**, according to the server address type, or choose **dns** if you enter a server domain name in the **Server Name Value** field.
Server Name Value	IP address or domain name of the server.
Source IP	By default, this is the system IP address. You can choose the **Device Specific** option to specify per device.
Priority	Filter the type of log messages saved using one of the following priority options, listed from lowest to highest priority. Each priority option configures the device to save log messages of that priority and all higher priorities. For example, information is the lowest priority of message, so choosing **information** includes information log messages and all other log messages too. Choosing **error** excludes information, notice, and warn log messages, but includes error messages and all other log messages of higher priority (critical, alert, and emergency). From lowest to highest priority, the options are the following: • information • notice • warn • error • critical • alert • emergency

- **Network Protocol** feature:

Table 93: Basic Configuration

Parameter Name	Description
Passthrough	The cellular gateway operates in one of two modes: IP passthrough and NAT. In IP passthrough mode, the cellular gateway passes the public IP address assigned by the internet service provider (ISP) to a downstream device attached to the cellular gateway. Disabling the **Passthrough** option enables NAT, which gives the devices that are connected to the cellular gateway access to a DHCP server and to the local gateway. **Note** Enabling passthrough mode disables and hides the other fields in the **Basic Configuration** section.
DHCP Pool	
DHCP Pool	Enable a DHCP pool for NAT.
DHCP Network Pool	IP address pool, in classless interdomain routing (CIDR) format.
Lease Days	Days for DHCP lease time Range: 0 to 365
Lease Hours	Hours for DHCP lease time. Range: 0 to 23
Lease Minutes	Minutes for DHCP lease time. Range: 0 to 59
PAT Configuration	
PAT Configuration	Enable port address translation (PAT).
Add PAT Config	Click this to add one or more PAT configurations.
Description	Description of the PAT configuration.
Protocol	Choose **TCP** or **UDP**.
LocalAddress	IPv4 format address.
LocalPort	Port number. Range: 0 to 65535
InterfaceName	Preconfigured as Cellular1/0, which is the WAN interface for the cellular gateway.

Parameter Name	Description
GlobalPort	Global port number. Range: 1 to 65535

Table 94: NTP Servers

Parameter Name	Description
NTP	To configure a network time protocol (NTP) server, enter an IPv4 address or a DNS name. Maximum number of NTP servers: 4

Step 3 (Optional) To add CLI configuration commands, follow these steps:

a) Open the **CLI Add-on Profile**.
b) Click **Add Feature**.
c) In the **Type** dropdown list, choose **Config**.
d) Enter a name for the feature.
e) Click **Save**.

Note
CLI configuration commands in the CLI Add-on Profile override any configuration done using the Global Profile.

What to do next

Refer to Deploy a Configuration Group in the *Cisco Catalyst SD-WAN Configuration Groups Reference Guide*.

Configure a cellular gateway with a feature template

Configure a cellular gateway device using a feature template.

Use feature templates in SD-WAN Manager to standardize device configurations and enable efficient updates.

For information about using a configuration group, see Configure a cellular gateway using a configuration group, on page 304.

Follow these steps to configure a cellular gateway using a feature template.

Procedure

Step 1 Create a device template for Cisco Cellular Gateway CG418-E devices.

After you enter a description for the feature template, do this:

a) From the SD-WAN Manager menu, choose **Configuration** > **Templates**.
b) Click **Device Templates**.

Note
In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

c) From the **Create Template** drop-down list choose **From Feature Template**.
d) From the **Device Model** drop-down list select the type of device for which you are creating the template.
e) Choose **Cellular Gateway** > **Cellular Gateway Platform** > **Create Template**. Then configure the Cellular Gateway Platform feature template as shown in this table.

Table 95: Cellular Gateway Platform Template Parameters

Parameter Name	Description
Basic Configuration Tab	
Time Zone	Choose the time zone to use for the device. The device uses this time zone for clock synchronization when NTP is configured.
Management Interface	Enter the IPv4 address of the management interface for accessing the device.
Admin-Password	Enter the admin user password for logging in to the device by using an SSH client or a console port.
NTP-Servers	Configure one or more NTP servers to which the device synchronizes its clock.
Cellular Configuration Tab	
IP-Src-Violation	Choose **v4 only**, **v6 only**, or **v4 and v6** to enable the IP source violation feature for the corresponding IP address types. Choose **None** if you do not want to enable this feature.
Auto-SIM	Choose **On** to enable the auto-SIM feature. When this feature is enabled, the device automatically detects the service provider to which SIMs in the device belong and automatically loads the appropriate firmware for that provider.
Primary SIM Slot	Choose the slot that contains the primary SIM card for the device. If the device loses service to this slot, it fails over to the secondary slot.
Failover-Timer (minutes)	Enter the number of minutes that the device waits before trying to communicate with the primary SIM slot after the device detects loss of service to this slot.
Max-Retry	Enter the number of consecutive unsuccessful attempts by the device to communicate with the primary SIM before failing over to the secondary slot

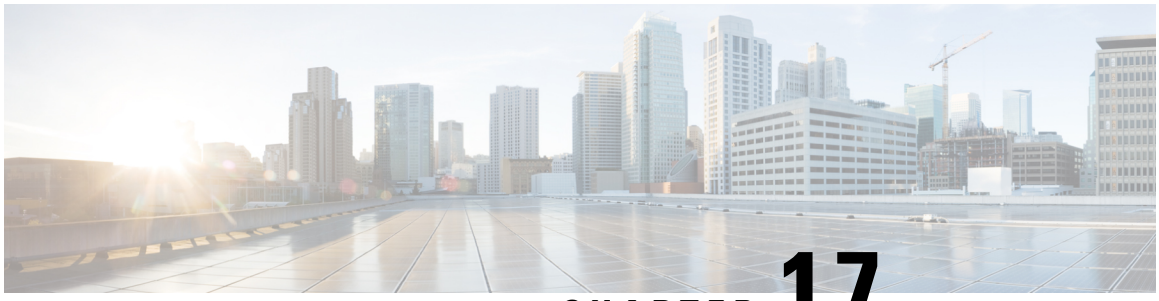
f) Choose **Cellular Gateway** > **Cellular Gateway Profile** and choose **Create Template** from the Cellular Gateway Profile drop-down list. Then configure the Cellular Gateway Profile feature template as shown in this table.

Table 96: Cellular Gateway Profile Template Parameters

Parameter Name	Description
Basic Configuration Tab	
SIM	Choose a SIM slot and configure the options to create a profile for the SIM in that slot. This profile indicates to the service provider which of its cellular networks the SIM should attach to. • Profile ID: Enter a unique ID for the profile • Access Point Name: Enter the name of the access point for this profile • Packet Data Network Type: Choose the type of network for data services for this profile (**IPv4**, **IPv6**, or **IPv4v6**) • Authentication: Choose the authentication method that this profile uses for data, and enter the user name and password for this method in the Profile Username and Profile Password fields that display You can configure one profile for each SIM slot in the device.
Add Profile	Click to add an access point name (APN) profile that the cellular device uses to attach to a cellular network. You can add up to 16 profiles.
Profile ID	Enter a unique identifier for the profile. Valid values: Integers 1 through 16.
Access Point Name	Enter a name to identify the cellular access point.
Packet Data Network Type	Choose the packet data network (PDN) type of the cellular network (**IPv4**, **IPv6**, or **IPv46**).
Authentication	Choose the authentication method that is used to attach to the cellular access point (**none**, **pap**, **chap**, **pap_chap**).
Profile Username	If you choose an authentication method other than **none**, enter the user name to use for authentication when attaching to the cellular access point.
Password	If you choose an authentication method other than **none**, enter the password to use for authentication when attaching to the cellular access point.

Parameter Name	Description
Add	Click to add the profile your are configuring.
Advanced Configuration Tab	
Attach Profile	Choose the profile that the device uses to connect to the cellular network.
Cellular 1/1 Profile	Choose the profile that the device uses for data connectivity over the cellular network.

Step 2 Attach the device template to the device.



CHAPTER 17

Cisco Unified Communications Voice Services

- Feature history for Cisco Unified Communications Voice Services, on page 313
- Cisco Unified Communications Voice Services, on page 314
- Configure Unified Communications Voice Services, on page 315
- Provision a device template for unified communications, on page 385
- Dial peer CSV file, on page 388
- Translation rules CSV file, on page 390
- Monitor UC operations, on page 391

Feature history for Cisco Unified Communications Voice Services

Table 97: Feature history

Feature Name	Release Information	Description
Cisco IP-based media services	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	You can now enable Cisco IP-based media services using a feature template.

Feature Name	Release Information	Description
Cisco Unified Communications Voice Services	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This feature enables you to configure Cisco Unified Communications (UC) voice services on supported routers using feature templates and voice policies. When enabled, these routers can process calls for various endpoints, including voice ports, POTS dial peers, SIP dial peers, and phone profiles in Cisco Unified SRST mode. You configure UC voice services from the Feature tab and the Voice Policy page for a supported device. To configure UC voice services, Cisco SD-WAN Manager must run Cisco vManage 20.1.1. This feature is supported on Cisco 4000 Series Integrated Services Routers.
DSP Farms for UC Voice Services with Workflow Library and Configuration Groups	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	You can now configure DSP farms for UC voice services using the Workflow Library and configuration groups.

Cisco Unified Communications Voice Services

Cisco Unified Communications (UC) voice services enable you to configure feature templates and voice policies for supported routers. These templates and policies configure parameters for Foreign Exchange Office (FXO), Foreign Exchange Station (FXS), and FXS/Direct Inward Dialing (DID) interfaces. Starting with Cisco IOS XE Catalyst SD-WAN Release 17.3.1a, you can also configure parameters for Primary Rate Interface (PRI) Integrated Services Digital Network (ISDN). Additionally, you can use the DSPFarm feature template to enable Cisco IP-based media services.

Capabilities

When enabled, UC voice services allow routers to process calls for various endpoints. These include voice ports for analog and digital interfaces, Plain Old Telephone Service (POTS) dial peers, Session Initiation Protocol (SIP) dial peers, and phone profiles in Cisco Unified Survivable Remote Site Telephony (SRST) mode.

Note Starting with Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, you can also configure and enable UC voice services using the Workflow library or configuration groups. For more information, see Cisco Unified Communications Voice Profile.

System requirements

To configure UC voice services for Cisco Unified Communications, Cisco SD-WAN Manager must run Cisco SD-WAN Release 20.3.1 or later.

For detailed information about commands to configure and maintain Cisco IOS voice applications, see the Cisco IOS Master Command List.

Configure Unified Communications Voice Services

This task provides the comprehensive workflow to enable Cisco Unified Communications (UC) voice services for supported routers, allowing them to process calls for various endpoints including voice ports, POTS dial peers, SIP dial peers, and phone profiles in Cisco Unified SRST mode. This ensures that Cisco IOS XE Catalyst SD-WAN devices can process calls for various endpoints and integrate IP-based media services.

Follow these steps to configure Unified Communications Voice Services:

Before you begin

Ensure that Cisco Catalyst SD-WAN Manager runs Cisco vManage Release 20.3.1 or later.

Procedure

Step 1 Add a voice card feature template.

Configures analog and PRI ISDN digital interfaces for voice cards. See Add a voice card feature template, on page 316

Step 2 Add a call routing feature template.

Configures parameters for TDM-SIP trunking and dial plans. See Add call routing feature template, on page 326

Step 3 Add an SRST feature template.

Configures parameters for Cisco Unified Survivable Remote Site Telephony (SRST) for SIP. See Add an SRST feature template, on page 331.

Step 4 Add a DSPFarm Feature Template.

Sets up and provisions a Digital Signal Processor (DSP) farm for media services like transcoding and conferencing. See Add a DSPFarm feature template, on page 333

Step 5 Add a voice policy.

Defines how the system augments and manipulates calls for various endpoint types. See Add a voice policy, on page 345.

Step 6 Provision a device template for Unified Communications.

Selects UC-specific feature templates and sets up the voice policy to include with the device template. See Provision a device template for unified communications, on page 385.

After completing this supertask, UC voice services will be enabled on supported Cisco IOS XE Catalyst SD-WAN devices, allowing them to process calls for various endpoints.

What to do next

To monitor the real-time statuses of lines, calls, interfaces, and related items that a device processes, navigate to **Monitor** > **Devices** from the SD-WAN Manager menu.

Add a voice card feature template

A voice card feature template configures analog and PRI ISDN digital interfaces, which provide configuration settings for ports on voice cards in routers. Use this procedure to create and configure such a template.

When you add a voice card feature template, you configure the type of voice card, port information, and service provider parameters for analog interfaces. For digital interfaces, you configure the type of voice card, the T1 or E1 controller, and related parameters. SD-WAN Manager assists with module placement by displaying available slots and sub-slots based on the device model.

Follow these steps to add a voice card feature template:

Before you begin

Ensure you have selected the supported device to which you want to add voice services in Cisco SD-WAN Manager.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**, and click **Add Template**.

In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

Step 3 Select the supported device to which you want to add voice services.

Step 4 Select **Voice Card** from the **Unified Communications** templates.

Step 5 In **Template Name**, enter a name for the template.

This field may contain uppercase and lowercase letters, digits 0 through 9, hyphens (-), and underscores (_).

Step 6 In **Description**, enter a description for the template.

This field can contain any characters and spaces.

Step 7 To configure an analog interface, click **New Analog Interface** and configure interface options as described in the Voice card analog interface configuration options, on page 317 topic.

From Cisco IOS XE Catalyst SD-WAN Release 17.3.1a, select **Analog Interface** in the Interface area to access **New Analog Interface**.

a) You can add as many analog interfaces as needed, based on the number of interfaces that your module supports. After you configure each analog interface, click **Add**.

If any analog interfaces are already configured, they appear in the interfaces table on this page. To edit an existing interface, click **...** and select its pencil icon to edit the options in the window that pops up as described in the Voice

card analog interface configuration options, on page 317 topic, and click **Save Changes**. To delete an interface, click **…** and click the trash can icon.

Step 8 To configure a PRI ISDN digital interface, in the **Interface** area, click **Digital Interface**, click **New Digital Interface**, and configure interface options as described in the Voice card digital interface configuration options, on page 319 topic.

a) Based on the number of interfaces that your module supports, you can add as many PRI ISDN digital interfaces as needed. After you configure each PRI ISDN digital interface, click **Add**.

If any digital interfaces are already configured, they appear in the interfaces table on this page. To edit an existing interface, click **...** and select its pencil icon to edit the options in the window that pops up as described in the Voice card digital interface configuration options, on page 319 topic, and click **Save Changes**. To delete an interface, click **…**, and click its trash can icon.

Note
After you save the interface configuration, you cannot change the module type, interface type, slot or sub-slot, or time slots.

If you want to change time slots, you must delete the interface and create a new one.

If you want to change the module type, interface type, and slot or sub-slot, detach the template from the device, unmap the voice policies that are associated with the interfaces, and delete all interfaces that are associated with the module and slot or sub-slot. Next, push the template to the device, reload the device, and create new required interfaces. Finally, push the new template to the device, and reattach the template to the device.

Step 9 Click **Save**.

Step 10 (Optional) To configure additional analog or PRI ISDN digital interfaces for this template:

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
b) Click **Feature Templates**.

In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

c) Click **...** for the template you wish to configure, and click **Edit**.
d) Repeat Step 7 or Step 8 and Step 9.

A voice card feature template is successfully added and configured.

Example

What to do next

If you need to configure more analog or PRI ISDN digital interfaces for this template later, you can edit the template by navigating to **Configuration** > **Templates** > **Feature Templates**, clicking **...** next to the template name, and selecting **Edit**. You can then repeat the configuration steps for analog or digital interfaces.

Voice card analog interface configuration options

This reference topic describes the various options available for configuring analog interfaces on voice cards within Cisco Unified Communications Voice Services. These options allow you to define the type of voice module, port characteristics, and service provider parameters for analog voice ports.

Analog Interface Configuration Options

This table describes the options for configuring an analog interface.

Table 98: Analog Interface Options

Option	Description	Cisco IOS CLI Equivalent
Module	Select the type of voice module that is installed in the router.	—
Module Slot/Sub-slot	Enter the slot and sub-slot of the voice module.	**voice-card** *slot/subslot*
Use DSP	Enable this option if you want to use the built-in DSPs on the network interface module for TDM calls.	**no local-bypass**
Port Type	Select the type of ports on the voice module that you are configuring for this interface (**FXS** or **FXO**). You can select **All** to define the port type for all ports of the selected type, or **Port Range** to define the port type for a specified range of ports. Using Port Range, you can create analog interfaces as described later in this procedure to configure different ranges of ports.	—
Description	Enter a description of the selected port or ports. For example, fax machine or paging system.	**description** *string*
Secondary Dialtone	Available if you select FXO from the Port Type drop-down list. Set to **On** if you want the selected ports to generate a secondary dial tone when callers access an outside line.	**secondary dialtone**
Connection PLAR	Enter the Private Line Automatic Ringdown extension to which the selected ports forward inbound calls.	**connection plar** *digits*
OPX	Available if you select FXO from the Port Type drop-down list. Check this option if you want to enable Off-Premises Extension for the PLAR extension.	**connection plar opx** *digits*

Option	Description	Cisco IOS CLI Equivalent
Signal Type	Select the Signal Type that indicates an on-hook or off-hook condition for calls that the ports receive. Options are **Loopstart**, **Groundstart**, or **DID**. The DID option is available if you select FXS from the Port Type drop-down list.	**signal** {groundstart | loopstart} **signal did** {delay-dial | immediate | wink-start}
Caller-ID Enable	Available if you select a signal type of Loopstart or Groundstart. Set to **ON** if you want to enable caller ID information for inbound calls.	**caller-id enable**
DID Signal Mode	Available if you select a signal type of DID. Choose the mode for the DID signal type (**Delay Dial**, **Immediate**, or **Wink Start**). Default: Wink Start.	**signal did** {delay-dial | immediate | wink-start}
Shutdown	Set to **ON** if you want to shut down ports that are not being used. Default: Off.	**shutdown**

Voice card digital interface configuration options

This reference topic describes the various options available for configuring digital interfaces on voice cards within Cisco Unified Communications Voice Services. These options allow you to define the type of T1/E1 voice module, interface characteristics, clock sources, and other parameters for digital voice ports.

Digital Interface Configuration Options

This table describes the options for configuring a digital interface.

Table 99: Digital Interface Options

Option	Description	Cisco IOS CLI Equivalent
Digital Interface Tab Provides options for configuring parameters for a T1/E1 voice module and the clock source for the module ports. Before you configure these options, ensure that you have the appropriate DSP module installed for each T1/E1 voice module.		
Module	Select the type of T1/E1 voice module that is installed in the router.	—

Option	Description	Cisco IOS CLI Equivalent
Interface Type	Select the type of interface on the voice module: • **T1 PRI**—Specifies T1 connectivity of 1.544 Mbps through the telephone switching network, using AMI or B8ZS coding • **E1 PRI**—Specifies a wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 2.048 Mbps	**card type** {**t1** | **e1**} *slot sub-slot*
Slot/Sub-slot	Enter the slot and sub-slot of the voice module.	**voice-card** *slot*/*sub-slot*
Use DSP	Enable this option if you want to use the built-in DSPs on the network interface module for TDM calls.	**no local-bypass**

Option	Description	Cisco IOS CLI Equivalent
Interface	Perform these actions to configure the number of T1/E1 ports to be provisioned on the module, and the clock source for each port: **1.** Click **Add**. The Port and Clock Selector window displays. **2.** Check the check box that corresponds to each port that you want to configure. The number of ports that you can configure depends on the Module type that you select. **3.** For each port, select the clock source: • **Line**—Sets the line clock as the primary clock source. With this option, the port clocks its transmitted data from a clock that is recovered from the line receive data stream. • **Primary Clock**—Sets the port to be a primary clock source. • **Secondary Clock**—Sets the port to be a secondary clock source. • **Network**—Sets the backplane clock or the system oscillator clock as the module clock source. We recommend that you set one port to be the primary clock and set another port going to the same network as a secondary clock source to act as a backup. **4.** Click **Add**.	**controller** {**t1** | **e1**} *slot*/*sub-slot*/*number* **clock source** {**network** | **line** | **line primary** | **line secondary**}
Network Participation	This check box displays after you add an interface. Check this check box to configure the T1/E1 module to participate in the backplane clock. Uncheck this check box to remove the clock synchronization with the backplane clock for the module. By defult, this check box is checked.	**network-clock synchronization participate** *slot*/*sub-slot*

Option	Description	Cisco IOS CLI Equivalent
Shutdown	Perform these actions to disable or enable the controller, serial interface, or voice port that is associated with the interface port. **1.** Click **Shutdown Selected**. The Shutdown window displays. **2.** For each port, select the item or items that you want to enable (**Controller**, **Serial**, or **Voice Port**. If you do not select an item, it is enabled. **3.** Click **Add**.	**controller e1/t1** *slot*/*sub-slot*/*port* **shutdown** **interface serial** *slot*/*sub-slot*/**port:**{**15** | **23**} **shutdown** **voice-port** *slot*/*sub-slot*/**port:**{**15** | **23**} **shutdown**
Time Slots	Select the number of time slots of the interface type. Valid ranges: • For T1 PRI—Time slots 1 through 24. The 24th time slot is the D channel. • For E1 PRI— Time slots 1 through 31. The 16th time slot is the D channel.	**controller e1/t1** *slot*/*sub-slot*/*port* **pri-group timeslots** *timeslot-range* [**voice-dsp**]
Framing	Select the frame type for the interface type. For a T1 PRI interface type, options are: • **esf**—Extended super frame (default) • **sf**—Super frame For an E1 PRI interface type, options are: • **crc4**—CRC4 framing type (default) • **no-crc4**—No CRC4 framing type	**controller t1** *slot*/*sub-slot*/*port* **framing** [**esf** | **sf**] **controller e1** *slot*/*sub-slot*/*port* **framing** [**crc4** | **no-crc4**] [**australia**]
Australia	This check box displays when you select E1 PRI for the interface type. Check this check box to use the **australia** framing type.	**controller e1** *slot*/*sub-slot*/*port* **framing** [**crc4** | **no-crc4**] **australia**

Option	Description	Cisco IOS CLI Equivalent
Line Code	Select the line code type for the interface type. For a T1 PRI interface type, options are: • **ami**—Use Alternate Mark Inversion as the line code type • **b8zs**—Use binary 8-zero substitution as the line code type (default) For an E1 PRI interface type, options are: • **ami**—Use Alternate Mark Inversion as the line code type • **hdb3**—Use high-density binary 3 as the line code type (default)	**controller t1** *slot/sub-slot/port* **linecode** [**ami** | **b8zs**] **controller e1** *slot/sub-slot/port* **linecode** [**ami** | **hdb3**]
Line Termination	This check box appears only for an Interface type of E1 PRI. Select the line termination type for the E1 controller: • **75-ohm**—75 ohm unbalanced termination • **120-ohm**—120 ohm balanced termination (default)	**controller e1** *slot/sub-slot/port* **line-termination** {**75-ohm** | **120-ohm**}
Cable Length Type	This check box appears only for an Interface type of T1 PRI. Select the cable length type for the T1 PRI interface type: • **long**—Long cable length • **short**—Short cable length	**controller t1** *slot/sub-slot/port* **cablelength** {**short** | **long**}
Cable Length	This check box appears only for an interface type of T1 PRI. Select the cable length for the T1 PRI interface type. Use this option to fine-tune the pulse of a signal at the receiver for a T1 cable. The default value is **0db**.	**controller t1** *slot/sub-slot/port* **cablelength** {**[short** [**110ft** | **220ft** | **330ft** | **440ft** | **550ft** | **660ft**]] [**long** [**-15db** | **-22.5db** | **-7.5db** | **0db**]]}

Option	Description	Cisco IOS CLI Equivalent
Network Side	Enable this option to have the device use the standard PRI network-side interface. By default, this option is disabled (set to **No**).	**interface serial** *slot*/*sub-slot*/**port:**{**15**| **23**} **isdn protocol-emulate** [**network**| **user**]
Switch Type	Select the ISDN switch type for this interface: • **primary-qsig**—Supports QSIG signaling according tot the Q.931 protocol. Network side functionality is assigned with the isdn protocol-emulate command. • **primary-net5**—NET5 ISDN PRI switch types for Asia, Australia, and New Zealand. ETSI-compliant switches for Euro-ISDN E-DSS1 signaling system. • **primary-ntt**—Japanese NTT ISDN PRI switches. • **primary-4ess**—Lucent (AT&T) 4ESS switch type for the United States. • **primary-5ess**—Lucent (AT&T) 5ESS switch type for the United States. • **primary-dms100**—Nortel DMS-100 switch type for the United States. • **primary-ni**—National ISDN switch type.	**interface serial** *slot*/*sub-slot*/**port:**{**15**| **23**} **isdn switch-type** [**primary-4ess** | **primary-5ess** |**primary-dms100** | **primary-net5** | **primary-ni** | **primary-ntt** | **primary-qsig**]

Option	Description	Cisco IOS CLI Equivalent
ISDN Timer	Perform these actions to configure the ISDN timers for the interface: **1.** Click **Add**. The ISDN Timer window displays. **2.** Configure the following timers as needed. The values are in milliseconds. • **T200**. Valid range: integers 400 through 400000. Default: 1000. • **T203**. Valid range: integers 400 through 400000. The default value is based on the switch type and network side configurations. • **T301**. Valid range: integers 180000 through 86400000. The default value is based on the switch type and network side configurations. • **T303**. Valid range: integers 400 through 86400000. The default value is based on the switch type and network side configurations. • **T306**. Valid range: integers 400 through 86400000. Default: 30000. • **T309**. Valid range: integers 0 through 86400000. The default value is based on the switch type and network side configurations. • **T310**. Valid range: integers 400 through 400000. The default value is based on the switch type and network side configurations. • **T321**. Valid range: Integers 0 through 86400000. The default value is based on the switch type and network side configurations. **3.** Click **Add**.	**interface serial** *slot*/*sub-slot*/**port:** {**15**| **23**} **isdn timer T200** *value* **isdn timer T203** *value* **isdn timer T301** *value* **isdn timer T303** *value* **isdn timer T306** *value* **isdn timer T309** *value* **isdn timer T310** *value* **isdn timer T321** *value*
Delay Connect Timer	Select the duration, in milliseconds, to delay connect a PRI ISDN hairpin call. Valid range: integers 0 through 200. Default: 20.	**voice-port** *slot*/*sub-slot*/**port:** {**15**| **23**} **timing delay-connect** *value*

Option	Description	Cisco IOS CLI Equivalent
Clock Tab Use this tab to configure priority order for the primary and secondary clock sources that you selected for each module. This tab is vailable after you configure a PRI ISDN digital interface and click **Add**.		
Clock Priority Sorting	Configure the priority of up to six clock sources. The drop-down list displays the interface ports for which a primary or secondary clock source is defined and that is configured for network participation. Check a check box to select the port for inclusion in the priority list, and use the **Up arrow** next to a port to change its priority. The list displays the ports in order of priority, with the port with the highest priority at the top of the list. After you configure the priority, this field displays the selected ports in priority order. We recommend that all ports in the priority list be of the same type, either E1-PRI or T1-PRI.	**network-clock input-source** priority **controller** [**t1**| **e1**] *slot*/*sub-slot*/*port*
Automatically Sync	Select **Add** to enable network synchronization between all modules and the router. Default: **On**.	network-clock synchronization automatic
Wait to restore clock	Enter the amount of time, in milliseconds, that the router waits before including a primary clock source in the clock selection process. Valid range: 0 through 86400. Default: 300.	network-clock wait-to-restore *milliseconds*

Add call routing feature template

A call routing feature template configures parameters for TDM-SIP trunking, including trusted IP addresses for preventing toll fraud, and a dial plan. Use this procedure to add and configure such a template.

A dial plan, made up of dial peers, defines how a router routes traffic to and from voice ports to the PSTN or to another branch. This template allows for the definition of global SIP communication settings and detailed dial peer configurations.

To add a call routing feature template:

Before you begin

Ensure you have selected the supported device to which you want to add call routing features in Cisco SD-WAN Manager.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**, and click **Add Template**.

In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

Step 3 Select the supported device to which you want to add voice services.

Step 4 Select **Voice Card** from the **Unified Communications** templates.

Step 5 In **Template Name**, enter a name for the template.

This field may contain uppercase and lowercase letters, digits 0 through 9, hyphens (-), and underscores (_).

Step 6 In **Description**, enter a description for the template.

This field can contain any characters and spaces.

Step 7 In **Global**, configure options as described in the Global call routing options, on page 327 topic.

Step 8 In **Dial Plan**, perform one of these actions:

To configure a dial peer directly, configure options as described in the Dial peer options, on page 328 topic.

To create or edit a dial peer CSV file, click **Download Dial Peer List** to download the system provided file named Dial-Peers.csv. The first time you download this file, it contains field names but no records. Update this file as needed by using an application such as Microsoft Excel. For more information about this file, see Dial peer CSV file, on page 388.

To import configuration information from a dial peer CSV file that you have created, click **Upload Dial Peer List**.

You can add as many dial peers as needed. Click **Add** after you configure each dial peer. If any dial peers already are configured, they appear in the dial peers table on this page. To edit a configured dial peer, click **…**, and click its pencil icon. Edit the options in the window that pops up as described in the table, and click **Save Changes**. To delete a dial peer, click **…**, and click its trash can icon.

Step 9 Click **Save**.

A call routing feature template is successfully added and configured.

What to do next

Proceed to add an SRST feature template if required for your Unified Communications deployment.

Global call routing options

This reference topic describes the global options available for configuring call routing parameters within a call routing feature template. These settings define how the router communicates through SIP and handles trusted IP addresses for call security.

Global call routing options

The following table describes global options for configuring call routing.

Table 100: Global Call Routing Options

Option	Description	Cisco IOS CLI Equivalent
Trusted IPv4 Prefix List	Enter the IPv4 addresses with which the router can communicate through SIP. Enter each IPv4 address in CIDR format. For example, 10.1.2.3/32. Separate each address with a comma (,). The router does not communicate with other IPv4 addresses, which prevents fraudulent calls being placed through the router. A Trusted IPv4 Prefix is required for TDM to IP calls.	**voice service voip** **ip address trusted list** **ipv4** *ipv4-address*/*ipv4-network-mask*
Trusted IPv6 Prefix List	Enter the IPv6 addresses with which the router can communicate through SIP. Separate each IPv6 address with a comma (,). The router does not communicate with other IPv6 addresses, which prevents fraudulent calls being placed through the router. A Trusted IPv6 Prefix is required for TDM to IP calls.	**voice service voip** **ip address trusted list** **ipv6** *ipv6-prefix*//*prefix-length*
Source Interface	Enter the name of the source interface from which the router initiates SIP control and media traffic. This information defines how the return/response to this traffic should be sent.	**voice service voip** **sip** **bind control source-interface** *interface-id* **bind media source-interface** *interface-id*

Dial peer options

This reference topic describes the various options available for configuring dial peers, which are essential components of a dial plan. Dial peers define how a router routes traffic for voice calls, including settings for incoming/outgoing calls and transport protocols.

Dial peer options

The following table describes options for configuring dial peers.

Table 101: Dial peer options

Option	Description	Cisco IOS CLI Equivalent
Voice Dial Peer Tag	Enter a number to be used to reference the dial peer.	**dial-peer voice** *number* {**pots** | **voip**}
Dial Peer Type	Select the type of dial peer that you are creating (**POTS** or **SIP**).	**dial-peer voice** *number* {**pots** | **voip**}
Direction	Select the direction for traffic on this dial peer (**Incoming** or **Outgoing**).	Incoming: dial-peer voice *number* {pots | voip} **incoming called-number** *string* Outgoing: dial-peer voice *number* {pots | voip} **destination-pattern** *string*
Description	Enter a description of this dial peer.	**description**
Numbering Pattern	Enter a string that the router uses to match incoming calls to the dial peer. Enter the string as an E.164 format regular expression in the form [0-9,A-F#*.?+%()-]*T?.	Incoming: dial-peer voice *number* {pots | voip} **incoming called-number***string* Outgoing: dial-peer voice *number* {pots | voip} **destination-pattern** *string*
Forward Digits Type	Available if you select the POTS dial peer type and the Outgoing direction. Select how the dial peer transmits digits in outgoing numbers: • **All**—The dial peer transmits all digits • **None**—The dial peer does not transmit digits that do not match the destination pattern • **Some**—The dial peer transmits the specified number of right-most digits Default: None.	All: dial-peer voice *number* pots **forward-digits all** None: dial-peer voice *number* pots **forward-digits 0** Some: dial-peer voice *number* pots **forward-digits** *number*

Option	Description	Cisco IOS CLI Equivalent
Forward Digits	Available if you select **Some** for Forward Digits Type. Enter the number of right-most digits in the outgoing number to transmit. For example, if you set this value to 7 and the outgoing number is 1112223333, the dial peer transmits 2223333.	dial-peer voice *number* pots **forward-digits** *number*
Prefix	Available if you select the POTS dial peer type and the Outgoing direction. Enter digits to be prepended to the dial string for outgoing calls.	dial-peer voice *number* pots **prefix** *string*
Transport Protocol	Available if you select SIP for the Dial Peer Type. Choose the transport protocol (**TCP** or **UDP**) for SIP control signaling.	dial-peer voice *number* voip **session transport** {**tcp** | **udp**}
Preference	Available if you select POTS or SIP for the Dial Peer Type. Select an integer from 0 to 10, where the lower the number, the higher the preference. If dial peers have the same match criteria, the system uses the one with the highest preference value. Default: 0 (highest preference).	dial-peer voice *number* voip **preference** *value* dial-peer voice *number* pots **preference** *value*
Voice Port	Available if you select the POTS dial peer type. Enter the voice port that the router uses to match calls to the dial peer. For an analog port, enter the port you want. For a digital **T1** PRI ISDN port, enter a port with the suffix:**23**. For a digital E1 PRI ISDN port, enter a port with the suffix :**15**. For an outgoing dial peer, the router sends calls that match the dial peer to this port. For an incoming dial peer, this port serves as an extra match criterion. The dial peers are matched only if a call comes in on this port.	dial-peer voice *number* pots For an analog port: **port** *slot*/*subslot*/*port* For a digital port: **port** *slot*/*subslot*/*port***:15** **port** *slot*/*subslot*/*port***:23**

Option	Description	Cisco IOS CLI Equivalent
Destination Address	Available if you select the SIP dial peer type and the Outgoing direction. Enter the network address of the remote voice gateway to which calls are sent after a local outgoing SIP dial peer is matched. Enter the address in one of these formats: • dns:*hostname.domain* • *sip-server* ipv4:*destination-addres* ipv6:*destination-address*	**session target** {**ipv4:***destination-address* | **ipv6:***destination-address*| **sip-server** | **dns:***hostname.domain*}

Add an SRST feature template

An SRST feature template configures parameters for Cisco Unified Survivable Remote Site Telephony (SRST) for SIP. With Cisco Unified SRST, if the WAN goes down or is degraded, SIP IP phones in a branch site can register to the local gateway so that they continue to function for emergency services. Use this procedure to add and configure such a template.

The SRST feature template allows you to define global SRST settings, such as system messages and maximum phone/directory numbers, as well as individual phone profiles for SIP phones.

•

Before you begin

Ensure you have selected the supported device to which you want to add Cisco Unified SRST features in Cisco SD-WAN Manager.

Follow these steps to add an SRST feature template:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**, and click **Add Template**.

In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

Step 3 Select the supported device to which you want to add Cisco Unified SRST features.

Step 4 Click **SRST** from the Unified Communications templates.

Step 5 In **Template Name**, enter a name for the template.

This field can contain uppercase and lowercase letters, digits 0 through 9, hyphens (-), and underscores (_).

Step 6 In **Description**, enter a description for the template.

This field can contain any characters and spaces.

Step 7 In **Global Settings**, configure options as described in the Global Cisco Unified SRST Options, on page 332 topic.

Step 8 From **Phone Profile**, click **New Phone Profile** to create a phone profile, and configure options as described in the SRST Phone profile options, on page 333 topic.

A phone profile provides pool tag and device network information for a SIP phone.

You can add as many phone profiles as needed. Click **Add** after you configure each phone profile.

If any phone profiles already are configured, they appear in the phone profiles table on this page. To edit a configured phone profile, click **…**, and click its pencil icon. Edit the options in the window that pops up as described in the table, and click **Save Changes**. To delete a phone profile, click **…**, and click its trash can icon.

Step 9 Click **Save**.

An SRST feature template is successfully added and configured.

What to do next

Proceed to add a DSPFarm Feature Template if required for your Unified Communications deployment.

Global Cisco Unified SRST Options

This reference topic describes the global options available for configuring Cisco Unified Survivable Remote Site Telephony (SRST) parameters. These settings define system-wide behaviors for SRST mode, including messages, phone capacity, and music on hold.

Table 102: Global Cisco Unified SRST Options

Option	Description	Cisco IOS CLI Equivalent
System Message	Enter a message that displays on endpoints when Cisco Unified SRST mode is in effect.	**voice register global** **system message** *string*
Max Phones	Enter the number of phones that the system can register to the local gateway when in Cisco Unified SRST mode. The available values and the maximum values that you can enter in this field depend on the device that you are configuring. Hover your mouse pointer over the Information icon next to this field to see maximum values for supported devices.	**voice register global** **max-pool** *max-voice-register-pools*
Max Directory Numbers	Enter the number of DNs that the gateway supports when in Cisco Unified SRST mode. The available values and the maximum values that you can enter in this field depend on the device that you are configuring. Hover your mouse pointer over the Information icon next to the Max phones to support field to see maximum values for supported devices.	**voice register global** **max-dn** *max-directory-numbers*

Option	Description	Cisco IOS CLI Equivalent
Music on Hold	Select **Yes** to play music on hold on endpoints when a caller is on hold when in Cisco Unified SRST mode. Otherwise, select **No**.	—
Music on Hold file	Enter the path and file name of the audio file for music on hold. The file must be in the system flash and must be in .au or .wav format. In addition, the file format must contain 8-bit 8-kHz data, for example, CCITT a-law or u-law data format.	**call-manager-fallback** **moh** *filename*

SRST Phone profile options

This reference topic describes the options available for configuring individual SRST phone profiles. These settings define the network identification for SIP phones registering to a local gateway in SRST mode.

Table 103: SRST Phone Profile Options

Option	Description	Cisco IOS CLI Equivalent
Voice Register Pool Tag	Enter the unique sequence number of the IP phone to be configured. The maximum value is defined by the Max phones to support option in the Global tab of the SRST feature template.	**voice register pool** *pool-tag*
Device Network IPv6 Prefix	Enter the IPv6 prefix of the network that contains the IP phone to support. For example, a.b.c.d/24.	**voice register pool** *pool-tag* **id** [**network** *address* **mask** *mask*]
Device Network IPv4 Prefix	Enter the IPv4 prefix of the network that contains the IP phone to support.	**voice register pool** *pool-tag* **id** [**network** *address* **mask** *mask*]

Add a DSPFarm feature template

A DSP farm is a pool of Digital Signal Processor (DSP) resources on a router used by Cisco Unified Communications Manager for controlled transcoding, conferencing (non-secure only), and media termination point (MTP) services. A DSPFarm feature template is used to set up and provision a DSP farm. Use this procedure to add and configure such a template.

When you add a DSPFarm feature template, you configure options for the following items:

- Media resource modules—DSP modules and their placement on a router. You determine and build DSP farm profiles based on media resource modules.
- DSP farm profiles—Each profile defines parameters for provisioning a specific DSP farm service type. A profile includes options for provisioning a group of DSP resources that is used for transcoding, conferencing (only non-secure conferencing is supported), or MTP services. A profile is registered to a

Cisco Unified Communications Manager so that the Cisco Unified Communications Manager can invoke the resources for a service as needed.

- SCCP config—Configures a local interface that is used to communicate with up to four Cisco Unified Communications Manager servers, and configures related information that is required to register the DSP farm profiles to Cisco Unified Communications Manager. Also configures one or more Cisco Unified Communications Manager groups, each of which includes up to four Cisco Unified Communications Manager servers that control the DSP farm services that, in turn, are associated with the servers.

Before you begin

Ensure you have selected the supported device to which you want to add a DSP farm in Cisco SD-WAN Manager.

Follow these steps to add a DSPFarm feature template:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**, and click **Add Template**.

Note
In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

Step 3 Select the supported device to which you want to add a DSP farm.

Step 4 Click **DSPFarm** from the **Unified Communications** templates.

Step 5 In **Template Name**, enter a name for the template.

This field can contain uppercase and lowercase letters, digits 0 through 9, hyphens (-), and underscores (_).

Step 6 In **Description**, enter a description for the template.

This field can contain any characters and spaces.

Step 7 Configure the DSPFarm parameters.

a) From **Media Resources Modules**, click **Add Media Resources**, and configure options as described in the Media resource options, on page 335 topic.

A media resource module is a DSP module that is used by DSP Farm profiles.

You can add as many media resources interfaces as needed.

Click **Add** after you configure each media resource. After you configure a media resource, you cannot modify or delete it because other configuration items are based on the module and its placement. If you need to change a media resource configuration, you must remove the DSPFarm feature template and create a new one.

If any media resources are already configured, they appear in the table in this tab. To edit a configured media resource, click **…**, and click its pencil icon. Edit the options in the window that pops up as described in the Media Resource Options table, and click **Save Changes**. To delete a media resource, click **…**, and click its trash can icon.

b) From **Profile**, click **Add New Profile** to add a profile for a DSP farm service on a router, and configure options for the profile as described in the DSPFarm service options, on page 335 topic.

Click **Add** after you configure a profile. You can add up to 10 DSP farm profiles for each feature template.

Before you create a profile, you must know the maximum number of sessions that can be configured with the DSP resources that are available on the router. These resources are based on the type of modules in the router. To determine these resources, you can use a DSP calculator.

After you add a profile, you can modify the List Codec, Maximum Sessions, Maximum Conference Participants, and Shutdown options. You cannot change the profile type. If you want to change the profile type, you must delete the profile and create a new one.

If any profiles are already configured, they appear in the table in this tab. To edit a configured profile, click **…**, and click its pencil icon. Edit the options in the window that pops up as described in the "DSP Farm Service Options" table, and click **Save Changes**. To delete a profile, click **…**, and click its trash can icon.

c) In **SCCP Config**, configure options as described in the SCCP options, on page 339 topic.

Step 8 Click **Save**.

A DSPFarm feature template is successfully added and configured.

What to do next

Proceed to add a voice policy if required for your Unified Communications deployment.

Media resource options

This reference topic describes the options available for configuring media resources within a DSPFarm feature template. These settings define the router resource modules that carry DSP resources and their physical placement (slot/sub-slot ID).

Table 104: Media Resource Options

Option	Description	Cisco IOS CLI Equivalent
Module	Select the router resource module to carry DSP resources that are used by DSPFarm profiles.	—
Slot/sub-slot ID	Select the slot and sub-slot in which the resource module that you selected resides.	**voice-card** *slot*/*subslot* **dsp service dspfarm**

DSPFarm service options

This reference topic describes the options available for configuring DSP farm services within a DSPFarm feature template. These settings define the type of DSP farm service (Transcoder, Conference, or MTP), codecs, maximum participants/sessions, and other service-specific parameters.

Table 105: DSP Farm Service Options

Option	Description	Cisco IOS CLI Equivalent
Profile Type	Select the type of DSP farm service that this profile is for. Options are **Transcoder**, **Conference**, and **MTP**	**dspfarm profile** *profile-identifier* {**conference** | **mtp** | **transcode**}
Profile ID	A system-generated unique identifier for the profile.	—
Universal	Available if you select Transcoder for the Profile Type When this check box is unchecked, transcoding is allowed only between the G.711 codec and other codecs. When this check box is checked, transcoding is allowed between codecs of any type.	**dspfarm profile** *profile-identifier* **transcode** [**universal**]

Option	Description	Cisco IOS CLI Equivalent
List Codec	Select the codecs that are available for the DSP farm service that this profile defines. The following codecs are supported. For MTP profile types, you can select one option, or you can select **pass-through** and one other option. If you want to change a codec, unselect the current codec before selecting a new one. • For the Transcoder profile type: • g711alaw, g711ulaw, g729abr8, g729ar8, g729br8, g729r8, g722-64, ilbc, iSAC • For the Conference profile type: • g711alaw, g711ulaw,g722r-64, g729abr8, g729ar8, g729br8, g729r8 • For the MTP profile type for software MTP only: • g711ulaw, g711alaw, g722-64, g729abr8, g729ar8, g729br8, g729r8, ilbc, iSAC, pass-through • For the MTP profile type for hardware MTP only, or for hardware and software MTP: • g711ulaw, g711alaw, pass-through	**codec** *codec-name*
Conference Maximum Participants	Available if you select Conference for the Profile Type. Select the maximum number of parties that can participate in a conference bridge (**8**, **16**, or **32**).	**maximum conference-participants** *number*

Option	Description	Cisco IOS CLI Equivalent
Maximum Sessions	Available if you select Transcoder or Conference for the Profile Type. Enter the maximum number of sessions that this profile can support. This value depends on the maximum number sessions that can be configured with the DSP resources that are available on the router. These resources are based on the type of modules in the router. To determine these resources, you can use a DSP calculator.	**maximum sessions** *number*
MTP Type	Available if you select MTP for the Profile Type. Select the way in which the router performs minor MTP translations such as G.711alaw to G.711ulaw, and DTMF conversions. Options are: • **Hardware**—MTP translations and conversions are performed by the hardware DSP resources • **Software**—MTP translations and conversions are performed by the router CPU	**maximum session** {**hardware** | **software**}
MTP Maximum Hardware Sessions	Available if you select Hardware for the MTP type. Select the maximum number of hardware sessions that can be used for MTP translations and conversions. Maximum value: 4000	**maximum session hardware** *number*
MTP Maximum Software Sessions	Available if you select Software for the MTP type. Select the maximum number of CPU sessions that can be used for MTP translations and conversions. Maximum value: 6000	**maximum session software** *number*

Option	Description	Cisco IOS CLI Equivalent
Application	Select the type of application to which the DSP farm services that are provisioned on the device are associated.	**associate application sccp**
Shutdown	Enable this option to take this profile out of service.	**shutdown**

SCCP options

This reference topic describes the options available for configuring SCCP (Signaling Connection Control Part) within a DSPFarm feature template. These settings define the local interface for SCCP communication and the Cisco Unified Communications Manager servers and groups to which DSP farm profiles will register.

Table 106: SCCP Options

Option	Description	Cisco IOS CLI Equivalent
CUCM Tab Configure up to 12 Cisco Unified Communications Manager servers to which the profiles that you defined in the Profile tab register.		

Option	Description	Cisco IOS CLI Equivalent
Local Interface	Enter the local interface that DSP services that are associated with the SCCP application use to register with Cisco Unified Communications Manager. Enter the interface in this format: *interface-type*/*interface-numberport* where: • *interface-type*—Type of interface that the services use to register with Cisco Unified Communications Manager. The type can be a GigabitEthernet interface or a port channel interface. • *interface-number*—Interface number that the services use to register with Cisco Unified Communications Manager. • *port*—(Optional) Port on which the interface communicates with Cisco Unified Communications Manager. If you do not specify a port, the default value 2000 is used. For example: GigabitEthernet0/0/0.	**sccp local** *interface-type interface-number* [**port** *port-number*]

Option	Description	Cisco IOS CLI Equivalent
Server List - *x*	Designate a Cisco Unified Communications Manager server to which the profiles that you defined in the Profile tab register. In the first field, enter the IP address or DNS name of the Cisco Unified Communications Manager server. In the second field, enter a numerical identifier for the Cisco Unified Communications Manager server. Click the Plus Sign icon (+) to configure up to 11 additional servers. To remove a server, click its corresponding Minus Sign icon. (–).	**sccp ccm** {*ipv4-address* | *ipv6-address* | *dns*} **identifier** *identifier-number* **version 7.0+**
CUCM Groups Tab This tab is available when at least one Cisco Unified Communications Manager server is configured in the Cisco Unified Communications Manager tab. Configure a Cisco Unified Communications Manager group, which includes up to 4 Cisco Unified Communications Manager servers that control the DSP farm services that, in turn, are associated with the servers. If any Cisco Unified Communications Manager groups are already configured, they appear in the table in this tab. To edit a configured Cisco Unified Communications Manager group, click its pencil icon in the Action column, edit the options in the window that pops up as described in the following rows, and click **Save Changes**. To delete a Cisco Unified Communications Manager group, click its trash can icon in the Action column.		
Add New CUCM Group	Click to add a new Cisco Unified Communications Manager group.	**sccp ccm group** *group-id*

Option	Description	Cisco IOS CLI Equivalent
Server Groups Priority Order	Select the priority in which the Cisco Unified Communications Manager servers in this Cisco Unified Communications Manager group are used. To do so: 1. Click this field to display a list of the Cisco Unified Communications Manager servers that you configured on the Cisco Unified Communications Manager tab. 2. Select the server that you want to be the primary server. This server has the highest priority. 3. Click the field again and select the server that you want to be the redundant server with the next highest priority. Repeat this step to select other redundant servers. The servers appear in this field in priority order. To remove a server from the group, click its X icon. To change the priority order of servers, remove the servers and add them back in the desired order.	**associate ccm** *cisco-unified-communications-manager-id* **priority** *priority*

Option	Description	Cisco IOS CLI Equivalent
CUCM Media Resource Name Profile to be Associated	In the Cisco Unified Communications Manager Media Resource Name field, enter a unique name that is used to register a DSP farm profile to the Cisco Unified Communications Manager servers. The name must contain from 6 to 15 characters. Characters can be letter, numbers, slashes (/), hyphens (-), and underscores (_). Space characters are not allowed. In the corresponding Profile to be Associated field, select a DSP farm profile to be registered to this Cisco Unified Communications Manager group using the name that you entered. To select a profile, click this field to display a list of the profile IDs that were configured on the Profile tab, and click the ID of the profile that you want. To add another Cisco Unified Communications Manager media resource name and profile, click the plus sign (+). You can add up to 4 Cisco Unified Communications Manager media resources and profiles. To remove a Cisco Unified Communications Manager media resource name and profile, click its corresponding minus sign (–).	**associate ccm** *profile-identifier* **register** *device-name*

Option	Description	Cisco IOS CLI Equivalent
CUCM Switchback	Select the switchback method that the Cisco Unified Communications Manager servers in this Cisco Unified Communications Manager group use to switch back after a failover: • **graceful**—Switchback occurs after all active sessions terminate gracefully. • **guard**—Switchback occurs either when active sessions are terminated gracefully or when the guard timer expires, whichever happens first. • **immediate**—Performs the Cisco Unified Communications Manager switchback to the higher priority Cisco Unified Communications Manager immediately when the timer expires, whether there is an active connection or not. Default: **graceful**.	**switchback method** {**graceful** | **guard** [*timeout-guard-value*] | **immediate**}
CUCM Switchover	Select the switchover method that Cisco Unified Communications Manager servers in this Cisco Unified Communications Manager use group when failing over: • **graceful**—Switchback occurs after all active sessions terminate gracefully. • **immediate**—Switchover occurs immediately, whether there is an active connection or not. Default: **graceful**.	**switchover method** {**graceful** | **immediate**}

Add a voice policy

A voice policy defines how the system augments and manipulates calls for various endpoint types. This supertask guides you through the process of creating a new voice policy and configuring its subpolicies for different communication endpoints.

Voice policies are crucial for tailoring call functionality for specific endpoints, including voice ports, POTS dial peers, SIP dial peers, and Cisco Unified SRST phone profiles.

Before you begin

Follow these steps to add a voice policy:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Unified Communications**.

Step 2 Click **Add Voice Policy**.

Step 3 In **Voice Policy Name**, enter a name for the policy.

Step 4 Configure the required subpolicies:

a) Configure voice ports for a voice policy.

Define how the system augments and manipulates calls for voice port endpoint types. See Configure voice ports for a voice policy, on page 345.

b) Configure POTS Dial Peers for a voice policy.

Define how the system augments and manipulates calls for POTS dial peer endpoint types. See Configure POTS dial peers for a voice policy, on page 361.

c) Configure SIP Dial Peers for a voice policy.

Define how the system augments and manipulates calls for SIP dial peer endpoint types. See Configure SIP Dial Peers for a voice policy, on page 370.

d) Configure SRST Phones for a voice policy.

Define how the system augments and manipulates calls for Cisco Unified SRST phone endpoint types. See Configure SRST phones for a voice policy, on page 383

Step 5 Click **Save Policy**.

A voice policy is successfully added and configured with its respective subpolicies.

What to do next

Proceed to provision a device template for Unified Communications to apply this voice policy to your devices.

Configure voice ports for a voice policy

This task defines how the system augments and manipulates calls for the voice port endpoint type within a voice policy. It allows you to set up various call functionality options such as trunk groups, translation rules, and line parameters.

When configuring voice ports for a voice policy, you define specific call functionality options depending on the type of voice card you are using (FXO, FXS, PRI ISDN, or FXS DID). These settings ensure calls are handled correctly based on your network requirements.

Before you begin

You must be in the process of adding a new voice policy or editing an existing one within Cisco SD-WAN Manager.

Follow these steps to configure voice ports for a voice policy:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Unified Communications**.

Step 2 Click **Add Voice Policy**, and choose **Voice Ports**.

Step 3 In **Voice Ports**, enter a name for the policy

From the **Add Voice Ports Policy Profile** drop-down list, select **Create New**.

Alternatively, you can select **Copy from Existing** to reuse settings from an existing policy profile.

Step 4 Select **FXO**, **FXS**, **PRI ISDN**, or **FXS DID** to specify the type of voice port that the policy is for.

Step 5 Select the types of call functionality policy options that you want to configure from the list of options that displays, and click **Next**.

Available options include **Trunk Group**, **Translation Profile**, **Station ID**, **Line Params**, **Tuning Params**, **Supervisory Disconnect**, and **DID Timers**

Step 6 Configure the selected call functionality options on the tabs that display: a.

a) For **Trunk Group** options, configure settings as described in the Voice Ports Trunk Group Options topic.

Define how voice ports function as members of a trunk group. After saving, configure priority by double-clicking the Priority field (1-64). If any trunk groups are already configured, they appear in the table. To edit, click **…** and select its pencil icon; to delete, select its trash can icon.

b) For **Translation Profile** options, configure settings as described in the Voice ports translation profile options, on page 351 topic.

Define translation rules for calling and called numbers. After saving, double-click the dash (-) in the **Direction** column to select **Incoming** or **Outgoing**. You can create up to two translation profiles for this endpoint.

You can create up to two translation profiles for this endpoint.

c) For **Station ID** options, configure settings as described in the Voice ports station ID options, on page 354 topic.

Define the name and number for caller ID display.

d) For **Line Params** options, configure settings as described in the Voice ports line parameters options, on page 354 topic.

Define line parameters for voice quality.

e) For **Tuning Params** options, configure settings as described in the Voice Ports Tuning Parameters Options topic.

Define parameters for signaling between voice ports and other instruments.

f) For **Supervisory Disconnect** options, configure settings as described in the Voice ports supervisory disconnect options, on page 358 topic.

Define parameters for supervisory disconnect events. You can configure as many supervisory disconnect events as needed.

g) For **DID Timers** options, configure settings as described in the Voice ports DID timers options, on page 360 topic.

Define timers for Direct Inward Dialing (DID) calls.

Step 7 Click **Next**.

Step 8 In **Policy Profile Name**, enter a name for this child policy.

Step 9 In **Policy Profile Description**, enter a description for this child policy.

Step 10 Click **Save**.

The voice ports for the voice policy are successfully configured.

What to do next

Return to the main Add a Voice Policy supertask to continue configuring other subpolicies (POTS Dial Peers, SIP Dial Peers, SRST Phones) as needed.

Voice ports trunk group options

This reference topic describes the options available for configuring trunk groups for voice ports within a voice policy. These settings define how voice ports function as members of a trunk group, including hunt schemes and call limits.

Table 107: Trunk group options

Option	Description	Cisco IOS CLI Equivalent
Add New Trunk Group	Click to add a trunk group for the selected card. You can add one trunk group for a voice port.	—
Copy from Existing	Click to copy an existing trunk group to a new trunk group. In the box that appears, change the name if desired, select a trunk group, and click **Copy**.	—
Name	Name of the trunk group. The name can contain up to 32 characters.	**trunk group** *name*

Option	Description	Cisco IOS CLI Equivalent
Hunt-Scheme		**trunk group** *name* **hunt-scheme least-idle** [**both** | **even** | **odd**] **hunt-scheme least-used** [**both** | **even** | **odd**] **hunt-scheme longest-idle** [**both** | **even** | **odd**] **hunt-scheme round-robin** [**both** | **even** | **odd**] **hunt-scheme sequential** [**both** | **even** | **odd**] **hunt-scheme random**

Option	Description	Cisco IOS CLI Equivalent
	Select the hunt scheme in the trunk group for outgoing calls: • **least-idle both**—Searches for an idle channel with the shortest idle time • **least-idle even**—Searches for an idle even-numbered channel with the shortest idle time • **least-idle odd**—Searches for an idle odd-numbered channel with the shortest idle time • **least-used both**—Searches for a trunk group member that has the highest number of available channels (applies only to PRI ISDN cards) • **least-used even**—Searches for a trunk group member that has the highest number of available even-numbered channels (applies only to PRI ISDN cards) • **least-used odd**—Searches for a trunk group member that has the highest number of available odd-numbered channels (applies only to PRI ISDN cards) • **longest-idle both**—Searches for an idle odd-numbered channel with the longest idle time • **longest-idle even**—Searches for an idle channel that has the highest number of available even-numbered channels • **longest-idle odd**—Searches for an idle channel that has the highest number of available odd-numbered channels • **round-robin both**—Searches trunk group members in turn for an idle channel, starting with the trunk group member that follows the last used member • **round-robin even**—Searches trunk group member in turn for an idle even-numbered channel, starting with the trunk group member that follows the last used member	

Option	Description	Cisco IOS CLI Equivalent
	• **round-robin odd**—Searches trunk group member in turn for an idle odd-numbered channel, starting with the trunk group member that follows the last used member • **sequential-both**—Searches for an idle channel, starting with the trunk group member with the highest preference within the trunk group • **sequential-even**—Searches for an idle even-numbered channel, starting with the trunk group member with the highest preference within the trunk group • **sequential-odd**—Searches for an idle odd-numbered channel, starting with the trunk group member with the highest preference within the trunk group • **random**—Searches for a trunk group member at random and selects a channel from the member at random Default: least-used both	
Max Calls	Enter the maximum number of calls that are allowed for the trunk group. If you do not enter a value, there is no limit on the number of calls. If the maximum number of calls is reached, the trunk group becomes unavailable for more calls. • In field—Enter the maximum number of incoming calls that are allowed for this trunk group • Out field— Enter the maximum number of outgoing calls that are allowed for this trunk group Valid range for both fields: integers 0 through 1000.	**trunk group** *name* **max-calls voice** *number-of-calls* **direction** [**in** | **out**]

Option	Description	Cisco IOS CLI Equivalent
Max-Retry	Select the maximum number of outgoing call attempts that the trunk group makes if an outgoing call fails. If you do not enter a value and a call fails, the system does not attempt to make the call again. Valid range: integers 1 through 5.	**trunk group** *name* **max-retry** *attempts*
Save Trunk Group	Click to save the Trunk Group that you configured.	—

Voice ports translation profile options

This reference topic describes the options available for configuring translation profiles for calling and called numbers for voice ports within a voice policy. These settings allow you to define rules for matching and replacing number strings.

Table 108: Translation profile options

Option	Description	Cisco IOS CLI Equivalent
Add New Translation Profile	Click to add a translation profile for the selected card. You can create up to two translation profiles for this endpoint.	**voice translation-profile** *name*
Copy from Existing	Click to copy an existing translation profile to a new translation profile. In the box that appears, change the name if desired, select a called translation rule and a calling translation rule, and click **Copy**.	—
Calling	Click to configure translation rules for the number that is calling in. The Translation Rules pane displays.	**translate calling** *translation-rule-number*
Called	Click to configure translation rules for the number that is being called. The Translation Rules pane displays.	**translate called** *translation-rule-number*

Option	Description	Cisco IOS CLI Equivalent
Translation Rules pane		**voice translation-rule** *number* Match and Replace Rule: **rule** *precedence* /*match-pattern*/ / *replace-pattern*/ Reject Rule: **rule** *precedence* **reject** /*match-pattern*/

Option	Description	Cisco IOS CLI Equivalent
	1. Click **Add New** to create a translation rule. Alternatively, you can click **Copy From Existing** to copy an existing translation rule to a new translation rule. In the box that appears, change the name if desired, select a called translation rule and a calling translation rule, and click **Copy**. 2. In the Translation Rule Number field, enter a unique number that designates the precedence for this rule. Valid range: integers 1 through 100. 3. (Optional) To copy existing translation rules from a CSV file, click **Import**. Continue to add rules or click **Finish**. For detailed information about this file, see Translation rules CSV file, on page 390. 4. Click **Add Rule**. 5. In the Match field, enter the string that you want the translation rule to affect. Enter the string in regular expression format beginning and ending with a slash (/). For example, /^9/. To include the backslash character (\) in a match string, precede the backslash with a backslash. 6. From the Action drop-down list, select the action that the system performs for calls that match the string in the Match field. The **Reject** option causes the system to reject the call. The **Replace** option causes the system to replace the match number with a value that you specify. 7. If you select the **Replace** action, in the Replace field that displays, enter the string to which to translate the matched string. Enter the number in regular expression format beginning and ending with a slash (/). For example, //, which indicates a replacement of no string.	

Option	Description	Cisco IOS CLI Equivalent
	To include the backslash character (\) in a replace string, precede the backslash with a backslash. As an example, if you specify a match string of /^9/ and a replace string of //, the system removes the leading 9 from calls with a number that begins with 9. In this case, the system translates 914085551212 to 14085551212. **8.** Click **Save**. **9.** Add more translation rules as needed. **10.** (Optional) Click **Export** to save the translation rules that you created in a CSV file. **11.** Click **Finish** at the bottom of the pane.	

Voice ports station ID options

This reference topic describes the options available for configuring station ID information for voice ports within a voice policy. These settings define the name and number displayed for caller ID.

Table 109: Station ID Options

Option	Description	Cisco IOS CLI Equivalent
Station Name	Enter the name of the station. The station name can contain up to 50 letters, numbers, and spaces, dashes (-), and underscores (_).	**station-id name** *name*
Station Number	Enter the phone number of the station in E.164 format. The station number can contain up to 15 numeric characters.	**station-id number** *number*

Voice ports line parameters options

This reference topic describes the options available for configuring line parameters for voice ports within a voice policy. These settings control voice quality aspects such as gain, attenuation, echo cancellation, and companding type.

Table 110: Line Parameters Options

Option	Description	Cisco IOS CLI Equivalent
Gain	Enter the gain, in dB, for voice input. Valid range: –6 through 14. Default: 0	**input gain** *decibels*
Attenuation	Enter the amount of attenuation, in dB, for transmitted voice output. Valid range: –6 through 14. Default: 3.	**output attenuation** *decibels*
Echo Canceller	Select **Enable** to apply echo cancellation to voice traffic. By default, this option is enabled.	**echo-cancel** *enable*
Voice Activity Detection (VAD)	Select **Enable** to apply VAD to voice traffic. By default, this option is enabled.	**vad**
Compand Type	Select the companding standard to be used to convert between analog and digital signals in PCM systems (**U-law** or **A-law**). Default: U-Law.	**compand-type** {**u-law** | **a-law**}
Impedance	This field does not apply to PRI ISDN cards. Select the terminating impedance for calls. Default: 600r.	**impedance** {**600c** | **600r 900c** | **900r** | **complex1** | **complex2** | **complex3** | **complex4** | **complex5** | **complex6**}
Call Progress Tone	Select the locale for call progress tones.	**cptone** *locale*

Voice ports tuning parameters options

This reference topic describes the options available for configuring tuning parameters for voice ports within a voice policy. These settings define signaling parameters between voice ports and other instruments, with specific options for FXO and FXS cards.

Table 111: Tuning Parameters Options

Option	Description	Cisco IOS CLI Equivalent
Tuning Params Options for FXO Cards		
Pre Dial Delay	Enter the delay, in seconds, of the delay on the FXO interface between the beginning of the off-hook state and the initiation of DTMF signaling. Valid range: 0 through 10. Default: 1.	**pre-dial-delay** *seconds*

Option	Description	Cisco IOS CLI Equivalent
Supervisory Disconnect	Select the type of tone that indicates that a call has been released and that a connection should be disconnected: • **Anytone**—Any tone indicates a supervisory disconnect • **Signal**—A disconnect signal indicates a supervisory disconnect • **Dualtone**—A dual-tone indicates a supervisory disconnect Default: Signal.	Anytone: supervisory disconnect **anytone** Signal: supervisory disconnect Dualtone: supervisory disconnect **dualtone** {**mid-call** | **pre-connect**}
Dial Type	Select the dialing method for outgoing calls: • **pulse**—Pulse dialer • **dtmf**—Dual-tone multifrequency dialer • **mf**—Multifrequency dialer Default: dtmf.	**dial-type** {**dtmf** | **pulse** | **mf**}
Timing Sup-Disconnect	Enter the minimum time, in milliseconds, that is required to ensure that an on-hook indication is intentional and not an electrical transient on the line before a supervisory disconnect occurs (based on power denial signaled by the PSTN or PBX). Valid range: 50 through 1500. Default: 350.	**timing sup-disconnect** *milliseconds*
Battery Reversal	Battery reversal reverses the battery polarity on a PBX when a call connects, then changes the battery polarity back to normal when the far-end disconnects. Select **Answer** to configure the port to support answer supervision by detection of battery reversal. Select **Detection Delay** to configure the delay time after which the card acknowledges a battery-reversal signal, then enter the delay time in milliseconds. Valid range: 0 through 800. Default: 0 (no delay). If an FXO port or its peer FXS port does not support battery reversal, do not configure battery reversal options to avoid unpredictable behavior.	**battery-reversal** [**answer**] **battery-reversal-detection-delay** *milliseconds*

Option	Description	Cisco IOS CLI Equivalent
Timing Hookflash out	Enter the duration, in milliseconds, of hookflash indications that the gateway generates on the FXO interface. Valid range: 50 through 1550. Default: 400.	**timing hookflash-out** *milliseconds*
Timing Guard out	Enter the number of milliseconds after a call disconnects before another outgoing call is allowed. Valid range: 300 through 3000. Default: 2000.	**timing guard-out** *milliseconds*
Tuning Params Options for FXS Cards		
Timing Hookflash In	Enter the minimum and maximum duration, in milliseconds, of an on-hook condition to be interpreted as a hookflash by the FXS card. Valid range for minimum duration: 0 through 400. Default minimum value: 50. Valid range for maximum duration: 50 through 1500. Default maximum value: 1000.	**timing hookflash-in** *maximum-milliseconds minimum-milliseconds*
Pulse Digit Detection	To enable pulse digit detection at the beginning of a call, select **Yes**. Default: Yes.	**pulse-digit-detection**
Loop Length	Select the length for signaling on FXS ports (**Long** or **Short**). Default: Short.	**loop-length** [**long** | **short**]
Ring	• **Frequency**—Select the frequency, in Hz, of the alternating current that, when applied, rings a connected device. Default: 25. • **DC Offset**—Applies only if Loop Length is set to Long. Select the voltage threshold below which a ring does not sound on devices. Valid values: 10-volts, 20-volts, 24-volts, 30-volts, and 35-volts.	**ring frequency** *number* **ring dc-offset** *number*
Ringer Equivalence Number (REN)	Select the REN for calls that this card processes. This number specifies the loading effect of a telephone ringer on a line. Valid range: 1 through 5. Default: 1.	**ren** *number*

Voice ports supervisory disconnect options

This reference topic describes the options available for configuring supervisory disconnect events for voice ports within a voice policy. These settings define how the system detects and handles call disconnections, particularly for FXO cards.

Table 112: Supervisory Disconnect Options

Option	Description	Cisco IOS CLI Equivalent
Add New Supervisory Disconnect	Click to add a supervisory disconnect event.	—
Mode	Choose the mode for the supervisory disconnect event: • **Custom CPTone**—Provides options for configuring cptone detection parameters for a supervisory disconnect event • **Dual Tone Detection Params**—Provides options for configuring dual-tone detection parameters for a supervisory disconnect event	**voice class custom-cptone** *cptone-name* **voice class dualtone-detect-params** *tag*
Supervisory Name	Applies to Custom CPTone mode. Enter a name for the supervisory disconnect event. The name can contain up to 32 characters. Valid characters are letters, numbers, dashes (-), and underscores (_).	**voice class custom-cptone** *cptone-name*
Dualtone	Applies to Custom CPTone mode. Select the type of dual-tone that causes a disconnect. Options are: • Busy • Disconnect • Number Unobtainable • Out of Service • Reorder • Ringback	**dualtone** {**ringback** |**busy** | **reorder** | **out-of-service** | **number-unobtainable** | **disconnect**}
Cadence	Applies to Custom CPTone mode. Enter the cadence interval, in milliseconds, of the dual-tones that cause a disconnect. Enter the cadence as an on/off value pair, separated with a space. You can enter up to 4 on/off value pairs, separated with a space.	**cadence** *cycle-1-on-time cycle-1-off-time* [*cycle-2-on-time cycle-2-off-time* [*cycle-3-on-time cycle-3-off-time* [*cycle-4-on-time cycle-4-off-time*]]]

Option	Description	Cisco IOS CLI Equivalent
Dualtone Frequency	Applies to Custom CPTone mode. Enter the frequency, in Hz, of each tone in the dual-tone. Valid range for each tone is 300 through 3600.	**frequency** *frequency-1* [*frequency-2*]
Supervisory Number	Applies to Custom Dual Tone Detection Params mode. Enter a unique number to identify dual-tone detection parameters. Valid range: 1 through 10000.	**voice class dualtone-detect-params** *tag-number*
Cadence-Variation	Applies to Custom Dual Tone Detection Params mode. Enter the maximum time, in milliseconds, by which the tone onset can vary from the onset time and still be detected. The system multiplies the value that you enter by 10. Valid range: 0 through 200 in units of 10. Default: 10.	**cadence-variation** *time*

Option	Description	Cisco IOS CLI Equivalent
Frequency	Applies to Custom Dual Tone Detection Params mode. • Max Delay—Enter the maximum delay, in milliseconds, before a supervisory disconnect is performed after the dual-tone is detected. The system multiplies the value that you enter by 10. Valid range: 0 through 100 in units of 10. Default: 10. • Max Deviation—Enter the maximum deviation, in Hz, by which each tone can deviate from configured frequencies and be detected. Valid range: 10 through 125. Default: 10. • Max Power—Enter the power of the dual-tone, in dBm0, above which a supervisory disconnect is no detected. Valid range: 0 through 20. Default: 10. • Min Power— Enter the power of the dual-tone, in dBm0, below which a supervisory disconnect is not detected. Valid range: 10 through 35. Default: 30. • Power Twist—Enter difference, in dBm0, between the minimum power and the maximum power of the dual-tone above which a supervisory disconnect is not detected. Valid range: 0 through 15. Default: 6.	**freq-max-delay** *time* **freq-max-deviation** *hertz* **freq-max-power** *dBm0* **freq-min-power** *dBm0* **freq-power-twist** *dBm0*
Save	Click to save the supervisory disconnect information that you configured.	—

Voice ports DID timers options

This reference topic describes the options available for configuring DID (Direct Inward Dialing) timers for voice ports within a voice policy.

Table 113: DID Timers Options

Option	Description	Cisco IOS CLI Equivalent
Wait Before Wink	Enter the amount of time, in milliseconds, that the card waits after receiving a call before sending a wink signal to notify the remote side that it can send DNIS information. Valid range: 100 through 6500. Default: 550.	**timing wait-wink** *milliseconds*
Wink Duration	Enter the maximum amount of time, in milliseconds, of the wink signal for the card. Valid range: 50 through 3000. Default: 200.	**timing wait-duration** *milliseconds*
Clear Wait	Enter the minimum amount of time, in milliseconds, between an inactive seizure signal and the call being cleared for the card. Valid range: 200 through 2000. Default: 400.	**timing clear-wait** *milliseconds*
Dial Pulse Min Delay	Enter the amount of time, in milliseconds, between wink-like pulses for the card. Valid range: 0 or 140 through 5000. Default: 140.	**timing dial-pulse min-delay** *milliseconds*
Answer Winkwidth	Enter the minimum delay time, in milliseconds, between the start of an incoming seizure and the wink signal. Valid range: 110 through 290. Default: 210.	**timing answer-winkwidth** *milliseconds*

Configure POTS dial peers for a voice policy

This task defines how the system augments and manipulates calls for the POTS dial peer endpoint type within a voice policy. It allows you to configure options such as trunk groups and translation profiles to manage call flow.

When configuring POTS dial peers for a voice policy, you define specific options that control how the system handles calls for this endpoint type. This includes settings for how calls are routed through trunk groups and how calling/called numbers are translated. Trunk Group configuration for POTS Dial Peers is available beginning with Cisco IOS XE Catalyst SD-WAN Release 17.3.1a.

Before you begin

You must be in the process of adding a new voice policy or editing an existing one within Cisco SD-WAN Manager.

Follow these steps to configure POTS dial peers for a voice policy:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Unified Communications**

Step 2 Click **Add Voice Policy**, and choose **POTS Dial Peer** in the left pane.

Step 3 From the **Add POTS Dial Peer Policy Profile** drop-down list, select **Create New**.

Alternatively, you can select **Copy from Existing** to reuse settings from an existing policy profile.

Step 4 Select the types of POTS dial peers that you that you want to configure from the list of options that displays, and click **Next**.

Options include **Trunk Group** (beginning with Cisco IOS XE Catalyst SD-WAN Release 17.3.1a) and **Translation Profile**.

Step 5 Configure the selected POTS dial peer options:

a) To configure trunk groups, configure options as described in the Voice policy POTS dial peer trunk group options, on page 363 topic.

Define how POTS dial peers function within trunk groups.

You can create up to 64 trunk groups for this endpoint. If any trunk groups are already configured, they appear in the trunk groups table on this page. To edit, click **…**, and select its pencil icon; to delete, select its trash can icon. After saving, configure the priority for a trunk group by double-clicking the Priority field (1-64) and entering a number. The number you enter is the priority of the POTS dial peer in the trunk group for incoming and outgoing calls.

b) To configure translation profiles, configure options as described in the Voice policy POTS dial peer translation profile options, on page 367 topic.

Define translation rules for calling and called numbers.

You can create up to two translation profiles for this endpoint. After saving, double-click the dash (-) in the **Direction** column to select **Incoming** or **Outgoing**.

The **Incoming** selection applies the corresponding translation rule to traffic that is incoming to this endpoint. The **Outgoing** selection applies the corresponding translation rule to traffic that is outgoing from this endpoint.

Step 6 Click **Next**.

Step 7 In **Policy Profile Name**, enter a name for this child policy.

Step 8 In **Policy Profile Name**, enter a name for this child policy.

Step 9 In **Policy Profile Description**, enter a description for this child policy.

Step 10 Click **Save**.

The POTS dial peers for the voice policy are successfully configured.

What to do next

Return to the main Add a Voice Policy supertask to continue configuring other subpolicies (SIP Dial Peers, SRST Phones) as needed.

Voice policy POTS dial peer trunk group options

This reference topic describes the options available for configuring trunk groups for POTS dial peers within a voice policy. These settings define how POTS dial peers are organized into trunk groups, including hunt schemes and maximum call limits.

Table 114: POTS dial peer trunk group options

Option	Description	Cisco IOS CLI Equivalent
Add New Trunk Group	Click to add a trunk group for the selected card. You can add one trunk group for a voice port.	—
Copy from Existing	Click to copy an existing trunk group to a new trunk group. In the box that appears, change the name if desired, select a trunk group, and click **Copy**. A trunk group name whose name is preceded with "{Master}" is already associated with this voice policy. When you copy a this type of trunk group, the system reuses the existing trunk group without creating another instance of the trunk group definition. In this case, you cannot change the name.	—
Name	Name of the trunk group. The name can contain up to 32 characters.	**trunk group** *name*

Option	Description	Cisco IOS CLI Equivalent
Hunt-Scheme		**trunk group** *name* **hunt-scheme least-idle** [**both** | **even** | **odd**] **hunt-scheme least-used** [**both** | **even** | **odd**] **hunt-scheme longest-idle** [**both** | **even** | **odd**] **hunt-scheme round-robin** [**both** | **even** | **odd**] **hunt-scheme sequential** [**both** | **even** | **odd**] **hunt-scheme random**

Option	Description	Cisco IOS CLI Equivalent
	Select the hunt scheme in the trunk group for outgoing calls: • **least-idle both**—Searches for an idle channel with the shortest idle time • **least-idle even**—Searches for an idle even-numbered channel with the shortest idle time • **least-idle odd**—Searches for an idle odd-numbered channel with the shortest idle time • **least-used both**—Searches for a trunk group member that has the highest number of available channels (applies to only PRI ISDN cards) • **least-used even**—Searches for a trunk group member that has the highest number of available even-numbered channels (applies only to PRI ISDN cards) • **least-used odd**—Searches for a trunk group member that has the highest number of available odd-numbered channels (applies only to PRI ISDN cards) • **longest-idle both**—Searches for an idle odd-numbered channel with the longest idle time • **longest-idle even**—Searches for an idle channel that has the highest number of available even-numbered channels • **longest-idle odd**—Searches for an idle channel that has the highest number of available odd-numbered channels • **round-robin both**—Searches trunk group members in turn for an idle channel, starting with the trunk group member that follows the last used member • **round-robin even**—Searches trunk group member in turn for an idle even-numbered channel, starting with the trunk group member that follows the last used member	

Option	Description	Cisco IOS CLI Equivalent
	• **round-robin odd**—Searches trunk group member in turn for an idle odd-numbered channel, starting with the trunk group member that follows the last used member • **sequential-both**—Searches for an idle channel, starting with the trunk group member with the highest preference within the trunk group • **sequential-even**—Searches for an idle even-numbered channel, starting with the trunk group member with the highest preference within the trunk group • **sequential-odd**—Searches for an idle odd-numbered channel, starting with the trunk group member with the highest preference within the trunk group • **random**—Searches for a trunk group member at random and selects a channel from the member at random Default: **least-used both**	
Max Calls	Enter the maximum number of calls that are allowed for the trunk group. If you do not enter a value, there is no limit on the number of calls. If the maximum number of calls is reached, the trunk group becomes unavailable for more calls. • **In field**—Enter the maximum number of incoming calls that are allowed for this trunk group. • **Out field**— Enter the maximum number of outgoing calls that are allowed for this trunk group. Valid range for both fields: integers 0 through 1000.	**trunk group** *name* **max-calls voice** *number-of-calls* **direction** [**in** | **out**]

Option	Description	Cisco IOS CLI Equivalent
Max-Retry	Select the maximum number of outgoing call attempts that the trunk group makes if an outgoing call fails. If you do not enter a value and a call fails, the system does not attempt to make the call again. Valid range: integers 1 through 5.	**trunk group** *name* **max-retry** *attempts*

Voice policy POTS dial peer translation profile options

This reference topic describes the options available for configuring translation profiles for POTS dial peers within a voice policy. These settings allow you to define rules for matching and replacing calling and called number strings for POTS dial peer calls.

Table 115: POTS dial peer translation profile options

Option	Description	Cisco IOS CLI Equivalent
Add New Translation Profile	Click to add a translation profile for the selected POTS dial peer. You can create up to two translation profiles for this endpoint.	—
Copy from Existing	Click to copy an existing translation profile to a new translation profile. In the box that appears, change the name if desired, select a called translation rule and a calling translation rule, and click **Copy**.	—
Name	Name of the translation profile. The name can contain up to 32 characters.	**voice translation-profile** *name*
Calling	Click to configure translation rules for the number that is calling in. The Translation Rules pane displays.	**translate calling** *translation-rule-number*
Called	Click to configure translation rules for the number that is being called. The Translation Rules pane displays.	**translate called** *translation-rule-number*

Option	Description	Cisco IOS CLI Equivalent
Translation Rules pane		**voice translation-rule** *number* Match and Replace Rule: **rule** *precedence* /*match-pattern*/ / *replace-pattern*/ Reject Rule: **rule** *precedence* **reject** /*match-pattern*/

Option	Description	Cisco IOS CLI Equivalent
	1. Click **Add New** to create a translation rule. Alternatively, you can click **Copy From Existing** to copy an existing translation rule to a new translation rule. In the box that appears, change the name if desired, select a called translation rule and a calling translation rule, and click **Copy**. 2. In the Translation Rule Number field, enter a unique number that designates the precedence for this rule. Valid range: integers 1 through 100. 3. (Optional) To copy existing translation rules from a CSV file, click **Import**. Continue to add rules or click **Finish**. For detailed information about this file, see Translation rules CSV file, on page 390. 4. Click **Add Rule**. 5. In the Match field, enter the string that you want the translation rule to affect. Enter the string in regular expression format beginning and ending with a slash (/). For example, /^9/. To include the backslash character (\) in a match string, precede the backslash with a backslash. 6. From the **Action** drop-down list, select the action that the system performs for calls that match the string in the Match field. The **Reject** option causes the system to reject the call. The **Replace** option causes the system to replace the match number with a value that you specify. 7. If you select the **Replace** action, in the Replace field that displays, enter the string to which to translate the matched string. Enter the number in regular expression format beginning and ending with a slash (/). For example, //, which indicates a replacement of no string.	

Option	Description	Cisco IOS CLI Equivalent
	To include the backslash character (\) in a replace string, precede the backslash with a backslash. As an example, if you specify a match string of /^9/ and a replace string of //, the system removes the leading 9 from calls with a number that begins with 9. In this case, the system translates 914085551212 to 14085551212. **8.** Click **Save**. **9.** Add more translation rules as needed. **10.** (Optional) Click **Export** to save the translation rules that you created in a CSV file. **11.** Click **Finish** at the bottom of the pane.	

Configure SIP Dial Peers for a voice policy

This task defines how the system augments and manipulates calls for the SIP dial peer endpoint type within a voice policy. It allows you to configure options such as translation profiles, media profiles, modem pass-through, and fax protocols.

When configuring SIP dial peers for a voice policy, you define specific options that control how the system handles calls for this endpoint type. This includes settings for how calling/called numbers are translated, codec preferences, DTMF relay options, and fax capabilities.

Before you begin

You must be in the process of adding a new voice policy or editing an existing one within Cisco SD-WAN Manager.

Follow these steps to configure SIP dial peers for a voice policy:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Unified Communications**.

Step 2 Click **SIP Dial Peer**.

Step 3 From the **Add SIP Dial Peer Policy Profile** drop-down list, choose **Create New**.

Alternatively, you can select **Copy from Existing** to reuse settings from an existing policy profile.

Step 4 Select the policy types that you want to create and click **Next**.

Step 5 In the page that displays, configure options in the tabs as needed:

a) For Translation Profile options, configure settings as described in the Voice policy SIP dial peer translation profile options, on page 371 topic.

Define translation rules for calling and called numbers.

After you click **Finish** when configuring a translation profile, you can add another translation profile (up to two for this endpoint). Click **Save Translation Profile**. For each translation profile, double-click the dash (-) in the **Direction** column to select **Incoming** or **Outgoing**.

b) For Media Profile options, configure settings as described in the Voice policy SIP Dial Peer Media profile options, on page 375 topic.

Define codecs and DTMF relay options for SIP calls.

c) For Modem Pass-through options, configure settings as described in the Voice Policy SIP Dial Peer Modem Pass-Through Options topic.

Configure the modem pass-through feature for this endpoint.

d) For Fax Protocol options, configure settings as described in the Voice policy SIP dial peer fax protocol options, on page 377 topic.

Configure the fax protocol capability for this endpoint.

Step 6 Click **Next**.

Step 7 In **Policy Profile Name**, enter a name for this child policy.

Step 8 In **Policy Profile Description**, enter a description for this child policy.

Step 9 Click **Save**.

The SIP dial peers for the voice policy are successfully configured.

What to do next

Return to the main Add a Voice Policy supertask to continue configuring other subpolicies (SRST Phones) as needed.

Voice policy SIP dial peer translation profile options

This reference topic describes the options available for configuring translation rules for calling and called numbers for SIP dial peers within a voice policy. These settings allow you to define rules for matching and replacing number strings for SIP dial peer calls.

Table 116: Voice policy SIP dial peer translation profile options

Option	Description	Cisco IOS CLI Equivalent
Add New Translation Profile	Click to add a translation profile for the selected SIP dial peer. You can create up to two translation profiles for this endpoint.	**voice translation-profile** *name*
Copy from Existing	Click to copy an existing translation profile to a new translation profile. In the box that appears, change the name if desired, select a called translation rule and a calling translation rule, and click **Copy**.	—

Option	Description	Cisco IOS CLI Equivalent
Calling	Click to configure translation rules for the number that is calling in. The Translation Rules pane displays.	**translate calling** *translation-rule-number*
Called	Click to configure translation rules for the number that is being called. The Translation Rules pane displays.	**translate called** *translation-rule-number*

Option	Description	Cisco IOS CLI Equivalent
Translation Rules pane		**voice translation-rule** *number* Match and Replace Rule: **rule** *precedence /match-pattern/ / replace-pattern/* Reject Rule: **rule** *precedence* **reject** */match-pattern/*

Option	Description	Cisco IOS CLI Equivalent
	1. Click **Add New** to create a translation rule. Alternatively, you can click **Copy From Existing** to copy an existing translation rule to a new translation rule. In the box that appears, change the name if desired, select a called translation rule and a calling translation rule, and click **Copy**. 2. In the Translation Rule Number field, enter a unique number that designates the precedence for this rule. Valid range: integers 1 through 100. 3. (Optional) To copy existing translation rules from a CSV file, click **Import**. Continue to add rules or click **Finish**. For detailed information about this file, see Translation rules CSV file, on page 390. 4. Click **Add Rule**. 5. In the Match field, enter the string that you want the translation rule to affect. Enter the string in regular expression format beginning and ending with a slash (/). For example, /^9/. To include the backslash character (\) in a match string, precede the backslash with a backslash. 6. From the Action drop-down list, select the action that the system performs for calls that match the string in the Match field. The **Reject** option causes the system to reject the call. The **Replace** option causes the system to replace the match number with a value that you specify. 7. If you select the **Replace** action, in the Replace field that displays, enter the string to which to translate the matched string. Enter the number in regular expression format beginning and ending with a slash (/). For example, //, which indicates a replacement of no string.	

Option	Description	Cisco IOS CLI Equivalent
	To include the backslash character (\) in a replace string, precede the backslash with a backslash. As an example, if you specify a match string of /^9/ and a replace string of //, the system removes the leading 9 from calls with a number that begins with 9. In this case, the system translates 914085551212 to 14085551212. **8.** Click **Save**. **9.** Add more translation rules as needed. **10.** (Optional) Click **Export** to save the translation rules that you created in a CSV file. **11.** Click **Finish** at the bottom of the pane.	

Voice policy SIP Dial Peer Media profile options

This reference topic describes the options available for configuring media profiles for SIP dial peers within a voice policy. These settings define the codecs available for SIP trunk communication and DTMF relay options for SIP calls.

Table 117: Voice policy SIP dial peer media profile options

Option	Description	Cisco IOS CLI Equivalent
Add New Media Profile	Click to add a translation profile for the dial peer.	—
Copy from Existing	Click to copy an existing media profile to a new media profile. In the box that appears, enter a media profile number for the profile, and click **Copy**.	—
Media Profile Number	Enter a number for this SIP media profile. Valid range: Integers 1 through 10000.	**voice class codec** *tag-number*
Codec	Move from the Source list to the Target list the codecs that you want to be made available for the SIP trunk to use when communicating with the remote dial peer. Codecs in the target list are in descending order of priority, with the highest priority at the top of the list. Drag and drop items in this list to rearrange them.	**voice class codec** *tag-number* **codec preference** *value codec-type*

Option	Description	Cisco IOS CLI Equivalent
DTMF	Move from the Source list to the Target list the DTMF relay options that you want the system to use for SIP calls. Items in the Target list are in descending order of priority, with the highest priority at the top of the list. Drag and drop items in this list to rearrange them. If you want to include the **Inband** option in the Target list, it can be the only option in that list. If you want to include other options in the Target list, move the Inband option to the Source list before saving the media profile.	**dtmf-relay** {[[**sip-notify**] [**sip-kpml**] [**rtp-nte**]]}
Save	Click to save the configuration settings that you made.	—

Voice policy SIP dial peer modem pass-through options

This reference topic describes the options available for configuring modem pass-through features for SIP dial peers within a voice policy. These settings define the protocol for modem pass-through functionality.

Table 118: Voice policy SIP dial peer modem pass-through options

Option	Description	Cisco IOS CLI Equivalent
Add New Modem Pass-through	Click to add a modem pass-through for this SIP dial peer endpoint.	—
Copy from Existing	Click to copy an existing modem pass-through to a new modem pass-through profile. In the box that appears, select an existing modem pass-through, enter new name if desired, and click **Copy**.	—
Name	Name of the modem pass-through. This name is used when you copy an existing modem pass-through profile to a new one.	—

Option	Description	Cisco IOS CLI Equivalent
Protocol	Select the protocol for the modem pass-through: • **None**—Modem pass-through is disabled on the device • **NSE G.711ulaw**—Uses named signaling events (NSEs) to communicate G.711ulaw codec switchover between gateways • **NSE G.711alaw**—Uses named signaling events (NSEs) to communicate G.711alaw codec switchover between gateways	None: **no modem passthrough** NSE G.711 ulaw: **modem passthrough nse codec g711ulaw** NSE G.711 alaw: **modem passthrough nse codec g711alaw**
Save Modem Pass-Through	Click to save the configuration settings that you made.	—

Voice policy SIP dial peer fax protocol options

This reference topic describes the options available for configuring fax protocol capabilities for SIP dial peers within a voice policy. These settings define the primary and fallback fax protocols, including various T.38 fax relay and pass-through options.

Table 119: Voice policy SIP dial peer fax protocol options

Option	Description	Cisco IOS CLI Equivalent
Add New Fax Protocol	Click to add a fax protocol for the dial peer.	—
Copy from Existing	Click to copy an existing fax protocol to a new fax protocol. In the box that appears, select an existing fax protocol, enter new name if desired, and click **Copy**.	—
Name	Name of the fax protocol. This name is used when you copy an existing fax profile to a new fax profile.	—

Option	Description	Cisco IOS CLI Equivalent
Primary	Select from a set of fax protocol options. Each option is a bundled set of related fax commands. For a detailed description of each bundle, see the “Primary Fax Protocol Command Bundles” table The descriptions of the bundles include the following components: • **nse**—Uses NSEs to switch to T.38 fax relay mode • **force**—Unconditionally uses Cisco Network Services Engines (NSE) to switch to T.38 fax relay • **version**—Specifies a version for configuring fax speed: • **0**—Configures version 0, which uses T.38 version 0 (1998–G3 faxing) • **3**—Configures version 3, which uses T.38 version 3 (2004–V.34 or SG3 faxing) • **none**—No fax pass-through or T.38 fax relay is attempted • **Pass-through**—The fax stream uses one of the following high-bandwidth codecs: • **g711ulaw**—Uses the G.711 ulaw codec • **g711alaw**—Uses the G.711 alaw codec	**fax protocol** { **none** | **pass-through** {**g711ulaw** | **g711alaw**} [**fallback none**]| **t38** [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] [**fallback** {**none** | **pass-through** {**g711ulaw** | **g711alaw**}}]}
Fallback	Available when the primary protocol bundle name that you selected in the Primary field begins with “T.38” or with “Fax Pass-through.” Select the fallback mode for fax transmissions. This fallback mode is used if the primary fax protocol cannot be negotiated between device endpoints. For a detailed description of each option, see the "Fallback Protocol Options” table.	**fax protocol** {none | pass-through {g711ulaw | g711alaw} [**fallback none**] | t38 [nse [force]] [version {0 | 3}] [ls-redundancy value [hs-redundancy value]] [**fallback** {**none** | **pass-through** {**g711ulaw** | **g711alaw**}}]}

Option	Description	Cisco IOS CLI Equivalent
Low Speed	Available when the primary protocol bundle name that you selected in the Primary field begins with "T.38." Specifies the number of redundant T.38 fax packets to be sent for the low-speed V.21-based T.30 fax machine protocol. Range: varies from 0 (no redundancy) to 5. Default: 0.	**ls-redundancy** *value*
High Speed	Available when the primary protocol bundle name that you selected in the Primary field begins with "T.38." Specifies the number of redundant T.38 fax packets to be sent for high-speed V.17, V.27, and V.29 T.4 or T.6 fax machine image data. Range: varies from 0 (no redundancy) to 2. Default: 0	**hs-redundancy** *value*
Save Fax Protocol	Click to save the configuration settings that you made.	—

The following table describes the bundled sets of fax commands that are available for the Primary option when you configure the fax protocol capability for a SIP dial peer endpoint.

For low speed (ls) redundancy, the range varies from 0 (no redundancy) to 5. For high speed (HS redundancy, the range varies from 0 (no redundancy) to 2.

Table 120: Primary fax protocol command bundles

Fax Command Protocol Bundle	Description	Cisco IOS CLI Equivalent
T.38 Fax Relay Version 3	Primary fax protocol is T.38 fax relay version 3. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 3** **ls-redundancy** *value* **hs-redundancy** *value* **no fax-relay sg3-to-g3**
T.38 Fax Relay Version 0	Primary fax protocol is T.38 fax relay version 0. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0** **ls-redundancy** *value* **hs-redundancy** *value*

Fax Command Protocol Bundle	Description	Cisco IOS CLI Equivalent
T.38 Fax Relay Version 3 NSE	Primary fax protocol is NSE based T.38 fax relay version 3. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 3 nse ls-redundancy** *value* **hs-redundancy** *value* **no fax-relay sg3-to-g3**
T.38 Fax Relay Version 3 NSE force	Primary fax protocol is NSE force option of T.38 fax relay version 3. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 3 nse force ls-redundancy** *value* **hs-redundancy** *value* **no fax-relay sg3-to-g3**
T.38 Fax Relay Version 0 NSE	Primary fax protocol is NSE option of T.38 fax relay version 0. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse ls-redundancy** *value* **hs-redundancy** *value*
T.38 Fax Relay Version 0 NSE force	Primary fax protocol is NSE force option of T.38 fax relay version 0. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse force ls-redundancy** *value* **hs-redundancy** *value*
T.38 Fax Relay Version 0 No ECM	Primary fax protocol is T.38 fax relay version 0 with ECM disabled. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable**
T.38 Fax Relay Version 0 NSE No ECM	Primary fax protocol is NSE based T.38 fax relay version 0 with ECM disabled. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable**
T.38 Fax Relay Version 0 NSE force No ECM	Primary fax protocol is NSE force option T.38 fax relay version 0 with ECM disabled. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse force ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable**

Fax Command Protocol Bundle	Description	Cisco IOS CLI Equivalent
T.38 Fax Relay Version 0 Rate 14.4 No ECM	Primary fax protocol is T.38 fax relay version 0 with ECM disabled and fax rate of 14,400 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable** **fax rate 14400**
T.38 Fax Relay Version 0 NSE Rate 14.4 No ECM	Primary fax protocol is NSE based T.38 fax relay version 0 with ECM disabled and fax rate of 14,400 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable** **fax rate 14400**
T.38 Fax Relay Version 0 NSE force Rate 14.4 No ECM	Primary fax protocol is NSE force option T.38 fax relay version 0 with ECM disabled and fax rate of 14,400 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse force ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable** **fax rate 14400**
T.38 Fax Relay Version 0 Rate 9.6 No ECM	Primary fax protocol is T.38 fax relay version 0 with ECM disabled and fax rate of 9,600 bps Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable** **fax rate 9600**
T.38 Fax Relay Version 0 NSE Rate 9.6 No ECM	Primary fax protocol is NSE based T.38 fax relay version 0 with ECM disabled and fax rate of 9,600 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable** **fax rate 9600**
T.38 Fax Relay Version 0 NSE force Rate 9.6 No ECM	Primary fax protocol is NSE force option T.38 fax relay version 0 with ECM disabled and fax rate of 9,600 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse force ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable** **fax rate 9600**

Fax Command Protocol Bundle	Description	Cisco IOS CLI Equivalent
T.38 Fax Relay Version 0 Rate 14.4	Primary fax protocol is T.38 fax relay version 0 with ECM and fax rate of 14,400 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 ls-redundancy** *value* **hs-redundancy** *value* **fax rate 14400**
T.38 Fax Relay Version 0 NSE Rate 14.4	Primary fax protocol is NSE based T.38 fax relay version 0 with ECM and fax rate of 14,400 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse ls-redundancy** *value* **hs-redundancy** *value* **fax rate 14400**
T.38 Fax Relay Version 0 NSE force Rate 14.4	Primary fax protocol is NSE force option T.38 fax relay version 0 with ECM and fax rate of 14,400 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse force ls-redundancy** *value* **hs-redundancy** *value* **fax rate 14400**
T.38 Fax Relay Version 0 Rate 9.6	Primary fax protocol is T.38 fax relay version 0 with ECM and fax rate of 9,600 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 ls-redundancy** *value* **hs-redundancy** *value* **fax rate 9600**
T.38 Fax Relay Version 0 NSE Rate 9.6	Primary fax protocol is NSE based T.38 fax relay version 0 with ECM and fax rate of 9,600 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse ls-redundancy** *value* **hs-redundancy** *value* **fax rate 9600**
T.38 Fax Relay Version 0 NSE force Rate 9.6	Primary fax protocol is NSE force option T.38 fax relay version 0 with ECM and fax rate of 9,600 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse force ls-redundancy** *value* **hs-redundancy** *value* **fax rate 9600**
None	Fax protocol is disabled.	**fax protocol none**
Fax Pass-through G711ulaw	Primary fax protocol is fax pass-through with pass-through codec set to g711ulaw.	**fax protocol pass-through g711ulaw**

Fax Command Protocol Bundle	Description	Cisco IOS CLI Equivalent
Fax Pass-through G711ulaw No ECM	Primary fax protocol is fax pass-through with pass-through codec set to g711ulaw and ECM disabled.	**fax protocol pass-through g711ulaw** **fax-relay ecm disable**
Fax Pass-through G711alaw	Primary fax protocol is fax pass-through with pass-through codec set to g711alaw.	**fax protocol pass-through g711alaw**
Fax Pass-through G711alaw No ECM	Primary fax protocol is fax pass-through with pass-through codec set to g711alaw and ECM disabled.	**fax protocol pass-through g711alaw** **fax-relay ecm disable**

The following table describes the selections that are available for the Fallback option when you configure the fax protocol capability for a SIP dial peer endpoint.

Table 121: Fallback protocol options

Fallback Fax Protocol Options	Description	Cisco IOS CLI Equivalent
None	Fallback Fax Protocol is None. All special fax handling is disabled.	**fax protocol t38** [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] **fallback none** **fax protocol pass-through** {**g711ulaw** | **g711alaw** } **fallback none**
Fax Pass-through G711ulaw	Fallback Fax Protocol is Fax Pass-through with pass-through codec set to g711ulaw.	**fax protocol t38** [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] **fallback pass-through g711ulaw**
Fax Pass-through G711alaw	Fallback Fax Protocol is Fax Pass-through with pass-through codec set to g711alaw.	**fax protocol t38** [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] **fallback pass-through g711alaw**

Configure SRST phones for a voice policy

This task defines how the system augments and manipulates calls for the Cisco Unified SRST phone endpoint type within a voice policy. It allows you to configure media profile options for phones operating in SRST mode.

When configuring SRST phones for a voice policy, you define the codecs and DTMF relay options that will be available for phones registered to the local gateway when in Cisco Unified SRST mode. These settings ensure proper call functionality during WAN outages or degradation.

Before you begin

You must be in the process of adding a new voice policy or editing an existing one within Cisco SD-WAN Manager

Follow these steps to configure SRST phones for a voice policy:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Unified Communications**

Step 2 Click **Add Voice Policy**, and choose **SRST Phone**.

Step 3 From the **Add SRST Phone Policy Profile** drop-down list, select **Create New**.

Alternatively, you can select **Copy from Existing** to reuse settings from an existing policy profile.

Step 4 Configure the Media Profile:

a) Click **Media Profile**, and click **Next**.

b) Click **Add New Media Profile**.

c) In the page that displays, configure options as described in the Voice policy SRST phones configuration options, on page 384 topic.

Define the codecs and DTMF relay options for SRST phones.

Step 5 Click **Next**.

Step 6 In **Policy Profile Name**, enter a name for this child policy.

Step 7 In **Policy Profile Description**, enter a description for this child policy.

Step 8 Click **Save**.

The SRST phones for the voice policy are successfully configured.

What to do next

You have now configured all subpolicies for the Add a Voice Policy supertask. Proceed to provision a device template for Unified Communications to apply this voice policy to your devices.

Voice policy SRST phones configuration options

This reference topic describes the options available for configuring SRST (Survivable Remote Site Telephony) phones within a voice policy. These settings define the media profile, including codecs and DTMF relay options, for phones operating in Cisco Unified SRST mode.

Table 122: Voice policy SRST phones configuration options

Option	Description	Cisco IOS CLI Equivalent
Medial Profile Number	Enter a number for this Cisco Unified SRST media profile. Valid range: Integers 1 through 10000.	**voice class codec** *tag-number*

Option	Description	Cisco IOS CLI Equivalent
Codec	Move from the Source list to the Target list the codecs that you want to be available for phones when they are in Cisco Unified SRST mode and communicating with other phones that are in the same site and registered to the same gateway. Codecs in the target list are in descending order of priority, with the highest priority at the top of the list. Drag and drop items in this list to rearrange them.	**voice class codec** *tag-number* **codec preference** *value codec-type*
DTMF field	Move from the source list to the target list the DTMF relay options that you want the system to use when in Cisco Unified SRST mode. Items in the target list are in descending order of priority, with the highest priority at the top of the list. Drag and drop items in this list to rearrange them. If you want to include the **Inband** option in the Target list, it can be the only option in that list. If you want to include other options in the Target list, move the Inband option to the Source list before saving the media profile.	**dtmf-relay** {[[**sip-notify**] [**sip-kpml**] [**rtp-nte**]]}
Save	Click to save the configuration settings that you made.	—

Provision a device template for unified communications

This task allows you to select UC-specific feature templates and set up the voice policy to include with a device template. This process applies the configured Unified Communications settings to your devices.

A device template bundles various feature templates and policies, enabling consistent and scalable deployment of configurations across multiple devices. This task is the final step in preparing your UC voice services for deployment.

Before you begin

Ensure that all necessary UC-specific feature templates (Voice Card, Call Routing, SRST, DSPFarm) and voice policies have been previously created and configured.

Follow these steps to provision a device template for Unified Communications:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Device Templates**, and click **Create Template**.

Note
In Cisco vManage Release 20.7.1 and earlier releases, **Device Templates** is called **Device**.

Step 3 From the **Create Template** drop-down list, select **From Feature Template**.

Step 4 From the **Device Model** drop-down list, select the type of supported device to which you want to attach the UC-specific feature templates and map the voice policy.

Step 5 Click **Unified Communications**.

Step 6 To select UC-specific feature templates to include with the device template, perform these actions:

a) From the **Voice Card** drop-down list, select the voice card feature template.
b) From the Call Routing drop-down list, select the call routing feature template.
c) From the SRST drop-down list, select the SRST feature template.
d) From the DSPFarm drop-down list, select the DSPFarm template.

Step 7 To set up the voice policy to include with the device template, perform these actions:

a) From the **Voice Policy** drop-down list, select the voice policy.
b) Click **Mapping**.
c) From the list of endpoint types in the left pane of the screen that displays, select the type of endpoint that contains the subpolicies that you want to map to specific endpoints.
d) From the list of subpolicies that displays, click **…**, and select **Mapping** for the subpolicy that you want to map to specific endpoints.
e) In the list of endpoints that displays, select each endpoint to which you want to map the subpolicy
f) Click **Map**.
g) Click **Save**.

When you map subpolicies to endpoints, the system generates the CLI commands. See Generated CLI commands for subpolicies to endpoints mapping, on page 387.

Step 8 To create the device template, click **Create**.

A device template for Unified Communications is successfully provisioned, including the selected UC-specific feature templates and voice policy mappings.

What to do next

The device template is now ready to be attached to devices to deploy the Unified Communications configurations.

Generated CLI commands for subpolicies to endpoints mapping

This reference topic describes the CLI commands that are automatically generated when subpolicies are mapped to specific endpoints within a device template. This table provides insight into the underlying configuration applied by the Cisco SD-WAN Manager.

Table 123: Generated CLI commands for subpolicies to endpoints mapping

Endpoint	Subpolicy	Cisco IOS CLI Application Mapping	Remarks
Voice Port FXO Voice Port FXS Voice Port FXS DID Voice Port PRI ISDN POTS Dial Peer SIP Dial Peer	Translation profile	**translation-profile incoming** *profile-name* **translation-profile outgoing** *profile-name*	A translation profile policy is applied to a dial peer or a voice profile.
SRST Phone SIP Dial Peer	Media profile	voice register pool *number* **voice-class codec** *number* **dtmf-relay** {[[**sip-notify**] [**sip-kpml**] [**rtp-nte**]]}	A media profile policy includes voice class codec and DTMF relay configurations. This policy is applied to an incoming SIP dial peer, an outgoing SIP dial peer, or an SRST phone profile.
Voice Port FXO	Supervisory disconnect	voice port *number* **supervisory custom-cptone** *cptone-name* **supervisory dualtone-detect=params** *tag*	A supervisory disconnect policiy such as custom-cptone or dualtone-detect-params is applied to FXO voice interfaces.

Endpoint	Subpolicy	Cisco IOS CLI Application Mapping	Remarks
Voice Port FXO Voice Port FXS Voice Port FXS DID Voice Port PRI ISDN POTS Dial Peer	Trunk group	**trunk-group name** [*preference-num*] **voice-port** *number* *trunk-group name* [*preference-num*] **interface serial** *slot*/*sub-slot*/**port:** {**15** | **23**} **dial-peer voice** *tag* **pots** **trunkgroup name** *preference-num*	If more than one interface is assigned to the same trunk group, the *preference-num* value determines the order in which the trunk group uses the interfaces. A preference-num value of 1 is the highest preference, so an interface with that value is used first. A value of 64 is the lowest preference so an interface with that value is used last.
SIP Dial Peer	Modem pass-through	None: **no modem passthrough** G.711 ulaw: **modem passthrough nse codec g711ulaw** G.711 alaw: **modem passthrough nse codec g711alaw**	—
SIP Dial Peer	Fax protocol	**fax protocol** {**none** | **pass-through** {**g711ulaw** | **g711alaw**} [**fallback none**] | **t38** [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] [**fallback** {**none** | **pass-through** {**g711ulaw** | **g711alaw**}}]}	—

Dial peer CSV file

This reference topic describes the structure and content requirements for a Dial Peer CSV (Comma Separated Values) file. This file includes information for one or more incoming and outgoing SIP and POTS dial peers, allowing for bulk configuration or import into Cisco SD-WAN Manager.

The file must be comma delimited, and each record in the file must include each field that the following table describes, in the order shown.

Table 124: Dial peer CSV file

Field	Description
Dial Peer Tag	Number that is used to reference the dial peer.
Dial Peer Type	Type of dial peer that you are creating (**pots** or **voip**).
Direction	Direction of traffic on the dial peer (**Incoming** or **Outgoing**).
Description	Description of the dial peer.
Forward Digits	How the dial peer transmits digits in outgoing numbers: • **All**—The dial peer transmits all digits in the number. • **None**—The dial peer does not transmit digits in the number that do not match the destination pattern. • *n*—The dial peer transmits the number of right-most digits in the number that the integer *n* represents. For example, if *n* is 7 and the outgoing number is 1112223333, the dial peer transmits 2223333.
Preference	For POTS dial peers, a unique numeric value for the dial peer. If dial peers have the same match criteria, the system uses the one with the highest preference value.
Prefix	Digits to be prepended to outgoing POTS dial peer calls.
Numbering Pattern	String that the router uses to match incoming calls to the dial peer.
Dest. Address	Network address of the remote voice gateway to which calls are sent after a local outgoing SIP dial peer is matched.
Voice Port	Voice port that the router uses to match calls to the dial peer. For an outgoing dial peer, the router sends the calls that match the dial peer to this port. For an incoming dial peer, this port serves as an additional match criterion. The dial peer is matched only if a call comes in on this port.

Field	Description
Transport Protocol	For SIP dial peers, transport protocol (**TCP** or **UDP**) for SIP control signaling.

Example dial peer CSV file

```
Tag,type,Direction,Description,Forward Digits,Preference,Prefix,Pattern,Dest. Address,Voice
 Port,Transport
6545,voip,Outgoing,description To Voice Gateway,,1,,23456,ipv4:166.2.121.17,,udp
6756,voip,Outgoing,description ***Fax Number 6362-6362***,,0,,34567,ipv4:166.2.121.16,,tcp
768,voip,Outgoing, description Fire Alarm Dialer,,8,,5678,ipv4:166.2.121.19,,udp
10,pots,Incoming,,,5,,0115T,,1/0/1,
54,pots,Outgoing,,,6,,.T,,1/0/3,
23,pots,Incoming,,all,0,,76..,,1/0/4,
26,pots,Incoming,,5,1,55,9800.......,,1/0/5,
27,pots,Incoming,,5,1,55,9800.......,,0/1/5:15,
```

Translation rules CSV file

This reference topic describes the structure and content requirements for a Translation Rules CSV (Comma Separated Values) file. This file can be used to import existing translation rule information when configuring translation profiles for voice policies.

The file must be comma delimited, and each record in the file must include each field that the following table describes, in the order shown.

Table 125: Translation rules CSV file

Field	Description
Match	String that you want the translation rule to affect. The string must be in regular expression format beginning and ending with a slash (/). For example, /^9/.
Action	Action that the system performs for calls that match the string in the Match field. Valid values are: • **reject**—Causes the system to reject the call • **replace**—Causes the system to replace the match string with the value in the Replace field
Replace	If the Action field contains **replace**, this field contains the string to which to translate the matched string. Enter the number in regular expression format beginning and ending with a slash (/). For example, //, which indicates a replacement of no string. As an example, if you specify a match string of /^9/ and a replace string of //, the system removes the leading 9 from calls with a number that begins with 9. In this case, the system translates 914085551212 to 14085551212.

Example translation rules CSV file

This section provides an example of a Translation Rules CSV file, illustrating the format and content described above.

```
Match,Action,Replace
/34/,replace,/34/
/23/,reject,
/56/,replace,/100/
/16083652563/,replace,/6083652563/
```

Monitor UC operations

This task allows you to monitor the real-time statuses of lines, calls, interfaces, and related items that a device processes after enabling UC voice services for supported routers.

Monitoring UC operations provides crucial insights into the performance and status of your Unified Communications deployment, helping you verify functionality and troubleshoot issues.

Before you begin

UC voice services must be enabled for the supported routers you wish to monitor.

Follow these steps to monitor UC operations:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

Note
Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

Step 2 In the table of devices, select the device for which you want to monitor UC operations.

Step 3 From **Security Monitoring**, click **Real Time**.

Step 4 In **Device Options**, select one of these options:

a) **Voice Calls**: Displays information for active voice calls. See Voice calls monitoring information, on page 392 table.

b) **Voice VOIP Calls**: Displays information for active VOIP calls. See Voice VoIP calls monitoring information, on page 392 table.

c) **Voice Phone Info**: Displays information about Cisco Unified SRST registrations. See Voice phone info monitoring information, on page 393 table.

d) **Voice Controller T1 E1 Current 15 mins Stats**: Displays configuration and status information for the T1/E1 voice module that is installed in the device, compiled over the past 15 minutes. See Voice controller T1 E1 current 15 Mins stats monitoring information, on page 394 table.

e) **Voice Controller T1 E1 Total Stats**: Displays configuration and status information for the T1/E1 voice module that is installed in the device, compiled since the module last started. See Voice controller T1 E1 total stats monitoring information, on page 395 table.

f) **Voice ISDN Status**: Displays information about Layer 1 and Layer 2 status for the ISDN controller, and information about active calls. See Voice ISDN status information, on page 396 table.

g) **Voice DSPFarm SCCP CUCM Groups**: Displays detailed information about Cisco Unified Communications Manager groups that are configured for DSP farm services on a device. See Voice DSPFarm SCCP CUCM groups monitoring information, on page 396 table.

h) **Voice DSPFarm Profile**: Displays detailed information about DSP farm service profiles and media resources that are configured on the device. See Voice DSPFarm profile monitoring information, on page 397 table.
i) **Voice DSP Farm SCCP Connections**: Displays detailed information about SCCP connections between the device and Cisco Unified Communications Manager. See Voice DSPFarm SCCP connections monitoring information, on page 398 table.
j) **Voice DSPFarm Active**: Displays operational and status information about DSP farm resources that are active on the device. See Voice DSPFarm active monitoring information, on page 398 table.
k) **Interface Detail**: Displays status and statistical information for interfaces that are configured for the router.
l) **Interface Statistics**: Displays statistical information for interfaces that are configured for the router
m) **Interface T1/E1**: Displays information for the T1/E1 voice module that is installed in the device

Real-time operational data for the selected UC services is displayed, providing insight into their status and performance.

Voice calls monitoring information

This reference topic describes the information displayed when monitoring active voice calls on a device. It provides details such as call ID, voice port, codec used, and packet statistics.

Table 126: Voice calls monitoring information

Field	Description
Call ID	System assigned identifier of a telephony call leg
Voice Port	Voice port used for the call
Codec	Negotiated codec used for the call
VAD	Indicates whether VAD is enabled or disabled for the call
DSP Cannel	DSP channel used for the call
DSP Type	Type of DSP used for the call
Aborted Packets	Number of packets aborted during the call
TX Packets	Number of packets transmitted during the call
RX Packets	Number of packets received during the call
Last Updated	Date and time when the information on this page was last updated

Voice VoIP calls monitoring information

This reference topic describes the information displayed when monitoring active VoIP calls on a device. It provides details such as call ID, codec, destination address, and packet statistics for RTP connections.

Table 127: Voice VoIP calls monitoring information

Field	Description
Call ID	System assigned identifier of an RTP connection for a call leg
Codec	Negotiated codec used for the call
Destination Address	IP address of the destination of the call
Destination Port	RTP port of the destination of the call
TX Packets	Number of packets transmitted during the call
RX Packets	Number of packets received during the call
Duration (ms)	Duration of the call, in milliseconds
Last Updated	Date and time when the information on this page was last updated

Voice phone info monitoring information

This reference topic describes the information displayed when monitoring voice phone information, specifically related to Cisco Unified SRST registrations on a device. It includes details about phone pools, network identifiers, and registration states.

Table 128: Voice phone info monitoring information

Field	Description
Pool Tag	Tag number that is assigned to the Cisco Unified SRST phone pool on the device
ID Network	Identifier of the network subnet that the device uses to register phones that fallback from Cisco Unified Communications Manager to this device
Registration State	Indicates whether phones that are in Cisco Unified SRST mode are registered to this device
Dialpeer Tag	System assigned tag used by the dial peer that is assigned to the directory number of phones that are in Cisco Unified SRST mode and are registered to this device
Address	IP address of the device interface that is used for SIP SRST call control when phones fail over
Directory Number	Directory number of each phone that is in Cisco Unified SRST mode
Last Updated	Date and time when the information on this page was last updated

Voice controller T1 E1 current 15 Mins stats monitoring information

This reference topic describes the configuration and status information displayed for a T1/E1 voice module, compiled over the past 15 minutes. It includes details such as interface status, clock source, and various error statistics.

Table 129: Voice controller T1 E1 current 15 Mins stats monitoring information

Field	Description
Interface-slot-num	Slot number of the controller.
Insterface-subslot-num	Subslot number of the controller.
Interface-port-num	Port number of the controller.
Status	Status of the controller.
Type	Type of the controller.
Clock Source	Clock source used for the controller.
Line Code Violations	Number line code violations that have occurred.
Path Code Violations	Number path code violations that have occurred.
Slip Seconds	Number of slip seconds that have occurred. A slip can occur when there is a difference between the timing of a synchronous receiving terminal and the received signal.
Frame Loss Seconds	Number of seconds in which out of frame (OOF) errors have occurred.
Line Err. seconds	Number of seconds in which Line Errored Seconds (LES) have occurred. A LES is a second in which one or more Line Code Violation errors are detected.
Degraded Minutes	Number of Degraded Minutes that have occurred. A Degraded Minute is one in which the estimated error rate exceeds 1E-6 but does not exceed 1E-3.
Errored Seconds	Number of Errored Seconds that have occurred.
Bursty Errored Seconds	Number of Bursty Error Seconds that have occurred. A Bursty Error Second is a second with less than 320 and more than 1 path coding violation errors, no severely errored frame defects, and no detected incoming AIS defects.
Severely Errored Seconds	Number of Severely Errored Seconds that have occurred.
Unavailable Seconds	Number of Unavailable Seconds that have occurred. This value is calculated by counting the number of seconds that the interface is unavailable.
Last Updated	Date and time when the information on this page was last updated.

Voice controller T1 E1 total stats monitoring information

This reference topic describes the configuration and status information displayed for a T1/E1 voice module, compiled since the device last started. It includes cumulative details such as interface status, clock source, and various error statistics.

Table 130: Voice controller T1 E1 total stats monitoring information

Field	Description
Interface-slot-num	Slot number of the controller.
Insterface-subslot-num	Subslot number of the controller.
Interface-port-num	Port number of the controller.
Status	Status of the controller.
Type	Type of the controller.
Clock Source	Clock source used for the controller.
Line Code Violations	Number line code violations that have occurred.
Path Code Violations	Number path code violations that have occurred.
Slip Seconds	Number of slip seconds that have occurred. A slip can occur when there is a difference between the timing of a synchronous receiving terminal and the received signal.
Frame Loss Seconds	Number of seconds in which out of frame (OOF) errors have occurred
Line Err. seconds	Number of seconds in which Line Errored Seconds (LES) have occurred. A LES is a second in which one or more Line Code Violation errors are detected.
Degraded Minutes	Number of Degraded Minutes that have occurred. A Degraded Minute is one in which the estimated error rate exceeds 1E-6 but does not exceed 1E-3.
Errored Seconds	Number of Errored Seconds that have occurred.
Bursty Errored Seconds	Number of Bursty Error Seconds that have occurred. A Bursty Error Second is a second with less than 320 and more than 1 path coding violation errors, no severely errored frame defects, and no detected incoming AIS defects.
Severely Errored Seconds	Number of Severely Errored Seconds that have occurred.
Unavailable Seconds	Number of Unavailable Seconds that have occurred. This value is calculated by counting the number of seconds that the interface is unavailable.
Last Updated	Date and time when the information on this page was last updated.

Voice ISDN status information

This reference topic describes the information displayed when monitoring voice ISDN status on a device. It provides details about Layer 1 and Layer 2 status for the ISDN controller and information about active calls.

Table 131: Voice ISDN status information

Field	Description
Key ID	Identifier of the table row
Interface	Name of the PRI ISDN digital interface
Switch Type	Switch type used for the PRI ISDN digital interface
Layer 1 Status	Layer 1 status of the PRI ISDN digital interface
Layer 2 Status	Layer 2 status of the PRI ISDN digital interface
Active Calls	Number of active calls on the PRI ISDN digital interface
Last Updated	Date and time when the information on this page was last updated

Voice DSPFarm SCCP CUCM groups monitoring information

This reference topic describes the detailed information displayed when monitoring Cisco Unified Communications Manager groups configured for DSP farm services on a device. It includes group IDs, switchover/switchback methods, and associated profiles.

Table 132: Voice DSPFarm SCCP CUCM groups monitoring information

Field	Description
CUCM Group ID	Identifier of the Cisco Unified Communications Manager group
Description	Description of the Cisco Unified Communications Manager group
Switchover Method	Method that the primary Cisco Unified Communications Manager server in this Cisco Unified Communications Manager group uses for failover
Switchback Method	Method that the secondary Cisco Unified Communications Manager server in this Cisco Unified Communications Manager group uses to switch back after a failover
CUCM ID	Identifier of each Cisco Unified Communications Manager server in the Cisco Unified Communications Manager group
CUCM Priority	Priority in which the Cisco Unified Communications Manager servers in this Cisco Unified Communications Manager group are used

Field	Description
Profile ID	Identifier of the DSP farm profile that is registered to each Cisco Unified Communications Manager server in the Cisco Unified Communications Manager group
Reg. Name	Name of the DSP farm profile that is registered to each Cisco Unified Communications Manager server in the Cisco Unified Communications Manager group
Last Updated	Date and time when the information on this page was last updated

Voice DSPFarm profile monitoring information

This reference topic describes the detailed information displayed when monitoring DSP farm service profiles and media resources configured on a device. It includes profile IDs, service types, operational status, and resource information.

Table 133: Voice DSPFarm profile monitoring information

Field	Description
Profile ID	Identifier of the DSP farm profile.
Service ID	Type of DSP farm service that is configured for this DSP farm profile.
Service Mode	Service mode for this DSP farm profile.
Resource ID	Resource identifier for the DSP resource group in this DSP farm profile.
Admin	Status of this DSP farm profile. If this field displays DOWN, ensure that the Shutdown option is not enabled in the Profile tab of the DSPFarm feature template that defines this DSP farm.
Operation	Status of the registration of the profile with Cisco Unified Communications Manager: • ACTIVE IN PROGRESS—Profile is in the process of registering with Cisco Unified Communications Manager • DOWN—Profile is unable to register with Cisco Unified Communications Manager • ACTIVE— Profile is registered with Cisco Unified Communications Manager
App. Type	Type of application with which the DSP farm services that are provisioned on the device are associated.

Field	Description
App. Status	Status of the association of this profile with Cisco Unified Communications Manager: • app-assoc-done—Profile is associated with Cisco Unified Communications Manager • app-assoc-not-done—Profile is not associated with Cisco Unified Communications Manager
Resource Provider	Information about the mediaresource family that relates to the profile.
Provider Status	Status of the media resources that relate to the profile.
Last Updated	Date and time when the information on this page was last updated.

Voice DSPFarm SCCP connections monitoring information

This reference topic describes the detailed information displayed when monitoring SCCP connections between a device and Cisco Unified Communications Manager. It includes connection IDs, session types, codecs, and remote/local endpoint details.

Table 134: Voice DSPFarm SCCP connections monitoring information

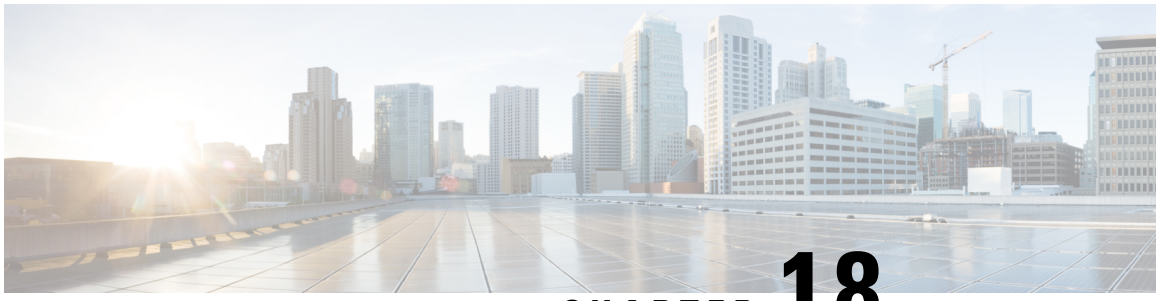
Field	Description
Connection ID	Identifier of an SCCP connection for an active call that uses this DSP farm service
Session ID	Identifier of an SCCP session for an active call that uses this DSP farm service
Session Type	Type of DSP farm service for this SCCP connection
Mode	Mode for direction of traffic for this SCCP connection
Codec	Codec provisioned for this SCCP connection
Remote IP	IP address of the remote endpoint for this SCCP connection
Remote Port	Port number of the remote endpoint for this SCCP connection
Source Port	Port number of the local endpoint for this SCCP connection
Last Updated	Date and time when the information on this page was last updated

Voice DSPFarm active monitoring information

This reference topic describes the operational and status information displayed for active DSP farm resources on a device. It includes details about DSP identifiers, status, and packet counts for active connections.

Table 135: Voice DSPFarm active monitoring information

Field	Description
DSP	Identifier of the DSP for an active call that uses this DSP farm service
Status	Status of the DSP for an active call that uses this DSP farm service
Resource ID	Resource Identifier that is associated with the DSP that this connection uses
Bridge ID	Bridge Identifier that is associated with the DSP that this connection uses
Transmit Packets	Number of packets that this connection has transmitted
Received Packets	Number of packets that this connection has received
Last Updated	Date and time when the information on this page was last updated



CHAPTER 18

Cisco Unified Border Element

- Feature history for Cisco Unified Border Element, on page 401
- Cisco unified border elements (CUBE), on page 403
- Supported devices for CUBE configuration, on page 403
- Restrictions for CUBE configuration, on page 404
- Use cases for CUBE, on page 404
- Configure CUBE, on page 404
- CUBE commands, on page 405
- SRST commands, on page 414

Feature history for Cisco Unified Border Element

Table 136: Feature history

Feature Name	Release Information	Description
Cisco Unified Border Element (CUBE)	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	You can configure CUBE functionality by using Cisco IOS XE Catalyst SD-WAN devices CLI templates or CLI add-on feature templates.

Feature Name	Release Information	Description
Secure SRST Support on Cisco Catalyst SD-WAN	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco vManage Release 20.10.1	Secure SRST Support on Cisco Catalyst SD-WAN allows you to configure Cisco Survivable Remote Site Telephony (SRST) commands and additional Cisco Unified Border Element (CUBE) commands. Using these commands within Cisco IOS XE Catalyst SD-WAN devices, you can: • Maintain voice services at remote sites during network outages. • Extend advanced voice and video connectivity within Cisco Catalyst SD-WAN You can configure these commands onCisco IOS XE Catalyst SD-WAN devices using Cisco SD-WAN Manager device CLI templates or CLI add-on feature templates.
Supported Voice and SIP-UA Commands	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	This feature provides support for specific commands that enhance voice and SIP-UA functionalities on Cisco IOS XE Catalyst SD-WAN devices. These commands include: • **cipher (voice class)** • **nat media-keepalive** • **secure-ciphersuite** • **transport tcp tls (sip-ua)** • **voice-class sip nat media-keepalive**
Survivable Remote Site Telephony (SRST) commands	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	This feature provides support for specific commands related to secure HTTP client communication and `call-manager-fallback` transport. These commands include: • **http client secure-ciphersuite** • **transport-tcp-tls (call-manager-fallback)**

Cisco unified border elements (CUBE)

A Cisco Unified Border Element (CUBE) is a network device or software that facilitates voice and video connectivity between different Voice over IP (VoIP) networks. It primarily functions as a Session Border Controller (SBC), enabling communication between enterprise networks and Internet telephony service providers (ITSPs).

Unlike traditional voice gateways that use circuit-switched connections, such as PRI, to connect to telephone companies, CUBE replaces physical voice trunks with IP-based voice trunks. This allows it to connect directly to other VoIP networks and ITSPs.

CUBE provides conventional SBC functions. It also offers a wide variety of advanced features to manage and secure VoIP sessions.

Configuration

You can configure CUBE functionality on Cisco IOS XE Catalyst SD-WAN device using device CLI templates or CLI add-on feature templates.

For more information about CUBE setup, functionality, usage, configuration, and related topics, see the Cisco Unified Border Element Configuration Guide.

Supported devices for CUBE configuration

The following devices support CUBE configuration:

- Cisco 1000 Series Integrated Services Routers
- Cisco 4000 Series Integrated Services Routers
- Cisco Catalyst 8200 Series Edge Platforms
- Cisco Catalyst 8300 Series Edge Platforms
- Cisco Catalyst 8000v Software Router
- Cisco ASR 1001-X Router
- Cisco ASR 1002-X Router
- Cisco ASR 1006-X Router with the Cisco ASR1000-RP3 Module, and the Cisco ASR1000-ESP100 or ASR1000-ESP100-X Embedded Services Processor
- Cisco ASR 1004 Router with the RP2 Route Processor and the Cisco ASR 1000-ESP40 Embedded Services Processor
- Cisco ASR 1006 Router with the RP2 Route Processor and the Cisco ASR 1000-ESP40 Embedded Services Processor
- Cisco ASR 1006-X Router with the RP2 Route Processor and the Cisco ASR 1000-ESP40 Embedded Services Processor

Restrictions for CUBE configuration

High-availability configuration is not supported for CUBE.

Use cases for CUBE

CUBE can configure SBC elements for various applications, such as:

- Enterprise Premises-Based Collaboration: using Cisco Unified Communications Manager (or another call control application) with centralized or local PSTN breakouts.
- Local Breakout Gateway for Cisco Unified Communications Manager Cloud: a Cisco-hosted cloud service for large enterprises.
- Local Gateway to Enable the Bring Your Own PSTN (BYoPSTN) Option for Cisco Webex Calling: to enable the Bring Your Own PSTN (BYoPSTN) option.
- Edge Audio for Cisco Webex Meetings: with a direct VoIP route to the Cisco Webex cloud or through existing PSTN services.

Configure CUBE

This task guides you on how to configure CUBE functionality on a device.

Complete these steps to configure CUBE:

Before you begin

Create a Cisco IOS XE Catalyst SD-WAN device CLI template or a CLI add-on feature template for the device to use the CUBE functionality

Procedure

Create a Cisco IOS XE Catalyst SD-WAN device CLI template or a CLI add-on feature template for the device to use the CUBE functionality

Example:

The following example shows a basic CUBE configuration using a CLI add-on template:

```
voice service voip
 ip address trusted list
  ipv4 10.0.0.0.255.0.0.0
  ipv6 2001:DB8:0:ABCD::1/48
  !
 allow-connections sip to sip
 sip
  no call service stop
  !
dial-peer voice 100 voip
  description Inbound LAN side dial-peer
```

```
 session protocol sipv2
 incoming called number .T
 voice-class codec 1
 dtmf-relay rtp-nte
 !
dial-peer voice 101 voip
 description Outbound LAN side dial-peer
 destination pattern [2-9].........
 session protocol sipv2
 session target ipv4:10.10.10.1
 voice-class codec 1
 dtmf-relay rtp-nte
 !
dial-peer voice 200 voip
 description Inbound WAN side dial-peer
 session protocol sipv2
 incoming called-number .T
 voice-class codec 1
 dtmf-relay rtp-nte
 !
dial-peer voice 201 voip
 description Outbound WAN side dial-peer
 destination pattern [2-9].........
 session protocol sipv2
 session target ipv4:20.20.20.1
 voice-class codec 1
 dtmf-relay rtp-nte
```

For information about device CLI templates and CLI add-on templates, refer to the *Cisco Catalyst SD-WAN Control Components and Device Management Guide*.

For information about CUBE configuration and usage, refer to the Cisco Unified Border Element Configuration Guide.

For information about the CUBE commands that Cisco Catalyst SD-WAN supports for use in a CLI template, refer to CUBE commands, on page 405 .

After successfully applying the configuration, the device is enabled to function as a Cisco Unified Border Element, processing voice and video traffic according to the defined dial-peers and voice service settings.

What to do next

After configuring CUBE, you should verify the voice service and dial-peer configurations to ensure proper call routing and media handling. You can also integrate the CUBE-enabled device with your Cisco Unified Communications Manager or other call control applications. For more information, refer to Verify CUBE on the Device.

CUBE commands

The following table lists the commands that are supported by Cisco Catalyst SD-WAN CLI templates for CUBE configuration. Click a command name in the Command column to view information about the command, its syntax, and its use.

Note Some configurations and protocols are identified as insecure and is a security risk for Cisco devices. Existing deployments continue to function, but new installations require intentional enablement. For more information on remediation, refer to Resilient Infrastructure: Cisco Catalyst SD-WAN and Routing

Table 137: Cisco Catalyst SD-WAN CLI template commands for CUBE configuration

Command	Description
address-hiding	Hides signaling and media peer addresses from endpoints other than the gateway.
anat	Enables Alternative Network Address Types (ANAT) on a SIP trunk.
answer-address	Specifies the full E.164 telephone number to be used to identify the dial peer of an incoming call.
application (global)	Enters application configuration mode to configure applications.
asserted-id	Enables support for the asserted ID header in incoming SIP requests or response messages, and to send the asserted ID privacy information in outgoing SIP requests or response messages.
asymmetric payload	Configures SIP asymmetric payload support.
audio forced	Allows only audio and image (for T.38 Fax) media types, and drops all other media types).
authentication	Enables SIP digest authentication.
bind	Binds the source address for signaling and media packets to the IPv4 or IPv6 address of a specific interface.
block	Configures global settings to drop (not pass) specific incoming SIP provisional response messages on a CUBE.
call spike	Configures the limit on the number of incoming calls received in a short period (a call spike).
call threshold global	Enables the global resources of a gateway.
call treatment action	Configures the action that the router takes when local resources are unavailable.
call treatment cause-code	Specifies the reason for the disconnection to the caller when local resources are unavailable.
call treatment isdn-reject	Specifies the rejection cause code for ISDN calls when all ISDN trunks are busied out, but the switch ignores the busyout trunks and still sends ISDN calls into the gateway.

Command	Description
call treatment on	Enables call treatment to process calls when local resources are unavailable.
callmonitor	Enables the call monitoring messaging functionality on a SIP endpoint in a VoIP network.
call-route	Enables header-based routing at the global configuration level.
cipher (voice class)	Configures the cipher setting, and associates it to a TLS profile.
clid	Passes the network-provided ISDN numbers in an ISDN calling party information element screening indicator field, and removes the calling party name and number from the calling-line identifier in voice service voip configuration mode. Alternatively, allows the presentation of the calling number by substituting for the missing **Display Name** field in the Remote-Party-ID and From headers.
codec preference	Specifies a list of preferred codecs to use on a dial peer.
codec profile	Defines audio and video capabilities that are needed for video endpoints.
codec transparent	Enables codec capabilities to be passed transparently between endpoints in a CUBE.
conn-reuse	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Reuses the TCP connection of a SIP registration for an endpoint behind a firewall.
connection-reuse	Uses global listener port for sending requests over UDP.
contact-passing	Configures pass-through of the contact header from one leg to the other leg for 302 pass-through.
cpa	Enables the call progress analysis (CPA) algorithm for outbound VoIP calls and to set CPA parameters.
credentials	Configures a SIP TDM gateway or CUBE to send a SIP registration message when in the UP state.
crypto signaling	Identifies the **trustpoint** *trustpoint-name* keyword and argument that is used during the Transport Layer Security (TLS) handshake that corresponds to the remote device address.
dial-peer cor custom	Specifies that named class of restrictions (COR) apply to dial peers.
dial-peer cor list	Defines a class of restrictions (COR) list name.

Command	Description
disable-early-media 180	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Specifies which call treatment, early media or local ringback, is provided for 180 responses with 180 responses with Session Description Protocol (SDP).
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
dtmf-interworking	Enables a delay between the dtmf-digit begin and dtmf-digit end events in the RFC 2833 packets sent from CUBE, and generates RFC 4733 compliance RTP Named Telephony Event (NTE) packets from CUBE.
early-media update block	Blocks the UPDATE requests with the Session Description Protocol (SDP) in an early dialog.
early-offer	Forces CUBE to send a SIP invite with Early Offer on the Out Leg.
emergency	Configures a list of emergency numbers.
error-code-override	Configures the SIP error code to be used at the dial peer.
error-passthru	Enables the passage of error messages from the incoming SIP leg to the outgoing SIP leg.
g729-annexb override	Configures the settings for G.729 codec interoperability and overrides the default value if the annexb attribute is not present.
gcid	Enables Global Call ID (GCID) for every call on an outbound leg of a VoIP dial peer for a SIP endpoint.
gw-accounting	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Enables an accounting method for collecting call detail records (CDRs).
handle-replaces	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Configures a Cisco IOS device to handle SIP INVITE with Replaces header messages at the SIP protocol level.
header-passing	Enables the passing of headers to and from SIP INVITE, SUBSCRIBE, and NOTIFY messages.
host-registrar	Populates the sip-ua registrar domain name or IP address value in the host portion of the diversion header and redirects the contact header of the 302 response.
http client connection idle timeout	Sets the number of seconds for which the HTTP client waits before terminating an idle connection.

Command	Description
http client connection persistent	Enables HTTP persistent connections so that multiple files can be loaded by using the same connection.
http client connection timeout	Sets the number of seconds for which the HTTP client waits for a server to establish a connection before abandoning its connection attempt.
ip qos dscp	Configures the DSCP value for QoS.
localhost	Globally configures CUBE to substitute a DNS hostname or domain as the localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers in outgoing messages.
max-conn	Specifies the maximum number of incoming or outgoing connections for a particular VoIP dial peer.
max-forwards	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Globally sets the maximum number of hops, that is, proxy or redirect servers that can forward the SIP request.
media	Enables media packets to pass directly between endpoints without the intervention of CUBE, and enables signaling services.
media disable-detailed-stats	Disables the collection of detailed call statistics.
media profile asp	Creates a media profile to configure acoustic shock-protection parameters.
media profile nr	Creates a media profile to configure noise-reduction parameters.
media profile stream-service	Enables stream service on CUBE.
media profile video	Creates a media profile video.
media-address voice-vrf	Associates an RTP port range with VRF.
media-inactivity-criteria	Specifies the mechanism for detecting media inactivity (silence) on a voice call.
midcall-signaling	Configures the method that is used for signaling messages.
min-se	Changes the minimum session expiration (Min-SE) header value for all the calls that use the SIP session timer.
nat	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Uses SIP Network Address Translation (NAT) global configuration.
nat media-keepalive	Enables media keepalive packet transmission for the specified interval of time.

Command	Description
notify redirect	Enables application handling of redirect requests for all VoIP dial peers.
notify ignore substate	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Specifies Ignoring the Subscription-State header in a Notify message.
notify telephone-event	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Configures the maximum interval between two consecutive NOTIFY messages for a particular telephone event.
num-exp	Defines how to expand a telephone extension number into a particular destination pattern.
options-ping	Enables in-dialog options.
outbound-proxy	Configures a SIP outbound proxy for outgoing SIP messages globally.
pass-thru content	Enables the pass-through of SDP from in-leg to the out-leg.
permit hostname	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Stores hostnames used during validation of initial incoming INVITE messages.
privacy	Sets privacy support at the global level as defined in RFC 3323.
privacy-policy	Configures the privacy header policy options at the global level.
progress_ind	Configures an outbound dial peer on a CUBE to override and remove or replace the default progress indicator in specified call messages.
protocol mode	Configures the Cisco IOS SIP stack.
random-contact	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Populates an outgoing INVITE message with random-contact information instead of clear-contact information.
reason-header override	Enables cause code passing from one SIP leg to another.
redirect ip2ip	Redirects SIP phone calls to SIP phone calls globally on a gateway.
redirection	Enables the handling of 3*xx* redirect messages
referto-passing	Disables dial peer lookup and modification of the Refer-To header when the CUBE passes across a REFER message during a call transfer.

Command	Description
registrar	Enables SIP gateways to register E.164 numbers on behalf of analog telephone voice ports (FXS), IP phone virtual voice ports (EFXS), and SCCP phones with an external SIP proxy or SIP registrar.
rel1xx	Enables SIP provisional responses (other than 100 Trying) to be sent reliably to the remote SIP endpoint.
remote-party-id	Enables translation of the Remote-Party-ID SIP header.
requri-passing	Enables pass-through of the host part of the Request-URI and To SIP headers.
retry bye	Configures the number of times that a BYE request is retransmitted to the other user agent.
retry invite	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Configures the number of times that a SIP INVITE request is retransmitted to the other user agent.
rtcp all-pass-through	Passes through all the RTCP packets in the datapath.
rtcp keepalive	Configures RTCP keepalive report generation and generates RTCP keepalive packets.
rtp payload-type	Identifies the payload type of an RTP packet.
rtp-media-loop count	Configures the number of media loops before RTP voice and video media packets are dropped.
rtp-port	Configures the real-time protocol range.
rtp-ssrc multiplex	Multiplexes RTCP packets with RTP packets and sends multiple synchronization source in RTP headers (SSRCs) in an RTP session.
secure-ciphersuite	Configures the cipher suites (encryption algorithms) to be used for encryption over HTTPS for a WebSocket connection in CUBE.
session refresh	Enables SIP session refresh globally.
session transport	Configures a VoIP dial peer to use TCP or UDP as the underlying transport layer protocol for SIP messages.
set pstn-cause	Maps an incoming PSTN cause code to a SIP error status code.
set sip-status	Maps an incoming SIP error status code to a PSTN cause code.
signaling forward	Configures global settings for transparent tunneling of QSIG, Q.931, H.225, and ISUP messages.
silent discard untrusted	Discards SIP requests from untrusted sources in an incoming SIP trunk.

Command	Description
sip-server	Configures a network address for the SIP server interface.
srtp	Specifies that SRTP be used to enable secure calls and call fallback.
srtp negotiate	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Enables the Cisco IOS Session Initiation Protocol (SIP) gateway to accept and send a Real-Time Transport Protocol (RTP) Audio/Video Profile (AVP) at the global configuration level.
stun	Enters STUN configuration mode for configuring firewall traversal parameters.
stun flowdata shared-secret	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Configures a secret shared on a call control agent.
stun usage firewall-traversal flowdata	Enables firewall traversal using STUN.
supplementary-service media-renegotiate	Globally enables midcall media renegotiation for supplementary services.
timers	Configures SIP-signaling timers.
transport	Configures the SIP user agent (gateway) for SIP signaling messages in inbound calls through the SIP TCP, TLS over TCP, or UDP socket. This command supports TLS version 1.3 and all associated ciphers.
uc secure-wsapi	Configures a secure Cisco Unified Communication IOS services environment for a specific application.
uc wsapi	Configures a nonsecure Cisco Unified Communication IOS services environment for a specific application.
update-callerid	Enables sending updates for caller IDs.
url (SIP)	Configures URLs to either the SIP, SIP secure (SIPS), or telephone (TEL) format for your VoIP SIP calls.
vad	Enables VAD for calls using a specific dial peer.
video codec	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a.
voice cause code	Sets the internal Q850 cause code mapping for, voice and enters voice cause configuration mode.
voice class codec	Enters voice-class configuration mode and assigns an identification tag number for a codec voice class.
voice class dpg	Creates a dial-peer group for grouping multiple outbound dial peers.

Command	Description
voice class e164-pattern-map	Creates an E.164 pattern map that specifies multiple destination E.164 patterns in a dial peer.
voice class media	Configures media control parameters for voice.
voice class server-group	Enters voice-class configuration mode and configures server groups (groups of IPv4 and IPv6 addresses) that can be referenced from an outbound SIP dial peer.
voice-class sip options-keepalive	Monitors connectivity between CUBE VoIP dial peers and SIP servers.
voice class sip-copylist	Configures a list of entities to be sent to the peer call leg.
voice class sip-event-list	Configures a list of SIP events to be passed through.
voice class sip-hdr-passthrulist	Configures a list of headers to be passed through the route string.
voice-class sip nat media-keepalive	Configures media keepalive to enable media keepalive packets to be transmitted for the interval specified.

voice class sip-profiles	Configures SIP profiles for a voice class.
	Configuring a sip profile, **request REGISTER sip-header Authorization modify "550\"," [550@dl.ims.airtel.in|mailto:550@dl.ims.airtel.in]"**, on a device throws a warning message:
	`Device# show run`
	`sec sip-profiles voice class sip-profiles 4 rule 2`
	`request REGISTER sip-header Authorization modify`
	`"550\","`
	`"[550@dl.ims.airtel.in|mailto:550@dl.ims.airtel.in]""`

voice class srtp-crypto	Enters voice class configuration mode and assigns an identification tag for an **srtp-crypto voice class** command.
voice class uri	Creates or modifies a voice class for matching dial peers to a SIP or TEL URI.
voice class tls-cipher	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Configures an ordered set of TLS cipher suites.
voice class tls-profile	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Enables voice class configuration mode, and assigns an identification tag for a TLS profile.
voice iec syslog	Enables viewing of internal error codes as they are encountered in real time.
voice statistics iec	Enables collection of internal error code statistics.

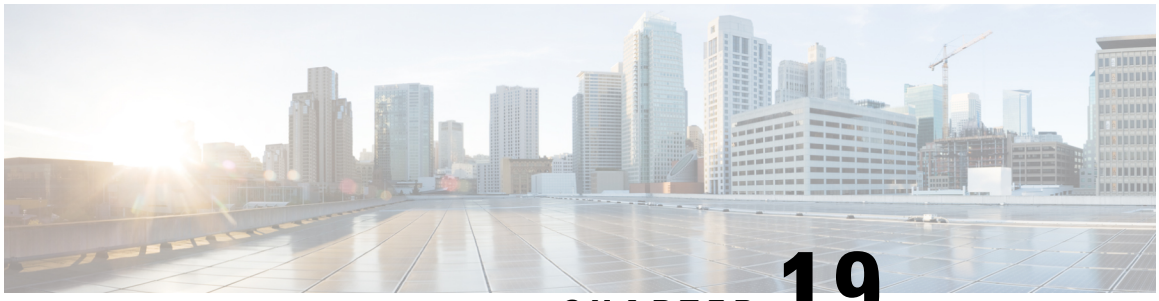
Command	Description
xfer target	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a . Routes the INVITE to the refer-to destination in the REFER consume case. The routing decision is made based on the xfer target destination.

SRST commands

The following table lists the commands that are supported by Cisco Catalyst SD-WAN CLI templates for SRST. Click a command name in the Command column to view information about the command, its syntax, and its use.

Table 138: Cisco Catalyst SD-WAN CLI template commands for SRST

Command	Description
http client secure-ciphersuite	Sets the secure encryption cipher suite for the HTTP client.
transport-tcp-tls (call-manager-fallback)	Configures a specific TLS version for Unified Secure SCCP SRST, in call-manager-fallback mode.



CHAPTER 19

Onboarding ThousandEyes Agent and Onboarding Tests

- Feature History for Simplified Onboarding of Cisco ThousandEyes Agent, on page 415
- Simplified workflow for onboarding Cisco ThousandEyes agents and configuring tests, on page 415
- Create an IP Pool for the Cisco ThousandEyes Agents, on page 416
- Prerequisites for simplified workflow, on page 416
- Restrictions for simplified workflow, on page 417
- Configure Cisco ThousandEyes agent and tests using simplified workflow, on page 418
- Monitor onboarded Cisco ThousandEyes agents and configured tests, on page 419
- Troubleshoot Cisco ThousandEyes agent on edge device, on page 419

Feature History for Simplified Onboarding of Cisco ThousandEyes Agent

This table describes the developments of this feature, by release.

Table 139: Feature History

Feature Name	Release Information	Feature Description
Simplified Workflow for Onboarding Cisco ThousandEyes Agent and Configuring Tests	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	A simplified workflow to easily onboard Cisco ThousandEyes agent and configure tests using Cisco SD-WAN Manager.

Simplified workflow for onboarding Cisco ThousandEyes agents and configuring tests

The workflow simplifies the process of onboarding Cisco ThousandEyes agents and configuration of tests in SD-WAN Manager. Using the simplified workflow, you can easily onboard Cisco ThousandEyes agents and

configure application monitoring tests directly from Cisco SD-WAN Manager in a few steps. The streamlined workflow involves these steps:

- Establish a connection to the Cisco ThousandEyes platform through SD-WAN Manager,
- Configure tests in Cisco ThousandEyes directly from SD-WAN Manager,
- Choose applications, sites, and devices for testing and configure the necessary parameters in SD-WAN Manager, and
- Monitor the agents and tests from the **ThousandEyes Monitoring** dashboard in SD-WAN Manager.

Create an IP Pool for the Cisco ThousandEyes Agents

This section describes the procedure of onboarding Cisco ThousandEyes agent

Procedure

Step 1 From the menu, choose **Configuration** > **Network Hierarchy**.

Note
The page displays the site pool and region pool for the Global node.

Step 2 Click **Pools**.

Step 3 Click **Add Pool**.

Step 4 In the **Pool Name** field, enter a name for the pool.

Step 5 In the **Pool Description** field, enter a description of the pool.

Step 6 From the **Pool Type** drop-down list, choose **ThousandEyes**.

Step 7 In the **IP Subnet*** field, enter an IP address.

Step 8 In the **Prefix Length*** field, enter the prefix length of the system IP pool.

Step 9 Click **Add**.

What to do next

- Monitor the status of agents and enable or disable agents in the **ThousandEyes Monitoring** dashboard in the Cisco SD-WAN Manager.
- Launch **ThousandEyes Monitoring** dashboard to view test results.

Prerequisites for simplified workflow

You must complete the tasks in this section before initiating the simplified workflow.

Table 140: Tasks Before Running the Simplified Workflow

Configuration Task	Information
Deploy Cisco IOS XE Catalyst SD-WAN devices using the configuration group.	Refer to Deploy Devices Using the Deploy Configuration Group Workflow.
Upload Cisco ThousandEyes Enterprise agent software.	• To upload software on the SD-WAN Manager software repository, refer to Upload the Cisco ThousandEyes Enterprise Agent software to SD-WAN Manager, on page 429. • To add virtual images from a remote server, refer to the Add Virtual Images to the Repository section in the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.
Create an IP pool in the global node of Network Hierarchy Manager. When deploying Cisco ThousandEyes agent through the workflow, the Virtual Port Group Interface IP address contains this IP pool.	Refer to Create an IP Pool for the Cisco ThousandEyes Agents, on page 416.
Add IPv4 DNS server details in the Transport VPN feature of the Configuration Group associated with the device.	Refer to DNS.

Restrictions for simplified workflow

Minimum supported releases: Cisco Catalyst SD-WAN Manager Release 20.16.1 and Cisco IOS XE Catalyst SD-WAN Release 17.16.1a

Editing limitations for deployed ThousandEyes Agent Sites

The workflow does not support editing tests or updating agent parameters for sites with deployed Cisco ThousandEyes agents.

Workflow only supports devices with configuration groups

The simplified workflow supports only devices that are associated with configuration groups.

Workflow only supports one device in a site

The simplified workflow supports only devices associated with configuration groups. In the workflow, you can select only one device in a site to deploy the Cisco ThousandEyes Agent and configure tests associated with it. To deploy Cisco ThousandEyes Agent on multiple devices in a site, use the Configuration Group method, see Using Configuration Groups.

Configure Cisco ThousandEyes agent and tests using simplified workflow

This section describes the procedure of onboarding Cisco ThousandEyes agents and configuring monitoring tests directly from the SD-WAN Manager.

Before you begin

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.16.1 and Cisco IOS XE Catalyst SD-WAN Release 17.16.1a

- Ensure the following before initiating the simplified workflow:
  - You have a Cisco ThousandEyes account before using the simplified workflow to configure a Cisco ThousandEyes agent in Cisco SD-WAN Manager.
  - You must be a user with the Organization Admin role to access the Cisco ThousandEyes account.
- Create an IP pool in the global node of Network Hierarchy Manager, see Create an IP Pool for the Cisco ThousandEyes Agents, on page 416.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.

Step 2 Start the **Configure ThousandEyes** workflow.

Step 3 Read the terms and conditions. After accepting the terms and conditions, click **Connect ThousandEyes** to start the workflow.

Step 4 When the Cisco ThousandEyes portal opens, log in to your account using your login credentials. The page redirects to Cisco SD-WAN Manager.

Step 5 Follow the instructions provided in the workflow.

Note

- In the workflow, select all sites associated with a specific Configuration Group simultaneously. This ensures that the Configuration Group with Cisco ThousandEyes agent applies to all sites associated with the Configuration Group.
- The time required to onboard Cisco ThousandEyes agent and configure tests varies based on the size of your network.

What to do next

- Monitor the status of agents and enable or disable agents in the **ThousandEyes Monitoring** dashboard in the Cisco SD-WAN Manager.
- Launch **ThousandEyes Monitoring** dashboard to view test results.

Monitor onboarded Cisco ThousandEyes agents and configured tests

You can monitor the status of Cisco ThousandEyes agents and configured tests in the SD-WAN Manager.

Before you begin

Ensure you are on release Cisco Catalyst SD-WAN Manager Release 20.16.1 and Cisco IOS XE Catalyst SD-WAN Release 17.16.1a.

Procedure

Step 1 To monitor the status of Cisco ThousandEyes agents and configured tests in the SD-WAN Manager monitoring dashboard, navigate to **Tools** > **ThousandEyes Monitoring**.

You can view the online, offline, and disabled agents, and launch Cisco ThousandEyes from the dashboard.

Step 2 In the monitoring dashboard, review these sections:

- **Tests**: View information about the tests configured using the simplified workflow.
- **Agents**: View information about the status of Cisco ThousandEyes agents configured using the simplified workflow. It also provides a list of configured devices and sites for the test with the option to enable, disable, or delete a Cisco ThousandEyes agent.

Troubleshoot Cisco ThousandEyes agent on edge device

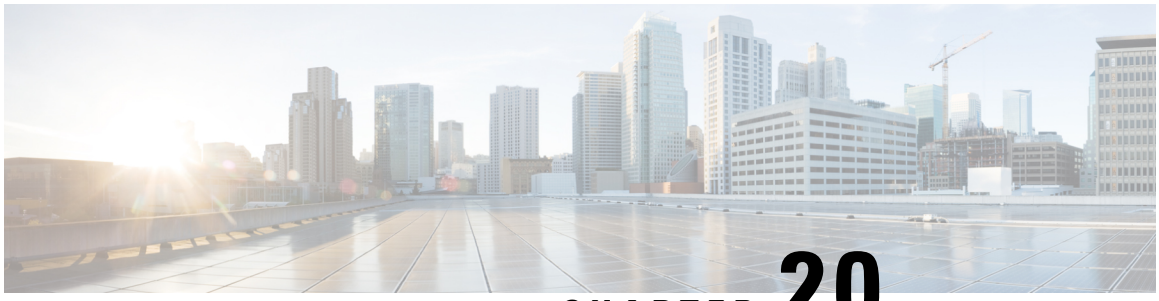
Before you begin

Ensure you are on release Cisco Catalyst SD-WAN Manager Release 20.16.1 and Cisco IOS XE Catalyst SD-WAN Release 17.16.1a.

Procedure

Step 1 Review these log files in SD-WAN Manager for error messages or relevant information: /var/log/nms/vmanage-server.log and /var/log/nms/vmanage-server-deviceconfig-template.log.

Step 2 Examine the audit logs to determine if the ThousandEyes test was posted or it failed.



CHAPTER 20

Monitoring with Cisco ThousandEyes

- Feature history for extended visibility with Cisco Catalyst SD-WAN and ThousandEyes, on page 421
- Extending visibility for Cisco Catalyst SD-WAN and Cisco ThousandEyes, on page 422
- Supported devices for running Cisco SD-WAN and Cisco ThousandEyes, on page 423
- ThousandEyes Enterprise Agent supported versions and system requirements, on page 425
- Prerequisites for extending visibility with SD-WAN Manager and Cisco ThousandEyes, on page 426
- Restrictions for Extending Visibility with SD-WAN Manager and Cisco ThousandEyes, on page 427
- Configure a Cisco ThousandEyes Enterprise Agent using a Configuration Group, on page 427
- Upload the Cisco ThousandEyes Enterprise Agent software to SD-WAN Manager, on page 429
- Provision Cisco ThousandEyes Enterprise Agent in a Service VPN or Transport VPN (VPN0), on page 430
- Provision a Cisco ThousandEyes Enterprise Agent in a Service VPN Using CLI, on page 433
- Uninstall the Cisco ThousandEyes Enterprise Agent software, on page 434
- Upgrade the Cisco ThousandEyes Enterprise Agent software, on page 434
- Troubleshoot the Cisco ThousandEyes Enterprise Agent on Cisco IOS XE Catalyst SD-WAN devices, on page 435

Feature history for extended visibility with Cisco Catalyst SD-WAN and ThousandEyes

The feature history table provides information about when specific features were introduced.

Table 141: Feature History

Feature Name	Release Information	Description
Extended Visibility with Cisco Catalyst SD-WAN and Cisco ThousandEyes	Cisco IOS XE Release 17.6.1a Cisco vManage Release 20.6.1	You can deploy Cisco ThousandEyes Enterprise agent natively as a container application on supported Cisco IOS XE Catalyst SD-WAN devices to integrate Cisco Catalyst SD-WAN with Cisco ThousandEyes. You can install and activate the Cisco ThousandEyes Enterprise agent through SD-WAN Manager. By integrating Cisco Catalyst SD-WAN with Cisco ThousandEyes, you can gain granular insights into network and application performance with full hop-by-hop path analysis across the Internet, and isolate fault domains for expedited troubleshooting and resolution.
Cisco ThousandEyes Support for Cisco 1000 Series Integrated Services Routers	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	You can deploy Cisco ThousandEyes Enterprise agent natively as a container application on Cisco ISR 1100X-6G devices. You can install and activate the Cisco ThousandEyes Enterprise agent through SD-WAN Manager.
Cisco ThousandEyes Support for Cisco Catalyst 8500 Series Edge Platforms and Cisco ASR 1000 Series Aggregation Services Routers	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	You can deploy Cisco ThousandEyes Enterprise agent natively as a container application on Cisco Catalyst 8500 Series Edge Platforms and Cisco ASR 1000 Series Aggregation Services Routers. You can install and activate the Cisco ThousandEyes Enterprise agent through SD-WAN Manager.
Extended Device Support for the Cisco ThousandEyes Agent in Cisco ISR 1100 Series	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	Support for the Cisco ThousandEyes Enterprise agent is extended to additional routers in Cisco ISR 1100 Series.
Extended Device Support for the Cisco ThousandEyes Agent to Industrial Routers	Cisco IOS XE Catalyst SD-WAN Release 17.18.2 Cisco Catalyst SD-WAN Manager Release 20.18.2	Support for the Cisco ThousandEyes Enterprise Agent is extended to include industrial routers in SD-WAN deployments.

Extending visibility for Cisco Catalyst SD-WAN and Cisco ThousandEyes

Cisco ThousandEyes is a SaaS application that:

- delivers end-to-end visibility across internal, external, and carrier networks,

- monitors network performance in real time to provide actionable insights, and
- optimizes application delivery and end-user experience through continuous analysis of network paths and services.

Deploy and configure the ThousandEyes Agent

From Cisco IOS XE Release 17.6.1, you can deploy and configure the Cisco ThousandEyes Enterprise agent on Cisco IOS XE Catalyst SD-WAN devices to enable extensive monitoring of the WAN traffic for enhanced visibility within and beyond the Cisco Catalyst SD-WAN fabric. The Cisco ThousandEyes Enterprise agent is an embedded Docker-based application that runs on Cisco IOS XE Catalyst SD-WAN devices as a docker-type container application using the IOX Docker application-hosting capability.

Services in the Cisco Networking Cloud

From Cisco Catalyst SD-WAN Manager Release 20.14.1, you can navigate to Cisco services hosted in the Cisco Networking Cloud, such as Cisco ThousandEyes. Enable the cross platform navigator in **Administration** > **Settings** > **Cross Platform Navigator**.

For more information on Cisco ThousandEyes and on configuring tests and viewing results in the Cisco ThousandEyes portal, see the *Cisco ThousandEyes Getting Started* documentation.

Supported devices for running Cisco SD-WAN and Cisco ThousandEyes

The table provides Cisco IOS XE Catalyst SD-WAN devices that support deployment of the Cisco ThousandEyes Enterprise agent as a container application.

Platform	Device Model	Architecture	Release
Cisco Catalyst 8300 Series Edge Platforms	C8300-1N1S-6T	x86_64	Cisco vManage Release 20.6.1 Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and later
	C8300-1N1S-4T2X		
	C8300-2N2S-6T		
	C8300-2N2S-4T2X		
Cisco Catalyst 8200 Series Edge Platforms	C8200-1N-4T	x86_64	
	C8200L-1N-4T		
Cisco 4000 Series Integrated Services Routers	ISR4461	x86_64	
	ISR4451		
	ISR4431		
	ISR4351		
	ISR4331		
	ISR4321		
	ISR4221X		

Platform	Device Model	Architecture	Release
Cisco 1000 Series Integrated Services Routers	ISR1100X-6G	x86_64	Cisco vManage Release 20.7.1 Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and later
Cisco Catalyst 8500 Series Edge Platforms	C8500-12X	x86_64	Cisco vManage Release 20.8.1 Cisco IOS XE Catalyst SD-WAN Release 17.8.1a and later
	C8500-12X4QC		
	C8500L-8S4X		
Cisco ASR 1000 Series Aggregation Services Routers	ASR 1001-HX	x86_64	
	ASR 1001-X		
	ASR 1002-HX		
	ASR 1002-X		
	ASR 1006-X (RP3)		
Cisco 1000 Series Integrated Services Routers	C1111X-8P	aarch64	Cisco Catalyst SD-WAN Manager Release 20.16.1 Cisco IOS XE Catalyst SD-WAN Release 17.16.1a
	C1121X-8P		
	C1121X-8PLTEP		
	C1121X-8PLTEPW		
	C1126X-8PLTEP		
	C1127X-8PLTEP		
	C1131X-8PW		
	C1131X-8PLTEPW		
	C1161X-8P		
	C1161X-8PLTEP		
Cisco 8100 Series Secure Routers	C8151-G2 C8161-G2	aarch64	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a
Cisco 8200 Series Secure Routers	C8235-E-G2, C8231-E-G2 C8235-G2 C8231-G2	aarch64	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a

Platform	Device Model	Architecture	Release
Cisco 8300 Series Secure Routers	C8355-G2 C8375-E-G2	aarch64	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a **Note** C8375-E-G2 is supported from Cisco IOS XE Catalyst SD-WAN 17.15.3
Cisco 8400 Series Secure Routers	C8400-G2	aarch64	Cisco IOS XE Catalyst SD-WAN 17.15.3
Cisco IR1800 Rugged Series Routers	IR1833 IR1835	aarch64	Cisco IOS XE Catalyst SD-WAN Release 17.18.2 Cisco Catalyst SD-WAN Manager Release 20.18.2
Cisco IR1101 Rugged Series Routers	IR1101	aarch64	Cisco IOS XE Catalyst SD-WAN Release 17.18.2 Cisco Catalyst SD-WAN Manager Release 20.18.2
Cisco IR8100 Heavy Duty Series Routers	IR8140H IR8140H-P	aarch64	Cisco IOS XE Catalyst SD-WAN Release 17.18.2 Cisco Catalyst SD-WAN Manager Release 20.18.2
Cisco IR8300 Rugged Series Routers	IR8340	x86_64	Cisco IOS XE Catalyst SD-WAN Release 17.18.2 Cisco Catalyst SD-WAN Manager Release 20.18.2

ThousandEyes Enterprise Agent supported versions and system requirements

We recommend you to update to the latest version of the ThousandEyes Enterprise agent. Download the latest version of the ThousandEyes Enterprise agent from the Cisco ThousandEyes Agent page.

Storage and DRAM Requirements

- External Storage: On devices that are equipped with external storage (SSD M.2 NVMe), the Cisco ThousandEyes Enterprise agent is installed in the external storage. The minimum external storage capacity that is required to install the Cisco ThousandEyes Enterprise agent is 8 GB. If the device does not have sufficient external storage capacity, upgrade the storage capacity to meet the minimum requirement.

  Although the minimum external storage capacity that is required is 8 GB, we recommend that you provision the device with an external storage capacity of 16 GB or more. With the minimum external

storage capacity, you may need to manually clean up files while upgrading the software image on the device.

- Bootflash: On devices that are not equipped with external storage, the Cisco ThousandEyes Enterprise agent is installed on the bootflash. The minimum bootflash capacity that is required to install the Cisco ThousandEyes Enterprise agent is 8 GB. If the device does not have sufficient bootflash capacity, upgrade the storage capacity to meet the minimum requirement.



Note On the ISR1100X-6G, the Cisco ThousandEyes Enterprise agent is installed on the bootflash. For this particular device model, the minimum bootflash capacity that is required to install the agent is 16 GB.

Although the minimum bootflash capacity that is required is 8 GB, we recommend that you provision the device with an bootflash capacity of 16 GB or more. With the minimum bootflash capacity, you may need to manually clean up files while upgrading the software image on the device.

- DRAM: The minimum DRAM capacity that is required to install the Cisco ThousandEyes Enterprise agent is 8 GB. If a device does not have the minimum DRAM capacity that is required to install the Cisco ThousandEyes Enterprise agent, upgrade the DRAM to meet the minimum requirement.
- Co-residency: Cisco ThousandEyes Enterprise agent can be deployed with other applications if the device has the resources (CPU, memory, and storage) to run the other applications. If the available resources are not sufficient to run the other applications, IOX generates an error message and does not run the other applications.
- To host the Cisco ThousandEyes Enterprise agent, a Cisco IOS XE Catalyst SD-WAN device must have a minimum of 8 GB DRAM. To host additional applications such as UTD and DRE on the same device, provision the device with at least a 16 GB DRAM.

Prerequisites for extending visibility with SD-WAN Manager and Cisco ThousandEyes

To extend network visibility using SD-WAN Manager and Cisco ThousandEyes, ensure you meet these prerequisites.

- Before deploying the Cisco ThousandEyes Enterprise agent, create an account on the Cisco ThousandEyes portal and obtain an account group token. The token authenticates the agent with Cisco ThousandEyes and associates it with the correct account.

  For information on obtaining the account group token, see *Where Can I Get the Account Group Token?* on Cisco ThousandEyes Documentation portal.
- The Cisco ThousandEyes Enterprise agent requires DNS name resolution and HTTP/HTTPS connectivity to discover and register with the Cisco ThousandEyes portal. Ensure that this connectivity exists before deploying the agent by configuring the appropriate firewall rules, NAT settings, upstream routing, and other related settings.

  For more information on the required firewall configuration, see *Firewall Configuration for Enterprise Agents* on Cisco ThousandEyes Documentation portal.

Restrictions for Extending Visibility with SD-WAN Manager and Cisco ThousandEyes

AppRoute data policies do not affect probes sourced from Virtual Port-Group interfaces

Cisco ThousandEyes Enterprise agent probes are sourced from Virtual Port-Group interfaces and are not affected by AppRoute data policies.

Browser-based application tests not supported

The Cisco ThousandEyes Enterprise agent, hosted natively as a container application on Cisco IOS XE Catalyst SD-WAN devices, does not support browser-based application tests, such as page load test and transaction test.

Limitations of ThousandEyes Instance Modification

For every configuration change to the ThousandEyes instance, you must uninstall or deactivate and then reinstall and reactivate it for the changes to take effect.

For Cisco IOS XE Catalyst SD-WAN devices prior to Cisco IOS XE Release 17.6.1, you can install the Docker Enterprise agent image either directly from ThousandEyes servers, or by uploading it using SCP, FTP, TFTP, or USB storage, depending on internet accessibility. It depends on whether the router has direct internet access or not.

For Cisco IOS XE Catalyst SD-WAN devices after Cisco IOS XE Release 17.6.1, you can install the Enterprise Agent using bootflash, in addition to the previous methods.

Configure a Cisco ThousandEyes Enterprise Agent using a Configuration Group

Configure Cisco ThousandEyes Enterprise Agent settings using the ThousandEyes feature in a configuration group.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure a ThousandEyes feature in Other profile.

a. Configure ThousandEyes parameters.

Table 142: Parameters

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Cisco Catalyst SD-WAN device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Cisco Catalyst SD-WAN device to a device template. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, host name, GPS location, and site ID.
Global (indicated by a globe icon)	Enter a value for the parameter and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

b. Configure the ThousandEyes settings.

Table 143: Settings

Field	Description
Type	Choose a feature from the drop-down list.
Feature Name	Enter a name for the feature.
Description	Enter a description of the feature. The description can contain any characters and spaces.
Account Group Token	Enter the Cisco ThousandEyes Account Group Token.
VPN	Service VPN. The **Global** or the **Device Specific** setting indicates service VPN. When you set the VPN configuration as a **Global** or a **Device Specific** setting, enter the ID of the service VPN in which you want to provision the Cisco ThousandEyes Enterprise agent.
Management IP	Enter an IP address for the Cisco ThousandEyes Enterprise agent. This field is available only when you specify the service VPN.
Management Subnet	Choose a subnet mask from the drop-down list for the Cisco ThousandEyes Enterprise agent. This field is available only when you specify the service VPN. **Note** This IP-prefix address (**Management IP** and **Management Subnet**) must be unique within the fabric and must not overlap with the IP addresses of other branch agents.

Field	Description
Agent Default Gateway	Enter a default gateway address. This IP address is assigned to the virtual port group of the router. This field is available only when you specify the service VPN.
Name Server IP	Enter the IP address of your preferred DNS server. This server can exist within or outside the Cisco Catalyst SD-WAN fabric but must be reachable from the service VPN.
Host Name	Enter the hostname that the agent must use when registering with the Cisco ThousandEyes portal. By default, the agent uses the hostname of the Cisco IOS XE Catalyst SD-WAN device.
Proxy Type	If the Cisco ThousandEyes Enterprise agent must use proxy server for external access, choose one of these as proxy type: • **static** • **pac** • **none** Static proxy settings: • **Proxy Host**: Set the configuration as a **Global** setting and enter the hostname of the proxy server. • **Proxy Port**: Set the configuration as a **Global** setting and enter the port number of the proxy server. PAC settings: • **PAC URL**: Set the configuration as a **Global** setting and enter the URL of the proxy auto-configuration (PAC) file.

What to do next

Also see Deploy a configuration group.

Upload the Cisco ThousandEyes Enterprise Agent software to SD-WAN Manager

Perform this task to make the Cisco ThousandEyes Enterprise Agent software available for installation through SD-WAN Manager.

Before you begin

Download the latest version of Cisco ThousandEyes Enterprise agent software from the Cisco ThousandEyes Agent Settings page.

Procedure

Step 1 From the SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.

Step 2 Click **Virtual Images**.

Step 3 Click **Upload Virtual Image** > **Manager**.

Step 4 In the **Upload VNF's Package to Manager** dialog box, browse to select the downloaded Cisco ThousandEyes Enterprise Agent software file, or drag and drop the file into the dialog box.

Step 5 Enter a description for the file.

Step 6 (Optional) Add desired tags.

Step 7 Click **Upload**.

What to do next

Proceed to install the uploaded Cisco ThousandEyes Enterprise agent software on relevant devices as needed.

Provision Cisco ThousandEyes Enterprise Agent in a Service VPN or Transport VPN (VPN0)

You can provision the Cisco ThousandEyes Enterprise agent in a service VPN for more visibility into the performance of the Cisco Catalyst SD-WAN overlay and underlay networks.

When you host the ThousandEyes agent on a router, you can deploy it in either a Service VPN or the Transport VPN (VPN0), based on your functional requirements and network topology. Deploying the ThousandEyes agent in VPN0 offers a simple routing approach when you need to send probe traffic over a single available underlay WAN link. In environments with multiple WAN links, Cisco recommends deploying the ThousandEyes agent in a Service VPN. This deployment method gives you granular control and enables you to create policies that direct probe traffic over specific underlay WAN paths, effectively simulating real-world traffic flows. If you deploy the ThousandEyes agent in VPN0 in a multi-WAN environment, the router load-balances probe traffic across all available WAN links, which may result in non-actionable monitoring insights.

Before you begin

- Ensure that DNS and NAT are correctly configured so that the Cisco ThousandEyes Enterprise Agent can access and connect to the Cisco ThousandEyes application.
- Upload Cisco ThousandEyes Enterprise agent software to SD-WAN Manager software repository.

Note If multiple versions of the Cisco ThousandEyes Enterprise agent software are present in the SD-WAN Manager software repository, while provisioning the agent, SD-WAN Manager installs and activates the latest version of the agent software.

- For application monitoring use cases, deploy the ThousandEyes agent in the Service VPN and use an SD-WAN data policy to send ThousandEyes probes across transports

Procedure

Step 1 Create feature template for the Cisco ThousandEyes Enterprise agent:

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

b) Click **Feature Templates**, and click **Add Template** to select an appropriate device model.

Note
In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled as **Feature**.

c) Choose the supported devices to which you want to apply this template.

d) In the **Other Templates** section, click **ThousandEyes Agent**.

e) **Template Name**: Enter a name for the template. Ensure that the template name is unique.

f) **Description**: Enter a description for the template.

g) In the **BASIC CONFIGURATION** section, configure these fields:

Account Group Token	Enter the Cisco ThousandEyes Account Group Token.
VPN	**1.** Set the VPN configuration as a **Global** or a **Device Specific** setting. **2.** Enter the ID of the service VPN in which you want to provision the Cisco ThousandEyes Enterprise agent.
Agent IP Address	Enter an IP address for the Cisco ThousandEyes Enterprise agent. This IP Address should be unique within the fabric and should not overlap with the IP addresses of other branch agents.
Agent Default Gateway	Enter a default gateway address. This IP address is assigned to the virtual port group of the router.

Note
You can create and allocate a service subnet for the agent network. Two usable IP addresses are required to provision the Cisco ThousandEyes Enterprise agent on each Cisco IOS XE Catalyst SD-WAN device. One of the IP addresses must be assigned to the agent and second IP address to the router virtual port group.

h) In the **ADVANCED** section, configure these fields:

Name Server	(Optional parameter from Cisco vManage Release 20.7.1 and Cisco IOS XE Release 17.7.1a) Enter the IP address of your preferred DNS server. This server can exist within or outside the Cisco Catalyst SD-WAN fabric but must be reachable from the service VPN.
Hostname	(Optional) Enter the hostname that the agent must use when registering with the Cisco ThousandEyes portal. By default, the agent uses the Cisco IOS XE Catalyst SD-WAN device's hostname.
Web Proxy Type	(Optional) If the Cisco ThousandEyes Enterprise agent must use proxy server for external access, choose one of the following as proxy type: • **Static** • **PAC** Static proxy settings: • **Proxy Host**: Set the configuration as a **Global** setting and enter the hostname of the proxy server. • **Proxy Port**: Set the configuration as a **Global** setting and enter the port number of the proxy server. PAC settings: • **PAC URL**: Set the configuration as a **Global** setting and enter the URL of the proxy auto-configuration (PAC) file.

i) Click **Save**.

Step 2 Attach the ThousandEyes Agent feature template to device template:

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
b) Click **Device Templates**.

Note
In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled as **Device**

c) Find the device template for the target device.
d) For this template, click **…**, and click **Edit**.
e) Click **Additional Templates**.
f) Click **Update**.
g) Update necessary variables, if any, and click **Next**.
h) Review the configuration and click **Configure Devices**.

Step 3 Repeat Step 2 for each device on which you want to deploy the Cisco ThousandEyes Enterprise agent.

The Cisco ThousandEyes Enterprise agent is deployed on the chosen devices. The agent registers with and establishes secure communication with the cloud-based Cisco ThousandEyes application to receive necessary updates and configuration.

What to do next

You can configure various tests and see resultant network and application telemetry data on the Cisco ThousandEyes portal.

Provision a Cisco ThousandEyes Enterprise Agent in a Service VPN Using CLI

This section also provides example CLI configurations to provision the Cisco ThousandEyes Enterprise agent in a service VPN.

Use the example command sequences described in this section to provision the Cisco ThousandEyes Enterprise agent on Cisco IOS XE Catalyst SD-WAN devices through a device CLI template or an add-on CLI template.

Before you begin

- Ensure that the appropriate DNS and NAT configuration exists to enable the Cisco ThousandEyes Enterprise agent to discover and connect to the Cisco ThousandEyes application.
- Upload Cisco ThousandEyes Enterprise agent software to SD-WAN Manager.

Note If you have uploaded more than one version of the Cisco ThousandEyes Enterprise agent software to the SD-WAN Manager software repository, while provisioning the agent, SD-WAN Manager installs and activates the latest version of the agent software.

Procedure

Step 1 Enable IOX on the device.

```
iox
```

Step 2 Configure virtual port group. The virtual port group acts as the gateway for the Cisco ThousandEyes Enterprise agent.

```
interface VirtualPortGroup4
 vrf forwarding 100
  ip address 192.168.61.1 255.255.255.252
```

Step 3 Configure app-hosting paramters for the Cisco ThousandEyes Enterprise agent.

```
app-hosting appid te
app-vnic gateway0 virtualportgroup 4 guest-interface 0
 guest-ipaddress 192.168.61.2 netmask 255.255.255.252
app-default-gateway 192.168.61.1 guest-interface 0
app-resource docker
 prepend-pkg-opts
 run-opts 1 "-e TEAGENT_ACCOUNT_TOKEN=z0kemf"
 run-opts 2 "--hostname ISR4461TE"
 run-opts 3 "-e TEAGENT_PROXY_TYPE=STATIC -e TEAGENT_PROXY_LOCATION=proxy-exmaple.com:80"
```

```
name-server0  192.168.168.183
start
```

Note

- Use the proxy configuration only if the Cisco ThousandEyes agent does not have an Internet access without a proxy. The hostname is optional. If you do not provide the hostname during the installation, the device hostname is used as the Cisco ThousandEyes agent hostname, which appears on the Cisco ThousandEyes portal. From Cisco IOS XE Release 17.7.1a, the DNS name server information is optional.
- If the Cisco ThousandEyes agent uses a private IP address, establish a connection to the device through NAT.

Uninstall the Cisco ThousandEyes Enterprise Agent software

Remove the Cisco ThousandEyes Enterprise Agent software from a device by updating its configuration template so the software is no longer provisioned or managed through SD-WAN Manager.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Device Templates**.

Note
In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled as **Device**

Step 3 Find the device template for the device from which the Cisco ThousandEyes agent software must be removed.

Step 4 For this template, click **…** and then click **Edit**.

Step 5 Click **Additional Templates**.

Step 6 In the **Additional Templates** section, for **ThousandEyes Agent** choose **None** from the drop-down list.

Step 7 Click **Update**.

Step 8 Update necessary variables, if any, and click **Next**.

Step 9 Review the configuration and click **Configure Devices**.

What to do next

Verify that the agent software has been removed from the affected device(s) by checking device status and software inventory.

Upgrade the Cisco ThousandEyes Enterprise Agent software

Upgrade Cisco ThousandEyes Enterprise Agent software on edge routers through SD-WAN Manager.

This section provides procedure to upgrade the Cisco ThousandEyes Enterprise Agents have the latest enhancements and security updates.

Before you begin

Download a new version of Cisco ThousandEyes Enterprise agent software and upload the software to SD-WAN Manager. See *Upload Cisco ThousandEyes Enterprise Agent Software to Cisco SD-WAN Manager*.

Procedure

Step 1 From the SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.

Step 2 Select the Cisco IOS XE Catalyst SD-WAN devices on which you want to upgrade the Cisco ThousandEyes Enterprise agent software.

Step 3 Click **Upgrade Virtual Image**.

Step 4 In the **Virtual Image Upgrade** dialog box, choose the new version of the Cisco ThousandEyes Enterprise agent software from the drop-down list.

Step 5 Click **Upgrade**.

Step 6 On the **Maintenance** > **Software Upgrade** page, select the Cisco IOS XE Catalyst SD-WAN devices on which you upgraded the Cisco ThousandEyes Enterprise agent software.

Step 7 Click **Activate Virtual Image**.

What to do next

Verify agent status and functionality on each router.

Troubleshoot the Cisco ThousandEyes Enterprise Agent on Cisco IOS XE Catalyst SD-WAN devices

Identify and resolve issues with the Cisco ThousandEyes Enterprise Agent running on supported Cisco IOS XE Catalyst SD-WAN devices.

Before you begin

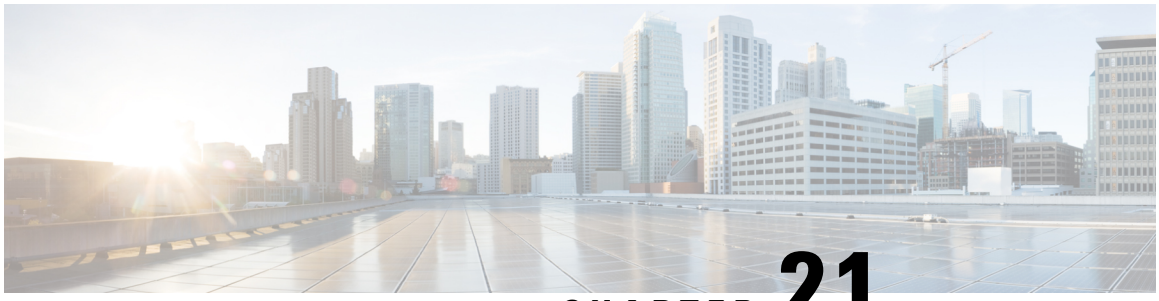
Procedure

Step 1 Connect to Cisco ThousandEyes Enterprise agent.

```
Device#app-hosting connect appid Appid session /bin/bash
```

Step 2 To verify the agent configuration, check the following CFG file: `/etc/te-agent.cfg`.

Step 3 To view the agent logs, check the following file: `/var/log/agent/te-agent.log`.



CHAPTER 21

EtherChannels

- Feature history for EtherChannels, on page 437
- EtherChannels on the service side, on page 438
- EtherChannels on the transport side, on page 446
- Monitor configured EtherChannel using CLI, on page 454
- Aggregate EtherChannel Quality of Service, on page 455

Feature history for EtherChannels

This table describes the developments of the EtherChannels feature, by release.

Table 144: Feature history

Feature Name	Release Information	Description
EtherChannels on the service side	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature allows you to configure EtherChannels on Cisco IOS XE Catalyst SD-WAN devices on the service side. EtherChannels provide fault-tolerant, high-speed links, redundancy, and increased bandwidth between Cisco Catalyst SD-WAN devices and other network equipment. You can configure EtherChannels only using the CLI device templates and CLI add-on feature templates.
EtherChannels on the transport side	Cisco IOS XE Catalyst SD-WAN Release 17.13.1aCisco Catalyst SD-WAN Manager Release 20.13.1	This feature adds support for configuring EtherChannels on the transport side of a Cisco IOS XE Catalyst SD-WAN devices. This feature also enables aggregate EtherChannel Quality of Service (QoS) on the transport side, optimizing network utilization and performance for specific traffic types. **Note** This feature has limited availability.

Feature Name	Release Information	Description
Load balancing for EtherChannels on the transport Side	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	This feature allows you to configure load balancing for EtherChannels on the transport side for Cisco IOS XE Catalyst SD-WAN devices.
Configuration Groups for EtherChannels	Cisco IOS XE Catalyst SD-WAN Release 17.15.x Cisco Catalyst SD-WAN Manager Release 20.15.1	This feature allows you to configure EtherChannels on both service and transport sides using configuration groups in Cisco SD-WAN Manager.
Load balancing for EtherChannels on individual port channels	Cisco IOS XE Catalyst SD-WAN Release 17.15.x Cisco Catalyst SD-WAN Manager Release 20.15.1	With this feature you can load balance EtherChannels for individual port channels on service and transport side using CLI templates.

EtherChannels on the service side

EtherChannels on the service side is a capability that

- extends EtherChannel functionality to the service-facing interfaces of Cisco IOS XE Catalyst SD-WAN device s,
- provides fault-tolerant, high-speed links, redundancy, and increased bandwidth for service-side connections, and
- is configurable through CLI device templates, CLI add-on feature templates, and configuration groups.

Supported devices for service side EtherChannel

This section provides a list of Cisco platforms that support EtherChannel functionality, including load balancing, on the service side. This information is crucial for planning and deploying Cisco Catalyst SD-WAN solutions that leverage EtherChannels for enhanced bandwidth and redundancy on service-facing interfaces.

The following platforms support EtherChannel and also offer load balancing for EtherChannel on the service side:

- Cisco 4000 Series Integrated Services Routers
  - Cisco 4451-X Integrated Services Router
  - Cisco 4461 Integrated Services Router
  - Cisco 4431 Integrated Services Router
  - Cisco 4331 Integrated Services Router
  - Cisco 4351 Integrated Services Router

- Cisco ASR 1000 Series Aggregation Services Routers
  - Cisco ASR 1001-X Router
  - Cisco ASR 1006-X Router
  - Cisco ASR 1001-HX Router
  - Cisco ASR 1002-HX Router
  - Cisco ASR 1002-X Router
- Cisco Catalyst 8000V Edge Software
- Cisco Catalyst 8200 Router
- Cisco Catalyst 8300 Router
- Cisco Catalyst 8500 Series Edge Router

Supported NIMs

Any L3 Ethernet interface on Network Interface Modules (NIMs) or Service Modules (SMs) can support EtherChannels on the service side.



Note Network Interface Modules (NIMs) with L2 ports do not support EtherChannels on the service side.

Prerequisites for EtherChannels on the service side

Before configuring EtherChannels on the service side, ensure that the following prerequisties are met. These prerequisites are essential for your EtherChannel configuration.

- All the LAN ports in each EtherChannel must be of the same speed.
- All the LAN ports must be configured on Layer 3 service-side ports.
- All member interfaces in a port channel must have the same speed and duplex, when using platforms that support multiple rate SFPs on the same port.

Restrictions for EtherChannels on the service side

Maximum port channels

The maximum number of port channel interfaces that a device can support varies, depending on the particular model of the device.

Port channel configuration

You can configure EtherChannels on a device by using the CLI, or using only the CLI templates or CLI add-on feature templates in Cisco SD-WAN Manager.

Hardware and interface compatibility

- Network Interface Modules (NIMs) with L2 ports do not support EtherChannels on the service side.
- The EtherChannel Quality of Service (QoS) feature on port channels is not supported on the service side.
- The Aggregate EtherChannel QoS feature on port channels is not supported on the service side.
- An EtherChannel does not support Digital Signal Processor (DSP) farm services and voice services.
- Sub interfaces cannot be added as member of EtherChannel.

Load balancing for service side EtherChannels using CLI commands

This topic describes the CLI commands and methods for configuring load balancing on service side EtherChannels, including enabling load balancing on individual port channels, configuring global and per-port-channel flow-based hash algorithms, and enabling VLAN load balancing.

The following tasks detail how to configure load balancing options for service side EtherChannels using the CLI commands:

- Enable load balancing on an individual port channel, on page 440
- Enable hash algorithms for flow-based load balancing on a global level, on page 442
- Enable hash algorithms flow-based load balancing on an individual port channel interface, on page 442
- Enable VLAN load balancing per port channel on the service side, on page 443
- Configure load balancing for EtherChannels on the service side using CLI commands, on page 444

Note From Cisco Catalyst SD-WAN Manager Release 20.15.1, you can use any other hash algorithims for load balancing on the service side.

The Hash Algorithms For Flow-based Load Balancing feature is supported only on Cisco Aggregation Services Routers platforms, where the hardware load-balancing for Etherchannel is supported. This command is not supported on Cisco Integrated Services Routers and Cisco Catalyst Router platforms.

Enable load balancing on an individual port channel

Use this procedure to apply load balancing on an individual port channel.

Before you begin

You must be in global configuration mode and have an existing port channel created.

Complete these steps to enable load balancing on an individual port channel.

Procedure

Step 1 Enter the port channel interface configuration mode.

```
interface Port-channel channel-number
```

Step 2 Enable load balancing on an individual port channel.

```
load-balancing flow
```

The specified port channel now uses the configured load balancing method, overriding any global settings.

This example shows how to set the load-balancing method to flow, when VLAN-manual method is configured globally:

```
Device# config-transaction
Device(config)# interface port-channel 1
Device(config-if)# load-balancing flow
```

This example shows how to set the load-balancing method to VLAN:

```
Device# config-transaction
Device(config)# interface port-channel 1
Device(config-if)# load-balancing vlan
```

This example shows a configuration where flow-based load balancing is configured on port channel 2 while the VLAN-manual method is configured globally:

```
 port-channel load-balancing vlan-manual
 interface Port-channel2
  ip address 10.0.0.1 255.255.255.0
  load-balancing flow

 interface GigabitEthernet2/1/0
  no ip address
  channel-group 2

 interface GigabitEthernet2/1/1
  no ip address
  channel-group 2
```

This example shows configuration for VLAN when the load balancing is set to default on the global level:

```
port-channel load-balancing vlan-manual


interface Port-channel1
interface Port-channel1.100
 encapsulation dot1Q 100 primary GigabitEthernet 1/1/1
 secondary GigabitEthernet 1/2/1
 ip address 10.16.2.100 255.255.255.0

interface Port-channel1.200
 encapsulation dot1Q 200 primary GigabitEthernet 1/2/1
 ip address 10.16.3.200 255.255.255.0
interface Port-channel1.300
 encapsulation dot1Q 300
 ip address 10.16.4.300 255.255.255.0

interface GigabitEthernet 1/1/1
 no ip address
 channel-group 1!
interface GigabitEthernet 1/2/1
 no ip address
 channel-group 1
```

Note Interface 1 and interface 2 must be member ports of a port channel when **encapsulation dot1q** is configured.

Enable hash algorithms for flow-based load balancing on a global level

Use this procedure to configure a specific hash algorithm for flow-based load balancing globally across all port channels on the device.

Before you begin

Complete these steps to enable hash algorithms for flow-based load balancing on a global level.

Procedure

Configure the desired flow-based hash algorithm globally.

```
port-channel load-balance-hash-algo hash-algo
```

Replace *hash-algo* with one of the following supported hash algorithms:

dst-ip; *dst-macsrc-dst-ipsrc-dst-ipsrc-dst-macsrc-dst-mixed-ip-portsrc-ipsrc-mac*

The selected hash algorithm is now applied globally for flow-based load balancing on all port channels.

This example shows configuration for enabling a hash algorithm on a global level flow-based load balancing:

```
device(config)# port-channel load-balance-hash-algo src-mac
```

Enable hash algorithms flow-based load balancing on an individual port channel interface

Use this procedure to configure a flow-based hash algorithm for load balancing on an individual port channel interface

Before you begin

This feature is supported from Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Manager Release 20.15.1.

Complete these steps to enable flow-based load balancing on an individual port channel interface.

Procedure

Step 1 Enter the port channel interface configuration mode.

```
interface Port-channel
```

Step 2 Enable flow-based load balancing hash algorithm.

```
load-balance-hash-algo hash-algo
```

Replace *hash-algo* with one of the following supported hash algorithms:

dst-ip; *dst-macsrc-dst-ipsrc-dst-ipsrc-dst-macsrc-dst-mixed-ip-portsrc-ipsrc-mac*

The specified port channel interface now uses the configured flow-based load balancing hash algorithm.

This example shows configuration of hash algorithms for flow-based load balancing on an individual port channel interface. When **sdwan** hash algorithm is configured on the transport side, you can enable different hash algorithm options on the service side.

```
device(config)# interface Port-channel 1
device(config-if)# load-balance-hash-algo sdwan
device(config-if)# exit
device(config)# interface Port-channel 2
device(config-if)# load-balance-hash-algo src-dst-mixed-ip-port
device(config-if)# exit
device(config)# interface Port-channel 3
device(config-if)# no shut
device(config-if)# commit
device(config-if)# end
```

Enable VLAN load balancing per port channel on the service side

Use this procedure to configure VLAN-based load balancing on a specific EtherChannel port channel on the service side.

Before you begin

Complete these steps to enable VLAN load balancing per port channel on the service side.

Procedure

Step 1 Enter the port channel interface configuration mode.

```
interface Port-channel channel-number
```

Step 2 Enable vlan on per port channel.

```
load-balancing vlan
```

The specified service side port channel is now configured to use VLAN-based load balancing.

This example shows configuration for VLAN load balancing on the service side, when the flow-based load balancing is set to default on the global level:

```
interface Port-channel channel-number
interface GigabitEthernet slot/subslot/port
 channel-group channel-group-number
 interface GigabitEthernet slot/subslot/port
 channel-group channel-group-number
interface Port-channel channel-number
 load-balancing vlan
interface Port-channel channel-number
 encapsulation dot1Q vlan_id primary interface1 secondaryinterface2
```

Note Interface 1 and interface 2 must be member ports of a port channel when **encapsulation dot1q** is configured.

port-channel load-balancing vlan-manual

Note This command is available for configuration in the global configuration mode, and applies to all the port-channel configured on the device.

This example shows how the load-balancing configuration can be globally applied to define policies for handling traffic by using the **port-channel load-balancing** command.

```
port-channel load-balancing vlan-manual

!
interface Port-channel1
!
interface Port-channel1.100
 encapsulation dot1Q 100 primary GigabitEthernet 1/1/1
 secondary GigabitEthernet 1/2/1
 ip address 10.16.2.100 255.255.255.0
!
interface Port-channel1.200
 encapsulation dot1Q 200 primary GigabitEthernet 1/2/1
 ip address 10.16.3.200 255.255.255.0
!
interface Port-channel1.300
 encapsulation dot1Q 300
 ip address 10.16.4.300 255.255.255.0
 !
interface GigabitEthernet 1/1/1
 no ip address
 channel-group 1!
interface GigabitEthernet 1/2/1
 no ip address
 channel-group 1
```

Configure load balancing for EtherChannels on the service side using CLI commands

Use this procedure to configure load balancing for EtherChannels on the service side of your Cisco IOS XE Catalyst SD-WAN devices, ensuring efficient traffic distribution across bundled links.

Load balancing optimizes the use of aggregated bandwidth provided by EtherChannels and enhances network performance. You can choose between flow-based or VLAN-based methods and apply configurations globally or on individual port channels, depending on your network requirements.

Before you begin

Complete these steps to configure load balancing for EtherChannels on the service side using CLI commands.

Procedure

Decide on the load balancing method you want to implement, flow-based or VLAN-based:

For flow-based:

- To configure load balancing on a global level or per port channel, seee Enable load balancing on an individual port channel, on page 440.
- To enable a specific hash algorithm for flow-based load balancing across all port channels, see Enable hash algorithms for flow-based load balancing on a global level, on page 442.
- To enable a specific flow-based hash algorithm on an individual port channel interface, see Enable hash algorithms flow-based load balancing on an individual port channel interface, on page 442.

For VLAN-based:

If you choose VLAN-based load balancing, configure it per port channel, see Enable VLAN load balancing per port channel on the service side, on page 443.

Load balancing is now configured for your service side EtherChannels according to your chosen method.

What to do next

Verify your load balancing configuration using the show etherchannel load-balancing command.

Configure a service-side port channel and member link interface using configuration groups

Use this procedure to configure EtherChannel port channels and their member links on the service side using configuration groups within Cisco Catalyst SD-WAN Manager.

Before you begin

Complete these steps to configure a service-side port channel and member link interface using configuration groups in Cisco Catalyst SD-WAN Manager.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Under **Service Profile**, click **Add New** to add a new service profile or select any existing service profiles, and click **Edit**.

Step 3 Select +, and click on the **Ethernet Interface** to add a new interface.

See Ethernet Interface for more details.

Step 4 Select **Add New** from the Ethernet Interface drop-down menu.

Step 5 Under **Basic Configurations**, enter the interface name and description.

Step 6 Click **Ether Channel**, and assign the EtherChannel to a **member interface** or a **port channel** interface from the drop down menu.

Note
If you configure the EtherChannel interface as a port channel, then the default port is LACP. You can assign a different port channel mode using the **Port Channel Mode** option from Cisco SD-WAN Manager.

Note
You can create multiple interfaces which can be either member or port channel interfaces.

Step 7 Click **Save**.

Step 8 Click **Configuration** tab, and deploy the newly created port channels.

A service-side port channel and its member links are configured using configuration groups, ready for deployment to your devices.

What to do next

Monitor the status of the deployed EtherChannels and verify traffic flow on the service side. For more information, see Monitor configured EtherChannel using CLI, on page 454.

EtherChannels on the transport side

EtherChannels on the transport side is a capability that

- extends EtherChannel functionality to the transport-facing interfaces of Cisco IOS XE Catalyst SD-WAN devices
- enables advanced network services like load balancing for aggregated links.
- is configurable through CLI device templates, CLI add-on feature templates, and configuration groups.

Supported devices for transport side EtherChannel

This section provides a comprehensive list of Cisco platforms that support EtherChannel functionality on the transport side. This information is crucial for planning and deploying Cisco Catalyst SD-WAN solutions that leverage EtherChannels for enhanced connectivity and resilience on transport-facing interfaces. It also indicates which platforms support load balancing for these EtherChannels.

The following platforms support EtherChannels, and also offer load balancing for EtherChannels on the service side:

- Cisco 4000 Series Integrated Services Routers
  - Cisco 4461 Integrated Services Router
- Cisco ASR 1000 Series Aggregation Services Routers
  - Cisco ASR 1001-HX Router
  - Cisco ASR 1002-HX Router
- Cisco Catalyst 8200 Series Edge Routers
- Cisco Catalyst 8300 Series Routers
- Cisco Catalyst 8500 Series Edge Routers

Note Starting with Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, the load balancing configuration command **portchannel load-balance-hash-algo sdwan** is supported only on the Cisco 4461 Integrated Services Router and Cisco Catalyst 8300 Series routers.

Prerequisites for EtherChannels on the transport side

Before configuring EtherChannels on the transport side, ensure that the following prerequisties are met. These prerequisites are essential for your EtherChannel configuration.

- All the member links in each EtherChannel must be of the same speed.
- All the member links must be configured on Layer 3 transport side ports.
- All member interfaces in a portchannel must have the same speed and duplex, when using platforms that support multiple rate SFPs on the same port.

Restrictions for EtherChannels on the transport side

Maximum port channel interfaces

The maximum number of port channel interfaces that a device can support varies depending on the particular model of the device.

Port channel configuration

You can configure EtherChannels on a device by using the CLI, or using only the CLI templates or CLI add-on feature templates in Cisco SD-WAN Manager.

Hardware and platform compatibility

- Network Interface Modules (NIMs) with L2 ports do not support EtherChannels on the transport side.
- The use of port channel on virtual devices such as Cisco Catalyst 8000V is not supported.
- Platforms such as the Cisco Catalyst 8500 Series Edge Routers support multi-rate interfaces, allowing 1G SFP modules to be used in default 10G interfaces. Despite this, in the output of show commands, the interfaces appear as TenGigabitEthernet x/x/x. You can bundle the 1G SFP interfaces together to form a port channel.

Deployment

- In a deployment involving an EtherChannel Link Aggregation Group (LAG) from a Cisco IOS XE Catalyst SD-WAN device to a multichassis LAG (MC-LAG) between two upstream paths, SLA-based Application-Aware Routing (AAR) forwarding can be inaccurate if the traffic load on the two upstream paths is not symmetric.
- Cisco IOS XE Catalyst SD-WAN Release 17.13.1a does not include support for an endpoint tracker on port-channel TLOCs.

Configure a transport side EtherChannels using a CLI template

Use this procedure to create a logical EtherChannel interface on the transport side of a Cisco IOS XE Catalyst SD-WAN device, bundling multiple physical links for increased bandwidth and redundancy.

This procedure describes how to configure EtherChannels on the transport side using CLI templates in Cisco SD-WAN Manager.

In Cisco SD-WAN Manager, you can configure EtherChannels on the transport side using CLI templates.

For more information about using CLI templates, see CLI add-on feature templates and CLI templates for Cisco IOS XE Catalyst SD-WAN devices.

.

Note By default, CLI templates execute commands in global config mode.

Before you begin

Complete these steps to configure a transport side EtherChannel using a CLI template.

Procedure

Step 1 Configure a Layer 3 port channel.

```
interface Port-channel channel-number
ip address ip-address mask
ipv6 address ipv6-address/prefix-length
```

Step 2 Assign Interfaces to a Layer 3 port channel with LACP active or passive options.

a.

```
interface GigabitEthernet slot/subslot/port
no ip address
channel-group channel-group-number mode {active passive}
exit
```

b. Configure EtherChannel with LACP Paramaters.

```
lacp system-priority priority
interface GigabitEthernet slot/subslot/port
lacp port-priority priority
```

c. Configure a static EtherChannel.

```
interface GigabitEthernet slot/subslot/port
no ip address
channel-group channel-group-number
```

Step 3 Configure tunnels.

```
interface Tunnel tunnel-number
ip unnumbered Port-channel channel-group-number
no ip redirects
tunnel source  Port-channel channel-group-number
tunnel mode sdwan

sdwan
 interface Port-channel channel-group-number
  tunnel-interface
   encapsulation {ipsec gre}
   color color-type
```

This example shows how to configure a Layer 3 EtherChannel, and how to assign two ports to channel 1 with the LACP mode as active and passive:

```
interface Port-channel1
ip address 10.48.48.15 255.255.255.0
ip ospf priority 0
ip ospf 65535 area 51
load-interval 30
no negotiation auto

interface GigabitEthernet0/0/0
no ip address
negotiation auto
lacp rate fast
channel-group 1 mode active
end

interface GigabitEthernet0/0/4
no ip address
negotiation auto
lacp rate fast
channel-group 1 mode passive
end
```

The following is a configuration example for creating an EtherChannel on the transport side.

```
interface Tunnel2
ip unnumbered Port-channel1
tunnel source Port-channel1
tunnel mode sdwan

interface Port-channel1
  tunnel-interface
   encapsulation ipsec
   color lte
```

A transport side EtherChannel is configured and operational, providing aggregated bandwidth and redundancy for your Cisco Catalyst SD-WAN transport connections.

What to do next

Verify the EtherChannel status using CLI commands like **show etherchannel summary** and **show etherchannel load-balancing**.

Configure load balancing for EtherChannels on the Transport Side using CLI Commands

Enable load balancing on individual portchannel interface

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1

Note We recommend using this method to configure load balancing for EtherChannels on the transport side.

1. Enter the port channel interface configuration mode.

   interface Portchannel *channel number*

2. Enable load balancing on an individual port channel.

   load-balance-hash-algo sdwan

Enable load balancing globally for EtherChannels on the Transport Side

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

For more information about using CLI templates, see CLI add-on feature templates and CLI templates for Cisco IOS XE Catalyst SD-WAN devices.

Enable load balancing globally for EtherChannels on the transport side.

```
port-channel load-balance-hash-algo sdwan
```

Note In this command, **port-channel load-balance-hash-algo sdwan**, the **sdwan** option was added in Cisco IOS XE Catalyst SD-WAN Release 17.14.1a.

Enable hash algorithms globally for EtherChannels on the Transport Side

1. Configure the algorithm used for load balancing.

   To configure load balancing for IPv4 addresses, which is the default setting, use the following configuration:

   ```
   sdwan
   ip load-sharing algorithm {src-dst-ip|ip-and-ports|src-ip-only}
   ```

   To configure load balancing for IPv6 addresses, use the following configuration:

   ```
   sdwan
   ipv6 load-sharing algorithm {src-dst-ip|ip-and-ports|src-ip-only}
   ```

   - **src-dst-ip**: Balances traffic based on both source and destination IP addresses.
   - **ip-and-ports**: Balances traffic using a combination of IP addresses and port numbers.
   - **src-ip-only**: Balances traffic based solely on the source IP address.

The **ip load-sharing algorithm** command is a global configuration that applies to all Cisco Catalyst SD-WAN tunnels. Changing the algorithm with options such as **src-dst-ip** or **src-dst-mixed-ip-port** affects the load-sharing mechanism for other Cisco Catalyst SD-WAN tunnel traffic as well.

When you configure a port channel on both the service side and the transport side, using the **port-channel load-balance-hash-algo sdwan** command applies load balancing to the transport side. For the Service side, the port channel defaults to the **src-dst-ip** load balancing mode.

To change the load-balancing algorithm for the Service side when a Transport-VPN port-channel is also configured, use the **port-channel load-balance-hash-algo** command. This command allow you to switch from the default **sdwan** mode to alternative modes such as **dst-ip**, **dst-mac**, **src-dst-ip**, **src-dst-mac**, **src-dst-mixed-ip-port**, **src-ip**, or **src-mac**. However, this change disables the SD-WAN-based load balancing for the transport side.

Here's the complete configuration for enabling load balancing and apply the desired hash algorithm for traffic distribution on the transport side of Cisco IOS XE Catalyst SD-WAN devices.

```
port-channel load-balance-hash-algo sdwan
sdwan
 ip load-sharing algorithm src-dst-ip

port-channel load-balance-hash-algo sdwan
sdwan
 ipv6 load-sharing algorithm src-dst-ip
```

This example shows configuration enabling load balancing for each port channel interface. When **sdwan** hash algorithm is configured on the transport side, you can enable different hash algorithm options on the service side.

```
device(config)# interface Port-channel 1
device(config-if)# load-balance-hash-algo sdwan
device(config-if)# exit

device(config)# interface Port-channel 2
device(config-if)# load-balance-hash-algo src-dst-mixed-ip-port
device(config-if)# exit

device(config)# interface Port-channel 3
device(config-if)# no shut
device(config-if)# commit
device(config-if)# end
```

The following is a sample output to view the configuration for per-interface port channel using **show etherchannel load-balancing** command.

```
device# show etherchannel load-balancing
flow-based
LB Algo type: Source Destination IP

 Port-Channel:                      LB Method
    Port-channel1                 :  flow-based (SDWAN Inner packet LB)
    Port-channel2                 :  flow-based (Source Destination Port, IP addr)
    Port-channel3                 :  flow-based (Source Destination IP)
```

Enable load balancing on individual portchannel interface on the transport side

Use this procedure to enable load balancing on a specific EtherChannel port channel interface on the transport side.

This method is recommended for configuring load balancing on the transport side, providing granular control over traffic distribution for individual port channels. This feature is supported from Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Manager Release 20.15.1.

Before you begin

An EtherChannel port channel must already be configured on the transport side.

Complete these steps to enable load balancing on an individual port channel interface.

Procedure

Step 1 Enter the port channel interface configuration mode.

interface Portchannel *channel number*

Replace *channel number* with the number of your port channel.

Step 2 Enable load balancing on an individual port channel.

load-balance-hash-algo sdwan

The specified transport side port channel interface is now configured for SD-WAN load balancing.

What to do next

Verify the individual port channel load balancing configuration using the **show etherchannel load-balancing** command.

Enable load balancing globally for EtherChannels on the transport side

Use this procedure to enable load balancing globally for all EtherChannels on the transport side of your device.

This configuration applies a default load balancing method to all transport side EtherChannels for which no individual load balancing method is explicitly configured. This feature is supported from Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1.

Before you begin

Complete these steps to enable load balancing globally for EtherChannels on the transport side.

Procedure

Enable load balancing globally for EtherChannels on the transport side.

```
port-channel load-balance-hash-algo sdwan
```

SD-WAN load balancing is now enabled globally for transport side EtherChannels.

What to do next

Verify the global load balancing configuration using the **show etherchannel load-balancing** command.

Enable hash algorithms globally for EtherChannels on the transport side

Use this procedure to configure specific hash algorithms for IP and IPv6 load balancing globally for EtherChannels on the transport side.

This global configuration applies to all Cisco Catalyst SD-WAN tunnels. Changing these algorithms affects the load-sharing mechanism for other SD-WAN tunnel traffic as well. This feature is supported from Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1.

Before you begin

Complete these steps to enable hash algorithms globally for EtherChannels on the transport side.

Procedure

Configure the algorithm used for load balancing.

- To configure load balancing for IPv4 addresses, which is the default setting, use the following configuration:

  ```
  sdwan
  ip load-sharing algorithm {src-dst-ip|ip-and-ports|src-ip-only}
  ```

  - **src-dst-ip**: Balances traffic based on both source and destination IP addresses.
  - **ip-and-ports**: Balances traffic using a combination of IP addresses and port numbers.
  - **src-ip-only**: Balances traffic based solely on the source IP address.

- To configure load balancing for IPv6 addresses, use the following configuration:

  ```
  sdwan
  ipv6 load-sharing algorithm {src-dst-ip|ip-and-ports|src-ip-only}
  ```

  The options are the same as for IPv4 load balancing.

The **ip load-sharing algorithm** command is a global configuration that applies to all Cisco Catalyst SD-WAN tunnels. Changing the algorithm with options such as **src-dst-ip** or **src-dst-mixed-ip-port** affects the load-sharing mechanism for other Cisco Catalyst SD-WAN tunnel traffic as well.

When you configure a port channel on both the service side and the transport side, using the **port-channel load-balance-hash-algo sdwan** command applies load balancing to the transport side. For the Service side, the port channel defaults to the **src-dst-ip** load balancing mode.

To change the load-balancing algorithm for the Service side when a Transport-VPN port-channel is also configured, use the **port-channel load-balance-hash-algo** command. This command allow you to switch from the default **sdwan** mode to alternative modes such as **dst-ip**, **dst-mac**, **src-dst-ip**, **src-dst-mac**, **src-dst-mixed-ip-port**, **src-ip**, or **src-mac**. However, this change disables the SD-WAN-based load balancing for the transport side.

Here's the complete configuration for enabling load balancing and apply the desired hash algorithm for traffic distribution on the transport side of Cisco IOS XE Catalyst SD-WAN devices.

```
port-channel load-balance-hash-algo sdwan
sdwan
```

```
 ip load-sharing algorithm src-dst-ip

port-channel load-balance-hash-algo sdwan
sdwan
 ipv6 load-sharing algorithm src-dst-ip
```

This example shows configuration enabling load balancing for each port channel interface. When **sdwan** hash algorithm is configured on the transport side, you can enable different hash algorithm options on the service side.

```
device(config)# interface Port-channel 1
device(config-if)# load-balance-hash-algo sdwan
device(config-if)# exit

device(config)# interface Port-channel 2
device(config-if)# load-balance-hash-algo src-dst-mixed-ip-port
device(config-if)# exit

device(config)# interface Port-channel 3
device(config-if)# no shut
device(config-if)# commit
device(config-if)# end
```

The following is a sample output to view the configuration for per-interface port channel using **show etherchannel load-balancing** command.

```
device# show etherchannel load-balancing
flow-based
LB Algo type: Source Destination IP

 Port-Channel:                       LB Method
    Port-channel1                   :  flow-based (SDWAN Inner packet LB)
    Port-channel2                   :  flow-based (Source Destination Port, IP addr)
    Port-channel3                   :  flow-based (Source Destination IP)
```

The specified IPv4 and IPv6 load-sharing algorithms are now applied globally for transport side EtherChannels.

What to do next

Verify the global load balancing configuration using the **show etherchannel load-balancing** command.

Monitor configured EtherChannel using CLI

This section provides CLI commands and their sample outputs for monitoring the status and configuration of EtherChannels. These commands allow you to verify the operational state, member links, and load balancing methods applied to your EtherChannels.

View EtherChannel summary

Use the **show etherchannel summary** command to display a summary of each configured channel group.

```
Device# show etherchannel summary

Flags:  D - down        P/bndl - bundled in port-channel
        I - stand-alone s/susp - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
```

```
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1       Po1(RU)         LACP     Te0/3/0(bndl) Te0/3/1(hot-sby)

RU - L3 port-channel UP State
SU - L2 port-channel UP state
P/bndl -  Bundled
S/susp  - Suspended
```

View EtherChannel load balancing configuration

Use the **show etherchannel load-balancing** command to display the load-balancing method applied to each port channel.

```
Device# show etherchannel load-balancing

EtherChannel Load-Balancing Method:
Global LB Method: flow-based
LB Algo type: SDWAN Inner packet LB

 Port-Channel:                       LB Method
    Port-channel1                   :  flow-based (SDWAN Inner packet LB)
```

Aggregate EtherChannel Quality of Service

The Aggregate EtherChannel Quality of Service (QoS) is a EtherChannel-related feature that

- improves quality of service on a port channel main interface or subinterface,
- effectively manages network parameters such as delay, jitter, bandwidth, and packet loss, and
- allows the application of an aggregate egress-queuing policy-map on the main or sub-interface of a port channel.

The Aggregate EtherChannel QoS facilitates QoS support on the aggregate port channel's main interface on Cisco IOS XE Catalyst SD-WAN device.

Prerequisites for Aggregate EtherChannel Quality of Service

- Identify aggregate port channel interfaces before creating them using the **platform qos port-channel-aggregate** command.
- In a port channel, all member links must be of the same speed.

Restrictions for Aggregate EtherChannel Quality of Service

Aggregate port channel member and interface limits

The aggregate port channel can support four member links and eight aggregate port channel interfaces.

QoS policy application restrictions on aggregate port channels

You can apply a policy map to the aggregate a port channel's main interface or sub-interface only. Member link QoS is not supported.

Limitations of aggregate port channel conversion

You cannot spontaneously convert port channels to and from the aggregate status. You must delete the interface port-channel from the configurations before adding or removing the matching **platform qos port-channel-aggregate** command.

Unsupported QoS applications on port channel member links

QoS applications which are used to manage, prioritize and control the behavior of data transmission over a network are not supported on port channel member links.

QoS policies applied to aggregate port channel main interfaces and port channel sub-interfaces are not supported.

Channel group modification process with aggregate QoS enabled

When you enable aggregate QoS, it is not possible to directly modify a channel group on a member link. To make changes, the old channel group needs to be removed and the new one must be added. First push one template to remove the old member link and port channel configuration, then another template to add the new configuration.

Configure Aggregate EtherChannel Quality of Service using CLI Template

Configure aggregate EtherChannel Quality of Service using a CLI template.

In SD-WAN Manager, you can configure aggregate EtherChannel QoS using the CLI templates to manage bandwidth and prioritize traffic across bundled links.

Before you begin

For more informationabout using CLI templates, see CLI add-on feature templates and CLI templates for Cisco IOS XE Catalyst SD-WAN devices.

Note By default, CLI templates execute commands in global config mode.

Follow these steps to configure aggregate EtherChannel QoS using a CLI template.

Procedure

Step 1 Create the aggregated port channel.

```
platform qos port-channel-aggregate port-channel-number
 interface Port-channel channel-number
 no shutdown
 ip address ip-address mask
```

Step 2 Assign member links to port channel.

```
 interface GigabitEthernet slot/subslot/port
  no negotiation auto
  channel-group channel-group-number mode {active passive}
  exit
```

Step 3 Configure tunnels.

```
 interface Tunnel tunnel-number
  no shutdown
  ip unnumbered port-channel-interface
  tunnel source port-channel-interface
  tunnel mode sdwan

 sdwan
  interfacechannel-group-number
   tunnel-interface
    encapsulation ipsec
    color public-internet
```

Step 4 Configure QoS.

```
 interface channel-group-number
  service-policy output pre-defined qos policy-map
```

Here's the complete configuration example for configuring aggregate EtherChannel QoS.

```
!
class-map match-any Best-Effort
 match qos-group 2
!
class-map match-any Bulk
 match qos-group 3
!
class-map match-any Business
 match qos-group 1
!
class-map match-any Critical
 match qos-group 0
!
policy-map qos_template
 class Critical
  police rate percent 15
  !
  priority level 1
```

```
 !
 class Business
  bandwidth remaining percent 55
 !
 class Best-Effort
  bandwidth remaining percent 10
 !
 class Bulk
  bandwidth remaining percent 20
 !
!
policy-map shape_Port-channel1
 class class-default
  service-policy qos_template
  shape average 100000000
 !
!
interface TenGigabitEthernet0/1/6
 no shutdown
 no negotiation auto
 channel-group 1 mode active
 lacp rate fast
exit
interface TenGigabitEthernet0/1/7
 no shutdown
 no negotiation auto
 channel-group 1 mode active
 lacp rate fast
exit
interface Port-channel1
 no shutdown
 ip address 10.1.15.15 255.255.255.0
 ipv6 nd ra suppress all
 service-policy output shape_Port-channel1
exit
interface Tunnel1
 no shutdown
 ip unnumbered Port-channel1
 tunnel source Port-channel1
 tunnel mode sdwan
exit
!
sdwan
 interface Port-channel1
  tunnel-interface
   encapsulation ipsec
   color lte
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   no allow-service snmp
   no allow-service bfd
  exit
 exit
```

What to do next

Verify aggregate EtherChannel QoS.

Verify Aggregate EtherChannel Quality of Service

To view QoS issues on a port channel interface, use the **show policy-map interface Port-channel** command.

```
Device# show policy-map interface Port-channel 1
Port-channel1

  Service-policy output: shape_Port-channel1

    Class-map: class-default (match-any)
      121 packets, 20797 bytes
      5 minute offered rate 2000 bps, drop rate 0000 bps
      Match: any
      Queueing
      queue limit 416 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 121/20797
      shape (average) cir 100000000, bc 400000, be 400000
      target shape rate 100000000

      Service-policy : qos_template

        queue stats for all priority classes:
          Queueing
          priority level 1
          queue limit 512 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 121/20797

        Class-map: Critical (match-any)
          121 packets, 20797 bytes
          5 minute offered rate 2000 bps, drop rate 0000 bps
          Match: qos-group 0
          police:
              rate 15 %
              rate 15000000 bps, burst 468750 bytes
            conformed 121 packets, 20797 bytes; actions:
              transmit
            exceeded 0 packets, 0 bytes; actions:
              drop
            conformed 2000 bps, exceeded 0000 bps
          Priority: Strict, b/w exceed drops: 0

          Priority Level: 1

        Class-map: Business (match-any)
          0 packets, 0 bytes
          5 minute offered rate 0000 bps, drop rate 0000 bps
          Match: qos-group 1
          Queueing
          queue limit 416 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          bandwidth remaining 55%

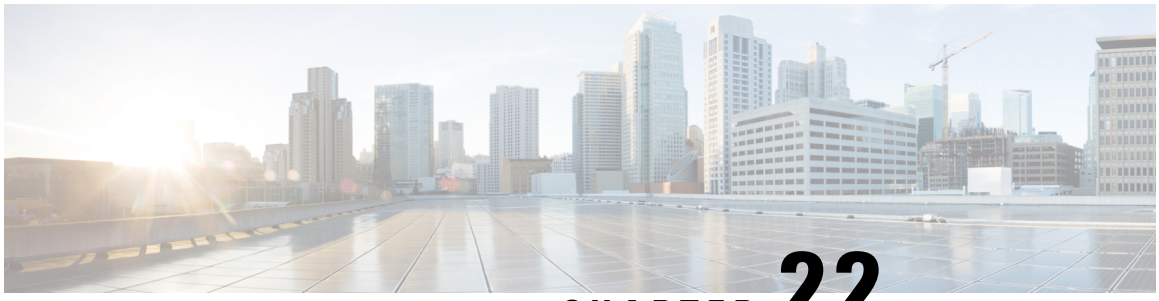
        Class-map: Best-Effort (match-any)
          0 packets, 0 bytes
          5 minute offered rate 0000 bps, drop rate 0000 bps
          Match: qos-group 2
```

```
  Queueing
  queue limit 416 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 0/0
  bandwidth remaining 10%

Class-map: Bulk (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: qos-group 3
  Queueing
  queue limit 416 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 0/0
  bandwidth remaining 20%

Class-map: class-default (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: any

  queue limit 416 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 0/0
```



CHAPTER 22

Network Interfaces

• Network Interfaces, on page 461

Network Interfaces

A network interface in Cisco Catalyst SD-WAN is a network component that,

- is associated with a VPN, and
- is configured and enabled within that VPN.

Each interface can be present only in a single VPN. Create VPN feature templates to configure VPN parameters, and then create interface feature templates to configure the interfaces in the VPN.

Interface operational requirements

For an interface to be operational, you must configure an IP address for the interface and mark it as operational (no shutdown). In practice, you always configure additional parameters for each interface.

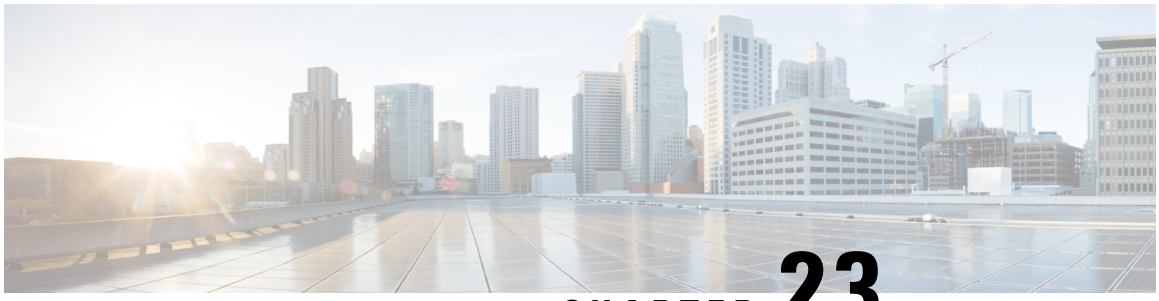
You can configure up to 512 interfaces on a Cisco IOS XE Catalyst SD-WAN device. This number includes physical interfaces, loopback interfaces, and subinterfaces.

Configure each network interface on a device with a unique IP address.

Note To maximize the efficiency of the load-balancing among Cisco SD-WAN Controllers, use sequential numbers when assigning system IP addresses to the Cisco IOS XE Catalyst SD-WAN devices in the domain. Example of a sequential numbering schemes is 172.16.1.1, 172.16.1.2, 172.16.1.3, and so on.

If you try to configure an interface or sub-interface beyond the supported limit, the device generates a notification to Cisco SD-WAN Manager.

Network Interfaces



CHAPTER 23

Bandwidth Utilization Reference Values

- Feature history for bandwidth utilization Reference Values, on page 463
- Bandwidth Utilization Reference Values , on page 463
- Generating Notifications, on page 464
- Monitoring Bandwidth Utilization with Interface Charts , on page 464
- Restrictions for bandwidth utilization reference values, on page 465
- Configure bandwidth utilization reference values , on page 465
- Monitor bandwidth utilization events, on page 467
- Verify bandwidth utilization reference values, on page 467

Feature history for bandwidth utilization Reference Values

Table 145: Feature History

Feature Name	Release Information	Description
Upstream and Downstream Bandwidth Reference Values	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	Use the upstream and downstream bandwidth reference values to govern how Cisco SD-WAN Manager displays interface utilization percentages in charts. The values also act as configurable thresholds that trigger interface-bw events when a network interface's utilization exceeds a defined point.

Bandwidth Utilization Reference Values

A bandwidth utilization reference value is a configurable parameter that

- specifies the upstream (egress) bandwidth and downstream (ingress) bandwidth for each interface, and
- acts as a reference for calculating bandwidth utilization and generating notifications.

You can configure bandwidth utilization reference values for each interface. Cisco SD-WAN Manager uses these reference values to display bandwidth utilization percentages in charts.

Generating Notifications

To receive notifications when the traffic bandwidth exceeds 85% utilization, configure reference values for both upstream (transmitted) and downstream (received) traffic. These values act as thresholds for generating the interface bandwidth events. The range is from 1 and 2,147,483,647 kbps.

The device samples the interface traffic each 10 seconds. If the received or transmitted bandwidth exceeds 85 percent of the configured value in 85 percent of the sampled intervals in a continuous 5-minute period, the device generates an SNMP trap. After the first trap is generated, sampling continues at the same frequency, but notifications are rate-limited to once per hour. A second trap is sent, and subsequent traps are sent, if the bandwidth exceeds 85 percent of the value in 85 percent of the 10-second sampling intervals over the next 1-hour period. If, after 1 hour, the device does not send another SNMP trap, the notification interval reverts to 5 minutes.

The upstream bandwidth and downstream bandwidth settings are solely for monitoring purposes and do not impose a bandwidth limit on the traffic. For example, in some network configurations, the full bandwidth of an interface may not be available. To ensure that utilization values reflect the available network bandwidth, set bandwidth utilization reference values lower than an interface's full speed.

You can verify the configured upstream and downstream bandwidth values using the **show interface detail** command, which displays the upstream bandwidth (tx-kbps) and downstream bandwidth (rx-kbps) fields usage.

You can monitor transport circuit bandwidth on Cisco IOS XE Catalyst SD-WAN devices and on Cisco SD-WAN Manager.

Monitoring Bandwidth Utilization with Interface Charts

Cisco SD-WAN Manager provides a chart showing bandwidth utilization for each interface of a device. To view the chart, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**, click a device and click **Interface**.

Configuring upstream or downstream reference values affects how the chart displays the percentages:

- No bandwidth utilization reference values configured: By default, devices calculate the bandwidth utilization value according to the interface speed of the connection.
- Bandwidth utilization reference values configured: If you configure bandwidth utilization reference values, devices calculate the bandwidth utilization value as a percentage of the reference point.

  For example, if you configure upstream bandwidth and downstream bandwidth values of 500 megabits per second, and if the downstream utilization is 500 megabits per second, the device reports downstream utilization as 100%.

Devices limit the calculated utilization value to 100% even if the traffic utilization is more than 100% of the configured reference value.

Restrictions for bandwidth utilization reference values

- Cisco SD-WAN Manager supports bandwidth data rate and utilization statistics only for a primary network interface, not a subinterface or loopback interface. You can still configure upstream and downstream bandwidth under a subinterface or loopback interface as a reference value or for per-tunnel QoS functionality.
- Configure upstream and downstream bandwidth references for service-side VPN interfaces using only a CLI template.

Configure bandwidth utilization reference values

Use one of these methods to configure bandwidth utilization reference values:

- Configuration group
- CLI commands
- Feature template

Configure bandwidth utilization reference values using a configuration group

Follow these steps to configure bandwidth utilization reference values using a configuration group

Before you begin

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.16.1a and Cisco Catalyst SD-WAN Manager Release 20.16.1

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Under Transport & Management Profile, click **...** adjacent to the transport profile, and choose **Edit**.

Step 3 Click the edit icon adjacent to Ethernet Interface.

Step 4 In the **Basic Configuration** section, enter the upstream and downstream bandwidth reference values.

Step 5 Click **Save**.

Configure bandwidth utilization reference values using CLI commands

This section provides example CLI configurations to configure upstream and downstream bandwidth reference values in Cisco SD-WAN Manager. For more information about using CLI templates, see *CLI Add-On Feature Templates* and *CLI Templates*.

By default, CLI templates execute commands in global config mode.

Procedure

Step 1 Enter the SD-WAN configuration mode.

Example:

```
sdwan
```

Step 2 Enter interface configuration mode.

Example:

```
interface interface-name
```

Step 3 Define the upstream or downstream bandwidth reference value in kbps.

Example:

```
bandwidth-upstream upstream-value
bandwidth-downstream downstream-value
```

Here is a complete configuration example for configuring upstream and downstream bandwidth reference values:

```
sdwan
!
interface GigabitEthernet1
bandwidth-upstream 10000
bandwidth-downstream 10000
```

Configure bandwidth utilization reference values using templates

Follow these steps to configure bandwidth utilization reference values using feature templates.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**.

Step 3 Do one of these:

- Click **Add Template**, choose a device, and create a Cisco VPN Interface Ethernet template.
- Edit an existing Cisco VPN Interface Ethernet template.

Step 4 In the **Basic Configuration** section, enter the upstream and downstream bandwidth reference values.

Step 5 Click **Update** to save the template.

Monitor bandwidth utilization events

Follow these steps to monitor upstream and downstream bandwidth events using the Cisco SD-WAN Manager.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **Events**.

Step 2 View the details of upstream and downstream bandwidth values in the device configuration section. The default name for interface bandwidth-related events is **interface-bw**.

Monitor bandwidth utilization reference values

Follow these steps to monitor bandwidth utilization reference values using Cisco SD-WAN Manager.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

Step 2 Click the **Device** tab.

Step 3 Click the hostname of the device you want to monitor.

Step 4 From the **Applications** section, choose **Interface**.

Step 5 Click the **Chart Options** drop-down list and choose **Utilization**.

Step 6 Hover over the real-time or historical data points to view the utilization percentage.

Verify bandwidth utilization reference values

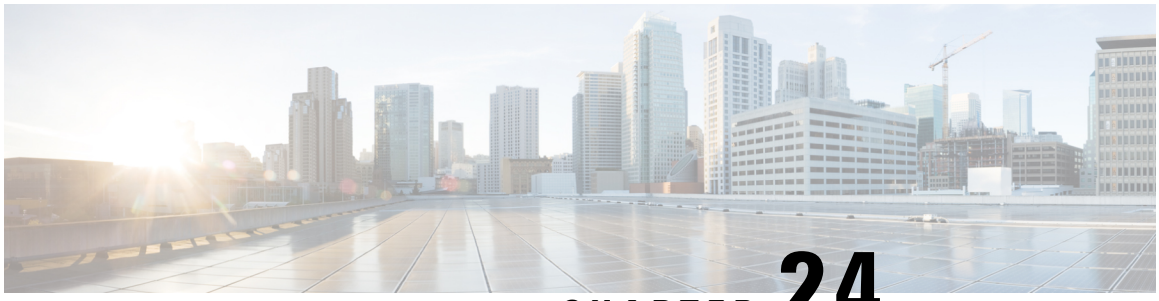
Monitor interface alarms

Use the **show platform software sdwan interface-alarm summary** command to display the bandwidth reference values for an interface in the alarm summary. This sample output shows the summary details of a GigabitEthernet interface alarm.

See Interface Alarm Summary, and Base and High Intervals for more information.

```
device# show platform software sdwan interface-alarm summary

============ Interface Alarm Summary ============
Interface Name      Upstream (kbps)  Downstream (kbps)   Base Interval(s)   High Interval(s)
GigabitEthernet1      10000               10000              300                3600
```



CHAPTER 24

Loopback Interfaces

- Feature history for loopback interfaces, on page 469
- Loopback interfaces, on page 470
- Implicit ACLs on loopback interfaces, on page 470
- Loopback TLOC interface bound to a physical WAN interface, on page 470
- Loopback TLOC interface not bound to a physical WAN interface, on page 471
- Bind mode and unbind mode, on page 471
- Configure implicit ACL on loopback interfaces using CLI commands, on page 472
- Examples of implicit ACL configurations on loopback interfaces, on page 473
- Verify implicit ACL configurations on loopback interfaces, on page 474

Feature history for loopback interfaces

Table 146: Feature History

Feature Name	Release Information	Description
Implicit ACL on Loopback Interfaces	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	When a loopback TLOC interface has its own implicit ACL, ACL rules are applied on the traffic destined for the interface. With implicit ACL enabled on the loopback TLOC interface, only limited services can be allowed, thereby enhancing your network security. When a loopback TLOC interface is bound to a physical interface on a Cisco IOS XE Catalyst SD-WAN device, the physical interface is treated like a physical TLOC interface.

Loopback interfaces

A loopback interface is a network interface that

- enables data traffic exchange across private WANs such as MPLS or metro Ethernet networks,
- allows routers behind private networks to communicate directly with other edge routers over the private WAN, and
- is configured as a tunnel interface instead of using a physical WAN interface.

Implicit ACLs on loopback interfaces

Implicit ACLs on loopback interfaces are access control mechanism that

- consist of default rules applied to traffic destined for loopback interfaces,
- can be present by default or enabled through configuration to limit or permit traffic, and
- is applied to traffic destined for loopback interfaces configured with a Transport Location (TLOC) in both bind mode (bound to a physical interface) and unbind mode (not bound to any physical interface) on Cisco IOS XE Catalyst SD-WAN devices.

Benefits

Implicit ACL on a loopback TLOC interface protects against denial of service (DoS) attacks by allowing only limited services. This enhances your network security.

Loopback TLOC interface bound to a physical WAN interface

When a loopback interface is a TLOC and is bound to a physical WAN interface, the corresponding implicit ACL rules are applied based on where the traffic is destined:

- If the traffic that is destined to the loopback TLOC interface is received on a physical WAN interface, the implicit ACL rules configured on the loopback TLOC interface is applied.
- If the traffic is not destined for the loopback TLOC interface, depending on whether the physical WAN interface is configured for TLOC or not, the following rules apply:
  - If the physical WAN interface is not configured with a TLOC, then routing decisions apply.
  - Forwarded or passthrough packets are dropped when a loopback TLOC interface is bound to a physical WAN interface—the same behavior as when a physical interface is configured as a TLOC. Therefore, an explicit ACL must be configured on the bound physical interface to forward packets.
- An explicit ACL is necessary to allow passthrough packets in the following sample scenarios:
  - Branch edge routers accessing controllers hosted in on-premises data centers: This scenario presumes that the branch edge routers access the controllers through the data center hub, which is configured with a loopback interface bound to a physical WAN interface.

- Branch routers accessing cloud-hosted controllers through data center internet circuits: This scenario presumes that the branch routers are connected to the data center edge using an MPLS network. Such branch routers then access the cloud-hosted controllers through the data canter edge router, which is configured with a loopback interface bound to a physical WAN interface.

- If a physical WAN interface is configured with TLOC, implicit ACL rules of the physical TLOC interface apply. In both these scenarios explicit ACLs on the bound physical WAN interface are necessary to allow passthrough traffic.



Note When a loopback interface with a public IP address is configured as a TLOC and bound to a NAT-enabled physical WAN interface, DIA forwarding works. However, strict color-based exit selection using centralized data policy local-tloc or local-tloc-list is not supported if the bound physical WAN interface is not itself configured as a TLOC.

Loopback TLOC interface not bound to a physical WAN interface

When a loopback interface is a TLOC, and is not bound to a physical WAN interface, implicit ACL rules are applied based on where the traffic is destined for:

- If the traffic that is destined for the loopback TLOC interface is received on a physical WAN interface, implicit ACL rules of the loopback TLOC are applied.
- If the traffic is not destined for the loopback TLOC interface, depending on whether the input physical WAN interface is configured for TLOC or not, the following rules apply:
  - If the physical WAN interface is not configured for TLOC, then routing decisions apply.
  - If the physical WAN interface is configured for TLOC, the configured implicit ACL rules apply.

Bind mode and unbind mode

The difference between the bind mode and the unbind mode for loopback TLOC is that in a bind mode the passthrough traffic is dropped because the bound physical interface is treated as a TLOC by itself. In an unbind mode, the passthrough traffic is allowed.

Bind mode

A Cisco IOS XE Catalyst SD-WAN device has Loopback1 and Loopback2 configured as TLOCs and bound to the physical interface GigabitEthernet1. The device also has another interface, Loopback3, which is not configured as a TLOC.

Physical interface GigabitEthernet1 will be treated as a TLOC interface for incoming VPN 0.

In this example:

- If the traffic is destined for Loopback1, implicit ACL rules of Loopback1 are applied.
- If the traffic is destined for Loopback2, implicit ACL rules of Loopback2 are applied.

- If the traffic is destined for Loopback3 on GigabitEthernet1, traffic is allowed.
- If the traffic is destined for another device passing through GigabitEthernet1, it is dropped.

If the bound interface, GigabitEthernet1, is also configured as a TLOC, the traffic to Loopback3 will be subjected to implicit ACL rules on GigabitEthernet1.

Unbind mode

A Cisco IOS XE Catalyst SD-WAN device has Loopback1 configured as a TLOC and is in unbind mode. Loopback2 is not configured as a TLOC. The device also has GigabitEthernet1 interface, which is configured as a TLOC, and GigabitEthernet4 interface, which is not configured as a TLOC.

In this example:

- If the traffic destined for Loopback1 arrives at GigabitEthernet1, the Loopback1 implicit ACL rules are applied. If the traffic is destined for GigabitEthernet1, the GigabitEthernet1 implicit ACL rules are applied.
- If the traffic destined for Loopback1 arrives at GigabitEthernet4, the Loopback1 implicit ACL rules are applied. If the traffic is destined for GigabitEthernet4, traffic is allowed.
- If the traffic destined for Loopback2 arrives on GigabitEthernet1, the GigabitEthernet1 implicit ACL rules are applied. If the traffic is destined for another device passing through GigabitEthernet1, it is dropped.

If the traffic is destined for another device passing through GigabitEthernet4, the traffic is forwarded.

Configure implicit ACL on loopback interfaces using CLI commands

You can configure implicit ACL on loopback interfaces using a feature template or using a CLI Add-on template in Cisco SD-WAN Manager.

To configure implicit ACL on loopback interfaces using a feature template, see *Configure VPN Ethernet Interface*.

For information on using the CLI Add-On template, see *Create a CLI Add-On Feature Template*.

Procedure

Step 1 Configure a loopback interface that emulates an interface that is always up.

Example:

```
Device(config)# sdwan
Device(config)# interface Loopback100
```

Use the interface name format **loopback** *string*, where *string* can be any alphanumeric value and may include underscores (_) and hyphens (–). The total interface name, including **loopback**, can be up to 16 characters long. Because of the flexibility of interface naming in the CLI, interfaces such as **lo0** and **loopback0** are parsed as different strings and are

not interchangeable. For the CLI to recognize an interface as a loopback interface, its name must begin with the full string **loopback**.

Step 2 Configure an interface as a secure transport connection.

Example:

```
Device(config)# tunnel-interface
```

Step 3 Permit or deny a service.

- To permit all the services, use the **allow-service** *all* command.
- To permit a specific service, use the **allow-service** *service name* command.
- To deny a service, use the **no allow-service** *service name* command.

Example:

```
Device(config)# no allow-service bgp
Device(config)# allow-service dhcp
```

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.16.1a, configuring the **allow-service** *all* command on Cisco SD-WAN Controller is only applicable for the following services **bgp**, **dhcp**, **dns**, **https**, **icmp**, **netconf**, **ntp**, **ospf**, **sshd**, and **stun**.

Step 4 Enable implicit ACL protection on a physical interface for incoming VPN 0 traffic.

Example:

```
Device(config)# implicit-acl-on-bind-intf
```

Use this command to enable implicit ACL protection on a physical interface in cases where a physical interface is not configured with a TLOC and bound to the loopback TLOC interface.

The following example shows implicit ACL configured on a loopback interface.

```
sdwan interface Loopback100
  tunnel-interface
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
  exit
```

Examples of implicit ACL configurations on loopback interfaces

Configuration Examples for Implicit ACL Configured on a Loopback Interface

Configuration Examples for Implicit ACL Configured on a Loopback Interface in Bind Mode with TLOC Configured

This example shows implicit ACL configured on a loopback interface in bind mode with TLOC configured:

```
Device(config)# sdwan interface Loopback1
Device (config-interface-Loopback1)# tunnel-interface
Device (config-tunnel-interface)# encap ipsec
Device (config-tunnel-interface)# color 3g
Device (config-tunnel-interface)# bind GigabitEthernet1
Device (config-tunnel-interface)# implicit-acl-on-bind-intf
Device (config-tunnel-interface)# no allow-service bgp
Device (config-tunnel-interface)# allow-service dhcp
Device (config-tunnel-interface)# allow-service dns
Device (config-tunnel-interface)# allow-service icmp
Device (config-tunnel-interface)# no allow-service sshd
Device (config-tunnel-interface)# no allow-service netconf
Device (config-tunnel-interface)# no allow-service ntp
Device (config-tunnel-interface)# no allow-service ospf
Device (config-tunnel-interface)# no allow-service stun
Device (config-tunnel-interface)# allow-service https
Device (config-tunnel-interface)# no allow-service snmp
Device (config-tunnel-interface)# no allow-service bfd
Device (config-tunnel-interface)# exit
```

Configuration Examples for Implicit ACL Configured on a Loopback Interface in unbind Mode with TLOC Configured

This example shows implicit ACL configured on a loopback interface in unbind mode with TLOC configured:

```
Device(config)# sdwan interface Loopback1
Device (config-interface-Loopback1)# tunnel-interface
Device (config-tunnel-interface)# encap ipsec
Device (config-tunnel-interface)# color 3g
Device (config-tunnel-interface)# no allow-service bgp
Device (config-tunnel-interface)# allow-service dhcp
Device (config-tunnel-interface)# allow-service dns
Device (config-tunnel-interface)# allow-service icmp
Device (config-tunnel-interface)# no allow-service sshd
Device (config-tunnel-interface)# no allow-service netconf
Device (config-tunnel-interface)# no allow-service ntp
Device (config-tunnel-interface)# no allow-service ospf
Device (config-tunnel-interface)# no allow-service stun
Device (config-tunnel-interface)# allow-service https
Device (config-tunnel-interface)# no allow-service snmp
Device (config-tunnel-interface)# no allow-service bfd
Device (config-tunnel-interface)# exit
```

Verify implicit ACL configurations on loopback interfaces

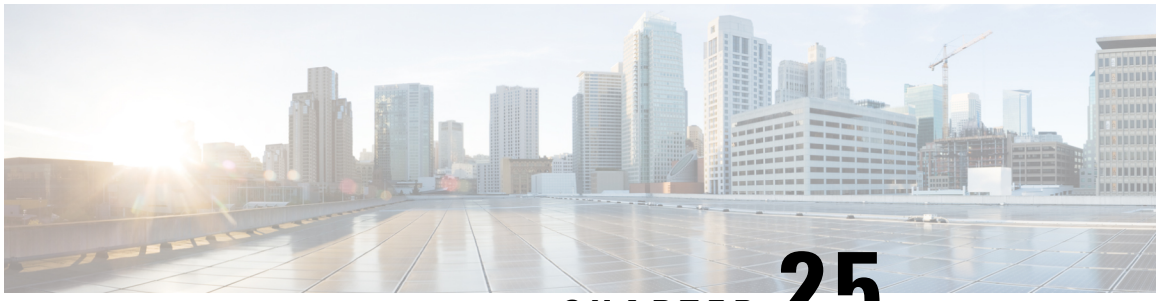
This section provides example for verifing implicit ACL configurations on loopback interfaces

Use the **show platform hardware qfp active statistics drop** command to verify implicit ACL configuration on loopback interfaces. The **show platform hardware qfp active statistics drop** command displays drop statistics that help identify implicit ACL activity on loopback interfaces.

The following is a sample output from the **show platform hardware qfp active statistics drop** command:

```
Device# show platform hardware qfp active statistics drop
Last clearing of QFP drops statistics : never


-------------------------------------------------------------------------
Global Drop Stats                          Packets                Octets
-------------------------------------------------------------------------
Disabled                                         4                   266
Ipv4EgressIntfEnforce                           15                 10968
Ipv6NoRoute                                      6                   336
Nat64v6tov4                                      6                   480
SVIInputInvalidMac                             244                 15886
SdwanImplicitAclDrop                           160                 27163
UnconfiguredIpv4Fia                         942525              58524580
UnconfiguredIpv6Fia                          77521               9587636
```



CHAPTER 25

Subinterfaces

- Subinterfaces, on page 477
- Configuration examples for subinterfaces, on page 478
- Verify configurations on subinterfaces, on page 479

Subinterfaces

Subinterfaces in Cisco Catalyst SD-WAN are logical interfaces that are configured on a physical interface to enable flexible network segmentation.

Interface speed

Interface speed is the rate at which data is transmitted over a physical or logical interface. When a Cisco IOS XE Catalyst SD-WAN device starts, the Cisco Catalyst SD-WAN software autodetects the SFPs present in the router and sets the interface speed accordingly. The software then negotiates the interface speed with the device at the remote end of the connection to establish the actual operating speed. For non-physical interfaces, such as those used for the system IP address and loopback interfaces, the interface speed defaults to 10 Mbps. In Cisco SD-WAN Controller and Cisco SD-WAN Manager systems, the initial interface speed is 1000 Mbps, with the operating speed negotiated with the remote device. The controller interface speed may vary depending on the virtualization platform, the NIC used, and the drivers present in the software

Interface MTU

MTU (Maximum Transmission Unit) is the largest size, in bytes, of a packet that can be sent on an interface without fragmentation. In Cisco Catalyst SD-WAN, by default, all interfaces have an MTU of 1500 bytes.

Here is the lookup table summarizing the MTU range for Cisco IOS XE Catalyst SD-WAN devices by release and interface type:

Release	Interface Type	MTU Range (bytes)
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and earlier		576 through 2000
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and later	1 GE interfaces	576 through 9216
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a and later	10 GE and 100 GE interfaces	576 through 9216

For Cisco SD-WAN Validator, Cisco SD-WAN Manager, and Cisco SD-WAN Controllers, you can configure interfaces to use ICMP to perform path MTU (PMTU) discovery. When PMTU discovery is enabled, the device automatically negotiates the largest MTU size that the interface supports in an attempt to minimize or eliminate packet fragmentation.

On Cisco IOS XE Catalyst SD-WAN device, the Cisco Catalyst SD-WAN BFD software automatically performs PMTU discovery on each transport connection (that is, for each TLOC, or color). BFD PMTU discovery is enabled by default, and it is recommended that you use it and not disable it.

Note If the network path only supports an MTU smaller than 1500 bytes and PMTU discovery is enabled, ICMP responses blocked by the firewall may prevent Cisco SD-WAN Manager from dynamically adjusting the MTU. In such cases, either configure the Cisco SD-WAN Manager interface MTU to match the network MTU or ensure ICMP traffic is allowed through the firewall.

Note BFD is a data plane protocol and so does not run on Cisco SD-WAN Validator, Cisco SD-WAN Manager, and Cisco SD-WAN Controllers.

Configuration examples for subinterfaces

This section provides configuration examples for subinterfaces.

When you create a subinterface that does not specify an IP MTU value, the subinterface inherits the IP MTU value from the parent interface. If you want the subinterface to have a different IP MTU value, use the **ip mtu** command in the subinterface configuration to set the IP MTU for the sub interface.

The following is a configuration example for subinterfaces:

```
interface GigabitEthernet0/0/0
 mtu 1504
 no ip address
!
interface GigabitEthernet0/0/0.9
 encapsulation dot1Q 9
 no shutdown
 ip address 192.168.9.32 255.255.255.0
!
interface Tunnel9
 no shutdown
 ip unnumbered GigabitEthernet0/0/0.9
 no ip redirects
 ipv6 unnumbered GigabitEthernet0/0/0.9
 no ipv6 redirects
 tunnel source GigabitEthernet0/0/0.9
 tunnel mode sdwan
!
sdwan
 interface GigabitEthernet0/0/0.9
  tunnel-interface
   encapsulation ipsec
   color private1
```

```
 !
!
```

Verify configurations on subinterfaces

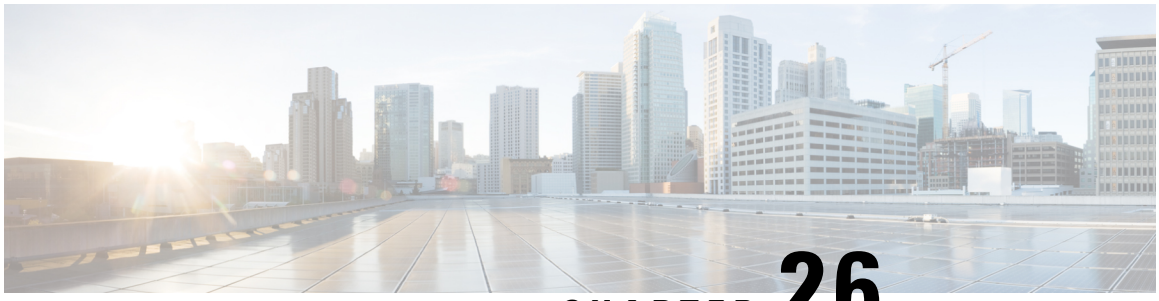
This section provides details on how to verify configurations on subinterfaces.

Configuration example to display information about interface speed and MTU

To display the actual speed of each interface, use the **show interfaces** command. The following example displays interface information on all interfaces.

```
Device# show interfaces
GigabitEthernet0/0/0 is up, line protocol is up
  Hardware is ISR4331-3x1GE, address is 084f.f99b.267c (bia 084f.f99b.267c)
  Description: INET
  Internet address is 10.3.6.2/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 1000Mbps, link type is auto, media type is RJ45
  output flow-control is off, input flow-control is off
  ARP type: ARPA, ARP Timeout 00:20:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 2000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 1 packets/sec
     235182 packets input, 23708237 bytes, 0 no buffer
     Received 1 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 170048 multicast, 0 pause input
     71585 packets output, 12131971 bytes, 0 underruns
     Output 6 broadcasts (0 IP multicasts)
     0 output errors, 0 collisions, 1 interface resets
     1 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
GigabitEthernet0/0/1 is up, line protocol is up
  Hardware is ISR4331-3x1GE, address is 084f.f99b.267d (bia 084f.f99b.267d)
  Description: Service
  Internet address is 10.3.13.2/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 1000Mbps, link type is auto, media type is RJ45
  output flow-control is off, input flow-control is off
  ARP type: ARPA, ARP Timeout 00:20:00
  Last input 00:00:00, output 00:00:14, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
```

```
  5 minute output rate 0 bits/sec, 0 packets/sec
     144332 packets input, 13390830 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 144332 multicast, 0 pause input
     13613 packets output, 5135370 bytes, 0 underruns
     Output 1 broadcasts (0 IP multicasts)
     0 output errors, 0 collisions, 1 interface resets
     1 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
<output truncated>
```



CHAPTER 26

Dynamic Interfaces

- Feature history for dynamic interfaces, on page 481
- Configure dynamic interfaces, on page 481

Feature history for dynamic interfaces

Table 147: Feature History

Feature Name	Release Information	Description
Configuring Dynamic Interfaces	Cisco IOS XE Catalyst SD-WAN Release 17.3.2 Cisco vManage Release 20.3.2	This feature allows you to configure dynamic interfaces for supported devices. A dynamic interface allows a device to select optimum paths in real-time. This feature applies only to the Cisco C8500-12X4QC router.

Configure dynamic interfaces

Configuring dynamic interfaces consists of these general steps:

1. Create a dynamic interface mode feature template. As part of this step, you define modes for the bays in a device.
2. Configure an Interface for Control Connections.
3. Associate the dynamic interface mode feature template with a device template.

You can configure dynamic interfaces for supported devices. A dynamic interface allows a device to select optimum paths in real-time.

When you create a dynamic interface mode feature template, you create a template that defines the modes for the bays in a device.

You can configure the mode for bay 1, bay 2, or both.

The mode for bay 0 is configured automatically and cannot be changed. If you configure the mode for bay 1 as 100G, bay 0 is disabled because the 10G interfaces on bay 0 do not apply in this case.

Procedure

Step 1 Create a dynamic interface mode feature template

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

b) Click **Device Templates**.

In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

c) Click the **Create Template** drop-down list and choose **Feature Template**.

d) From the **Device Model** drop-down list, choose the device for which you wish to create the template.

In **Template Name**, enter a name for the template. This field may contain uppercase and lowercase letters, digits 0 through 9, hyphens (-), and underscores (_).

In **Description**, enter a description of the template. This field can contain any characters and spaces.

e) From **Additional Templates**, choose the **Dynamic Interface Mode** drop-down list and click **Create Template**.

In **Template Name**, enter a name for the template. This field may contain uppercase and lowercase letters, digits 0 through 9, hyphens (-), and underscores (_).

In **Description**, enter a description of the template. This field can contain any characters and spaces.

f) Configure the mode for bay 1, bay 2, or both bays by choosing the desired value in the **Bay 1**, **Bay 2**, or both fields.

You cannot change the default value for bay 0.

g) Click Save.

Open a TAC case when there is a mismatch between confd and iosd configurations while changing the bay subslot mode on Cisco C8500-12X4QC router..

Step 2 Configure a new VPN 0 interface for an existing control connection to operate with the bays that you configured in Step 1.

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

b) Click **Device Templates**.

In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

c) Click **...** of the template for which you want to configure the interface, and then choose **Edit**.

d) Click **Transport & Management VPN** and perform these actions to create interfaces for the bays:

1. Click **VPN Interface** in the **Additional VPN 0** Template.
2. Choose the new **VPN Interface Ethernet** menu that displays, and then click **Create Template**.
3. In **Template Name**, enter a name for the template.

   This field may contain uppercase and lowercase letters, digits 0 through 9, hyphens (-), and underscores (_).
4. In **Description**, enter a description of the template.

   This field can contain any characters and spaces.

5. Add control connections to the bays that you configured as described in Step 1.

e) Choose **Basic Configuration** and perform these actions:

1. In **Interface Name**, enter a name for the interface.

   Enter a name in the format that this example shows: “FortyGigabitEthernet0/1/0.”

2. Configure other options on this tab as needed.

f) From **Tunnel**, set **Tunnel Interface** to **On**.

g) Click Save.

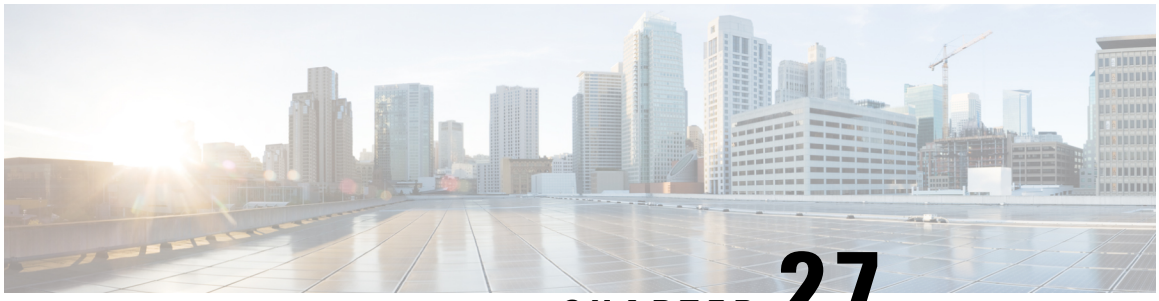
h) Choose **IPv4 Route** and perform these actions to configure an IPv4 route for the VPN0 template:

1. Click **New IPv4 Route**.
2. In **Prefix**, enter a prefix for the IPv4 route.
3. In **Gateway**, choose **Next Hop**.
4. Configure items as needed in **Next Hop**, and then click **Add**.
5. Click **Save**.

i) Click **Update**.

What to do next

After you create the dynamic interface mode feature template, associate it with a device template and attach the device template to a device. For instructions, see *Create a Device Template from Feature Templates*.



CHAPTER 27

VPN Ethernet Interface

- Configure VPN ethernet interface, on page 485

Configure VPN ethernet interface

Use one of these methods to configure VPN ethernet interface:

- Configuration group
- Feature template

Configure VPN ethernet interface using a configuration group

Follow these steps to configure VPN ethernet interface using a configuration group.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure a Transport VPN feature in Transport and Management profile.

Step 3 Create and configure Ethernet Interface feature in Transport VPN.

a) Configure basic VPN parameters.

Field	Description
Shutdown	Enable or disable the interface.
Interface Name*	Enter a name for the interface. Spell out the interface names completely (for example, GigabitEthernet0/0/0). Configure all the interfaces of the router, even if you are not using them, so that they are configured in the shutdown state and so that all default values for them are configured.

Field	Description
Description	Enter a description for the interface.
Auto Detect Bandwidth	Enable this option to automatically detect the bandwidth for WAN interfaces. The device detects the bandwidth by contacting an iPerf3 server to perform a speed test.
IPv4 Settings	Configure an IPv4 VPN interface. • **Dynamic**: Choose **Dynamic** to set the interface as a Dynamic Host Configuration Protocol (DHCP) client so that the interface receives its IP address from a DHCP server. • **Static**: Choose **Static** to enter an IP address that doesn't change.
Dynamic DHCP Distance	Enter an administrative distance value for routes learned from a DHCP server. This option is available when you choose **Dynamic**. Default: 1
IP Address	Enter a static IPv4 address. This option is available when you choose **Static**.
Subnet Mask	Enter the subnet mask. From Cisco Catalyst SD-WAN Control Components Release 20.15.1, if you enter a variable in the IP Address field, this field automatically uses a variable.
Configure Secondary IP Address	Enter up to four secondary IPv4 addresses for a service-side interface. • **IP Address**: Enter the IP address. • **Subnet Mask:** Enter the subnet mask.
DHCP Helper	To designate the interface as a DHCP helper on a router, enter up to eight IP addresses, separated by commas, for DHCP servers in the network. A DHCP helper interface forwards BOOTP (broadcast) DHCP requests that it receives from the specified DHCP servers.
IPv6 Settings	Configure an IPv6 VPN interface. • **Dynamic**: Choose **Dynamic** to set the interface as a Dynamic Host Configuration Protocol (DHCP) client so that the interface receives its IP address from a DHCP server. • **Static**: Choose **Static** to enter an IP address that doesn't change. • **None**
IPv6 Address Primary	Enter a static IPv6 address. This option is available when you choose **Static**.
Add Secondary Ipv6	
IP Address	Enter up to two secondary IPv6 addresses for a service-side interface.
Bandwidth Upstream	Enter upstream bandwidth reference value.

Field	Description
Bandwidth Downstream	Enter downstream bandwidth reference value.

b) **Apply Access Lists and QoS Parameters**

Field	Description
Adaptive QoS	To enable or disable adaptive QoS on an ethernet interface on the transport side.
Shaping Rate	Enter the shaping rate to control the maximum rate of traffic sent.
ACL	To define IPv4 and IPv6 ACL as ingress and egress.

c) Create a tunnel interface.

Field	Description
Tunnel Interface	Enable this option to create a tunnel interface.
Per-tunnel QoS	Enable this option to apply a Quality of Service (QoS) policy on individual tunnels.
Color	Choose a color for the TLOC.
Color Description	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enter a description associated to the TLOC color.
Restrict	Enable this option to limit the remote TLOCs that the local TLOC can establish BFD sessions with. When a TLOC is marked as restricted, a TLOC on the local router establishes tunnel connections with a remote TLOC only if the remote TLOC has the same color.
Groups	Enter a group number. Range: 1 through 4294967295
Border	Enable this option to set the TLOC as a border TLOC.
Maximum Control Connections	Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 100 Default: 2
Validator As Stun Server	Enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the Cisco IOS XE Catalyst SD-WAN device is located behind a NAT.
Exclude Controller Group List	Set the identifiers of one or more Cisco SD-WAN Controller groups that this tunnel is not allowed to connect to. Range: 1 through 100

Field	Description
Manager Connection Preference	Set the preference for using a tunnel interface to exchange control traffic with Cisco SD-WAN Manager. Range: 0 through 8 Default: 5
Full Port Hop	Minimum release: Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled
Port Hop	Enable port hopping. If port hopping is enabled globally, you can disable it on an individual TLOC (tunnel interface). Default: Enabled Starting from Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, this field is deprecated. Instead use the **Full Port Hop** option. See the **Full Port Hop** field.
Low-Bandwidth Link	Enable this option to characterize the tunnel interface as a low-bandwidth link.
Tunnel TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 500 to 1460 bytes Default: None
Clear-Dont-Fragment	Enable this option to clear the Don't Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than the MTU of the interface are fragmented before being sent.
CTS SGT Propagation	Enable CTS SGT propagation on an interface.
Network Broadcast	Enable this option to accept and respond to network-prefix-directed broadcasts.

Field	Description
Allow Service	Allow or disallow the following services on the interface: • **All** • **BGP** • **DHCP** • **NTP** • **SSH** • **DNS** • **ICMP** • **HTTPS** • **OSPF** • **STUN** • **SNMP** • **NETCONF** • **BFD**
Encapsulation	

Field	Description
Encapsulation*	Choose an encapsulation type: • **gre**: Use GRE encapsulation on the tunnel interface. • **ipsec**: Use IPsec encapsulation on the tunnel interface. **Note** If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. When you choose **gre**, the following fields appear: • **GRE Preference**: Enter a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 • **GRE Weight**: Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1 When you choose **ipsec**, the following fields appear: • **IPSEC Preference**: Enter a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 • **IPSEC Weight**: Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1
Multi-Region Fabric **Note** These options appear only when Multi-Region Fabric is enabled.	
Connect to Core Region	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) (Applicable to a border router only) In a Multi-Region Fabric scenario, enable this option to specify how to use the Ethernet interface: • **Share Interface with Access Region**: Share the interface between the access region and core region. • **Keep Exclusive to Core Region**: Use the interface only for the core region.

Field	Description
Connect to Secondary Region	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) (Applicable to an edge router only) In a Multi-Region Fabric scenario, enable this option to specify how to use the Ethernet interface: • **Share Interface with Access Region**: Share the interface between the primary and secondary regions. • **Keep Exclusive to Secondary Region**: Use the interface only for the secondary region.

d) Configure an interface as a NAT device.

Field	Description
IPv4 Settings	
NAT	Enable this option to have the interface act as a NAT device.
NAT Type	Choose the NAT translation type for IPv4: • **interface** • **pool** • **loopback** Default: **interface**. It is supported for NAT64.
UDP Timeout	Specify when NAT translations over UDP sessions time out. Range: 1 through 8947 minutes Default: 1 minute
TCP Timeout	Specify when NAT translations over TCP sessions time out. Range: 1 through 8947 minutes Default: 60 minutes (1 hour)

Field	Description
Add Multiple NAT	Choose the NAT type: • **Interface**: This is the default value. • **Pool**: Configure the following: • **Pool ID**: Enter a NAT pool number configured in the centralized data policy. The NAT pool name must be unique across VPNs and VRFs. You can configure up to 31 (1–32) NAT pools per router. • **Range Start**: Enter a starting IP address for the NAT pool. • **Range End**: Enter a closing IP address for the NAT pool. • **Prefix length**: Specify the maximum number of source IP addresses that can be NATed in the NAT pool. • **Overload**: Enable this option to configure per-port translation. If this option is disabled, only dynamic NAT is configured on the end device. Per-port NAT is not configured. Default: Disabled • **Loopback**: Provide a value for the NAT inside source loopback interface.
Configure New Static NAT	Add a static NAT mapping
Source IP	Enter the source IP address to be translated.
Translate IP	Enter the translated source IP address.
Direction	Choose the direction in which to perform network address translation. • **inside**: Translates the IP address of packets that are coming from the service side of the device and that are destined for the transport side of the router. • **outside**: Translates the IP address of packets that are coming to the device from the transport side device and that are destined for a service-side device.
Source VPN	Enter the source VPN ID.
IPv6 Settings	
IPv6 NAT	Enable this option to have the interface act as a NAT device.
Select NAT	Choose NAT64 or NAT66. When you choose NAT66, the following fields appear: • **Source Prefix**: Enter the source IPv6 prefix. • **Translated Source Prefix**: Enter the translated source prefix. • **Source VPN ID**: Enter the source VPN ID. • **Egress Interface**: Enable this option to have the interface act as an egress interface.

e) Add ARP table entries.

Field	Description
IP Address	Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name.
MAC Address	Enter the MAC address in colon-separated hexadecimal notation.

f) Configure advanced properties.

Field	Description
Duplex	Specify whether the interface runs in full-duplex or half-duplex mode. Default: full
MAC Address	Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation.
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 through 9216 Default: 1500 bytes
Interface MTU	Enter the maximum transmission unit size for frames received and transmitted on the interface. Range: 1500 through 1518 (GigabitEthernet0), 1500 through 9216 (other GigabitEthernet) Default: 1500 bytes
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 500 to 1460 bytes Default: None
Speed	Specify the speed of the interface, for use when the remote end of the connection does not support autonegotiation. Values: 10, 100, 1000, 2500, or 10000 Mbps
ARP Timeout	ARP timeout controls how long we maintain the ARP cache on a router. Specify how long it takes for a dynamically learned ARP entry to time out. Range: 0 through 2147483 seconds Default: 1200 seconds
Autonegotiate	Enable this option to turn on autonegotiation.

Field	Description
Media Type	Specify the physical media connection type on the interface. Choose one of the following: • **auto-select**: A connection is automatically selected. • **rj45**: Specifies an RJ-45 physical connection. • **sfp**: Specifies a small-form factor pluggable (SFP) physical connection for fiber media.
TLOC Extension	Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN. **Note** TLOC extension over L3 is supported only for Cisco IOS XE Catalyst SD-WAN devices. If configuring TLOC extension over L3 for a Cisco IOS XE Catalyst SD-WAN device, enter the IP address of the L3 interface.
GRE tunnel source IP	Enter the IP address of the extended WAN interface.
XConnect	Enter the name of a physical interface on the same router that connects to the WAN transport.
Load Interval	Enter an interval value for interface load calculation.
IP Directed Broadcast	An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet, but which originates from a node that is not itself part of that destination subnet. A device that is not directly connected to its destination subnet forwards an IP directed broadcast in the same way it would forward unicast IP packets destined to a host on that subnet. When a directed broadcast packet reaches a device that is directly connected to its destination subnet, that packet is broadcast on the destination subnet. The destination address in the IP header of the packet is rewritten to the configured IP broadcast address for the subnet, and the packet is sent as a link-layer broadcast. If directed broadcast is enabled for an interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which that interface is attached are broadcast on that subnet.
ICMP Redirect Disable	ICMP redirects are sent by a router to the sender of an IP packet when a packet is being routed sub-optimally. The ICMP redirect informs the sending host to forward subsequent packets to that same destination through a different gateway. By default, an interface allows ICMP redirect messages.

What to do next

Also see *Deploy a Configuration Group*.

Configure prefix list for VRRP using a configuration group

Follow these steps to configure prefix list for VRRP using a configuration group.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure Prefix List for VRRP in a Policy Object Profile.

a) Choose the **Prefix** policy object from the **Select Policy Object** drop-down list.
b) Enter the **Prefix List Name**.
c) In the **Internet Protocol** field, click **IPv4** or **IPv6**.
d) Under **Add Prefix**, enter the prefix for the list. Optionally, click the **Choose a file** link to import a prefix list.
e) Click **Save**.

The following table describe the options for configuring the prefix.

Table 148: Prefix List

Field	Description
Prefix List Name	Enter a name for the prefix list.
Internet Protocol	Specifies the internet protocol. The options are IPv4 and IPv6.

What to do next

Also see *Deploy a configuration group*.

Configure VPN ethernet interface using templates

Follow these steps to configure VPN ethernet interface using feature template.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Device Templates**, and click **Create Template**.

Note
In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

Step 3 From the **Create Template** drop-down list, choose **From Feature Template**.

Step 4 From the **Device Model** drop-down list, choose the type of device for which you are creating the template.

Step 5 To create a template for VPN 0 or VPN 512:

a) Click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.

b) Under **Additional VPN 0 Templates**, click **Cisco VPN Interface Ethernet**.

c) From the **VPN Interface** drop-down list, click **Create Template**. The **Cisco VPN Interface Ethernet** template form displays.

This form contains fields for naming the template, and fields for defining the VPN Interface Ethernet parameters.

d) In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

e) In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

Step 6 Configure the VPN ethernet interface parameters.

a) Configure basic interface functionality in a VPN.

Parameter Name	IPv4 or IPv6	Options	Description
Shutdown*	Click **No** to enable the interface.		
Interface name*	Enter a name for the interface. For Cisco IOS XE Catalyst SD-WAN devices, you must: • Spell out the interface names completely (for example, GigabitEthernet0/0/0). • Configure all the router's interfaces, even if you are not using them, so that they are configured in the shutdown state and so that all default values for them are configured.		
Description	Enter a description for the interface.		
IPv4 / IPv6	Click **IPv4** to configure an IPv4 VPN interface. Click **IPv6** to configure an IPv6 interface.		
Dynamic	Click **Dynamic** to set the interface as a Dynamic Host Configuration Protocol (DHCP) client, so that the interface receives its IP address from a DHCP server.		
	Both	**DHCP Distance**	Optionally, enter an administrative distance value for routes learned from a DHCP server. Default is 1.
	IPv6	**DHCP Rapid Commit**	Optionally, configure the DHCP IPv6 local server to support DHCP Rapid Commit, to enable faster client configuration and confirmation in busy environments. Click **On** to enable DHCP rapid commit. Click **Off** to continue using the regular commit process.

Parameter Name	IPv4 or IPv6	Options	Description
Static	Click **Static** to enter an IP address that doesn't change.		
	IPv4	**IPv4 Address**	Enter a static IPv4 address.
	IPv6	**IPv6 Address**	Enter a static IPv6 address.
Secondary IP Address	**IPv4**	Click **Add** to enter up to four secondary IPv4 addresses for a service-side interface.	
IPv6 Address	**IPv6**	Click **Add** to enter up to two secondary IPv6 addresses for a service-side interface.	
DHCP Helper	**Both**	To designate the interface as a DHCP helper on a router, enter up to eight IP addresses, separated by commas, for DHCP servers in the network. A DHCP helper interface forwards BootP (broadcast) DHCP requests that it receives from the specified DHCP servers.	
Block Non-Source IP	**Yes** / **No**	Click **Yes** to have the interface forward traffic only if the source IP address of the traffic matches the interface's IP prefix range. Click **No** to allow other traffic.	

b) Configure a tunnel interface.

Parameter Name	Description
Tunnel Interface	Click **On** to create a tunnel interface.
Color	Select a color for the TLOC.
Color Description	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enter a description associated to the TLOC color.
Full Port Hop	Minimum release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled
Port Hop	Click **On** to enable port hopping, or click **Off** to disable it. If port hopping is enabled globally, you can disable it on an individual TLOC (tunnel interface). To control port hopping on a global level, use the System configuration template. Default: Enabled Cisco SD-WAN Manager and Cisco SD-WAN Controller default: Disabled Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, this field is deprecated. Instead use the **Full Port Hop** option. See the **Full Port Hop** field.

Parameter Name	Description
TCP MSS	TCP MSS affects any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS is examined against the MSS exchanged in the three-way handshake. The MSS in the header is lowered if the configured TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. If the TCP MSS is to be configured, it should be set at 40 bytes lower than the minimum path MTU. Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes Default: None
Clear-Dont-Fragment	Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent. Click **On** to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, packets larger than the MTU of the interface are fragmented before being sent. **Note** **Clear-Dont-Fragment** clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected.
Allow Service	Select **On** or **Off** for each service to allow or disallow the service on the interface.

To configure additional tunnel interface parameters, click **Advanced Options**:

Parameter Name	Description
Carrier	Select the carrier name or private network identifier to associate with the tunnel. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default Default: default
NAT Refresh Interval	Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds Default: 5 seconds
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 10000 milliseconds Default: 1000 milliseconds (1 second)

Parameter Name	Description
Hello Tolerance	Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down. Range: 12 through 60 seconds Default: 12 seconds

c) Configure an interface as a NAT device.

For information on how to configure NAT, see the *Cisco Catalyst SD-WAN NAT Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x*.

d) Configure the shaping rate for an interface and apply QoS map, rewrite rules, access lists, and policers to an interface.

Parameter Name	Description
Shaping rate	Configure the aggregate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).
QoS Map	Specify the name of the QoS map to apply to packets being transmitted out the interface.
Rewrite Rule	Click **On**, and specify the name of the rewrite rule to apply on the interface.
Ingress ACL – IPv4	Click **On**, and specify the name of the access list to apply to IPv4 packets being received on the interface.
Egress ACL – IPv4	Click **On**, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface.
Ingress ACL – IPv6	Click **On**, and specify the name of the access list to apply to IPv6 packets being received on the interface.
Egress ACL – IPv6	Click **On**, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface.
Ingress Policer	Click **On**, and specify the name of the policer to apply to packets received on the interface.
Egress Policer	Click **On**, and specify the name of the policer to apply to packets being transmitted on the interface.

e) Configure static ARP table entries on the interface.

Parameter Name	Description
IP Address	Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name.
MAC Address	Enter the MAC address in colon-separated hexadecimal notation.

f) Configure VRRP to allow multiple routers to share a common virtual IP address for default gateway redundancy.

Parameter Name	Description
Group ID	Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups. Range: 1 through 255

Parameter Name	Description
Priority	Enter the priority level of the router. There router with the highest priority is elected as primary VRRP router. If two routers have the same priority, the one with the higher IP address is elected as primary VRRP router. Range: 1 through 254 Default: 100
Timer (milliseconds)	Specify how often the primary VRRP router sends VRRP advertisement messages. If subordinate routers miss three consecutive VRRP advertisements, they elect a new primary VRRP routers. Range: 100 through 40950 milliseconds Default: 1000 msecs **Note** When the timer is 100 ms for the VRRP feature template on Cisco IOS XE Catalyst SD-WAN devices, the VRRP fails if the traffic is high on LAN interface. Use the 100 msec timer only if the Cisco IOS XE Catalyst SD-WAN device platform supports it, and if there are fewer tunnel groups.
Track OMP Track Prefix List	By default, VRRP uses of the state of the service (LAN) interface on which it is running to determine which router is the primary virtual router. if a router loses all its WAN control connections, the LAN interface still indicates that it is up even though the router is functionally unable to participate in VRRP. To take WAN side connectivity into account for VRRP, configure one of the following: **Track OMP**—Click **On** for VRRP to track the Overlay Management Protocol (OMP) session running on the WAN connection. If the primary VRRP router loses all its OMP sessions, VRRP elects a new default gateway from those that have at least one active OMP session. **Note** From Cisco Catalyst SD-WAN Manager Release 20.18.1, enabling **Track OMP** changes the device CLI command from **vrrp track omp shutdown** to **vrrp track omp decrement 10**. **Track Prefix List**—Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the primary VRRP router loses all its OMP sessions, VRRP failover occurs as described for the Track OMP option. In addition, if reachability to all of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic is dropped while the routers determine the primary VRRP router.
IP Address	Enter the IP address of the virtual router. This address must be different from the configured interface IP addresses of both the local router and the peer running VRRP.

g) Configure other advanced interface properties.

Parameter Name	Description
Duplex	Choose full or half to specify whether the interface runs in full-duplex or half-duplex mode. Default: full
MAC Address	Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation.
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 through 1804 Default: 1500 bytes
PMTU Discovery	Click **On** to enable path MTU discovery on the interface. PMTU determines the largest MTU size that the interface supports so that packet fragmentation does not occur.
Flow Control	Select a setting for bidirectional flow control, which is a mechanism for temporarily stopping the transmission of data on the interface. Values: autonet, both, egress, ingress, none Default: autoneg
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes Default: None
Speed	Specify the speed of the interface for use when the remote end of the connection does not support autonegotiation. Values: 10, 100, 1000, or 10000 Mbps
Clear-Dont-Fragment	Click **On** to clear the Don't Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent. **Note** Clear-Dont-Fragment clears the DF bit when there is fragmentation needed and the DF bit is set. For packets not requiring fragmentation, the DF bit is not affected.

Parameter Name	Description
Autonegotiation	**Note** For releases before Cisco vManage Release 20.6.1, the default value of the field is **On**. To turn autonegotiation off, click **Off**. From Cisco vManage Release 20.6.1, the default behavior of the field is as follows: • For the Gigabit Ethernet interface type, the **Autonegotiation** field is blank by default. However, the autonegotiation is set to **On** when the field is left blank. • For other interface types such as Ten Gigabit Ethernet and Hundred Gigabit Ethernet, the **Autonegotiation** field is blank by default. To turn autonegotiation on or off, click **On** or **Off** respectively. From Cisco SD-WAN Manager Release 20.12.4: In the Cisco Catalyst 8300 Series devices, for the TenGigabitEthernet interface type, do not leave the **Autonegotiation** field blank.
TLOC Extension	Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN. Note that TLOC extension over L3 is only supported for Cisco IOS XE routers. If configuring TLOC extension over L3 for a Cisco IOS XE router, enter the IP address of the L3 interface.
GRE Tunnel Source IP	Enter the IP address of the extended WAN interface.
Xconnect (on IOS XE routers)	Enter the name of a physical interface on the same router that connects to the WAN transport.

Configure a prefix list for VRRP

Follow these steps to configure a prefix list for VRRP.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy**.

Step 2 Click **Localized Policy**.

From the **Custom Options** drop-down list, click **Lists**.

Step 3 Click **Prefix** from the left pane, and click **New Prefix List**.

Step 4 In **Prefix List Name**, enter a name for the prefix list.

Choose **IPv4** as the **Internet Protocol**.

Step 5 In **Add Prefix**, enter the prefix entries separated by commas.

a) Click **Add**.
b) Click **Next** and configure **Forwarding Classes/QoS**.
c) Click **Next** and configure **Access Control Lists**.
d) Click **Next** and in **Route Policy** pane, select a relevant route policy and click **…** , and click **Edit** to add the newly added prefix list.
e) From the **Match** pane, click **AS Path List** and in the **Address**, choose the newly added prefix list.
f) Click **Save Match and Actions**.
g) Click **Next** and enter the **Policy Name** and **Policy Description** in the **Policy Overview** screen.
h) Click **Save Policy**.

Configure a prefix list for VRRP in the device template

Follow these steps to configure the prefix list to the VRRP and the localized policy in the device template.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Device Templates**.

In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

Step 3 Select a relevant device template and click **…** and click **Edit** to edit the template details.

Step 4 From **Policy**, select the policy with the newly added prefix list.

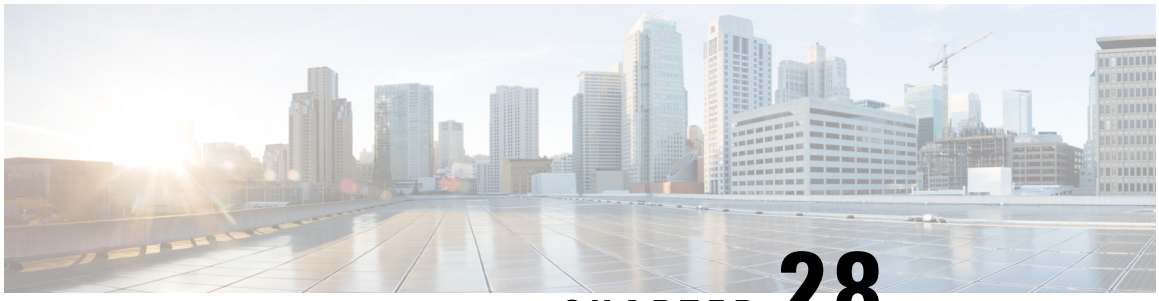
a) Click **Update**.
b) Click **Feature Templates**.
c) Select a relevant device template and click **…** and click **Edit** to edit the template details.
d) Click **VRRP**.
e) Select a relevant group ID and click the pen icon to associate the new prefix-list to the VRRP details.
f) Click the **Track Prefix List** drop-down list and enter the newly added prefix-list name.
g) Click **Save Changes**.

Click **Update** to save the changes.

Step 5 Click **Device Templates** and select the policy with the newly added prefix list.

Step 6 Click **…** and click **Attach Devices**.

Step 7 From **Available Devices**, double-click the relevant device to move it to **Selected Devices**, and then click **Attach**.



CHAPTER 28

Cellular Interfaces

- Feature history for cellular interfaces, on page 505
- Cellular interfaces, on page 506
- Supported devices, on page 507
- Guidelines, on page 508
- Configure cellular interface, on page 508
- Reset the profile configuration of a cellular modem, on page 527
- Troubleshoot LTE modem crash, on page 528

Feature history for cellular interfaces

Table 149: Feature History

Feature Name	Release Information	Description
Configure Cellular Interfaces	Cisco Catalyst SD-WAN Manager Release 18.1.1	You can configure cellular interfaces on devies with cellular modules to enable LTE connectivity.
Ability to Configure APNs under Running Configurations for Single and Dual SIMs	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	This feature allows you to create a data profile for a cellular device.
Cellular Module Support for Cisco Catalyst Rugged Series Routers	Cisco IOS XE Catalyst SD-WAN Release 17.15.4 Cisco Catalyst SD-WAN Manager 20.15.4	Support for cellular modules on Cisco Cisco Catalyst IR1101, IR1800 and IR18340 Rugged Series Routers.

Feature Name	Release Information	Description
Reset the Profile Configuration of Cellular Modem	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	This sub-feature of the Cellular Controller feature enables you to reset the configuration of a cellular modem operating on a device using CLI.
Band Select Support in Controller Mode	Cisco Catalyst SD-WAN Manager Release 20.18.1	This sub-feature of the Cellular Controller feature introduces the Cellular Band Select feature-parcel, enabling you to specify which cellular bands to use.

Cellular interfaces

A cellular interface is a network interface that enables wireless communication over a cellular network.

- Provides wireless connectivity when all wired WAN tunnel interfaces on the device are unavailable.
- Functions as the primary WAN link for a branch office, depending on usage patterns and supported data rates.

Cellular module and data profile components

The following components are essential for cellular interface operation:

- Cellular module: Installed in a router to enable LTE connectivity, provides wireless connectivity over a service provider's cellular network, and supports network access for use cases such as branch office connectivity.
- Data profile: Defines parameters for how the device connects to a cellular network and uses the parameters for communication with the service provider.

Supported devices

Table 150: Supported Platforms and Modules

Platform	Minimum Supported Release	Supported Modules
IR1101 Rugged Series Router	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	P-LTE-MNA, P-LTE-VZ, P-LTE-US, P-LTE-GB, P-LTE-IN, P-LTE-JN, P-LTEA-EA, P-LTEA-LA, P-LTEAP18-GL, P-5GS6-GL
	Cisco IOS XE Catalyst SD-WAN Release 17.15.4 Cisco Catalyst SD-WAN Manager 20.15.4	P-LTEA7-JP, P-LTEA7-NA, P-LTEA7-EAL, P-5GS6-R16SA-GL
	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.x	P-LTE-450
IR8100 Rugged Series Router	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	IRMH-LTE-MNA, IRMH-LTEA-EA, IRMH-LTEA-LA, IRMH-LTEAP18-GL, IRMH-5GS6-GL
	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	IRMH-LTE7-NA-900, IRMH-5GR16SA, IRMH-LTE7-EAL
IR1800 Rugged Series Router	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	P-LTE-MNA, P-LTE-VZ, P-LTE-US, P-LTE-GB, P-LTE-IN, P-LTE-JN, P-LTEA-EA, P-LTEA-LA, P-LTEAP18-GL, P-5GS6-GL
	Cisco IOS XE Catalyst SD-WAN Release 17.15.4 Cisco Catalyst SD-WAN Manager 20.15.4	P-LTEA7-NA, P-LTEA7-JP, P-LTEA7-EAL, P-5GS6-R16SA-GL
	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.x	P-LTE-450
IR8340 Rugged Series Router	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	P-LTE-MNA, P-LTEA-EA, P-LTEA-LA, P-LTEAP18-GL P-5GS6-GL
	Cisco IOS XE Catalyst SD-WAN Release 17.15.4 Cisco Catalyst SD-WAN Manager 20.15.4	P-LTEA7-NA, P-LTEA7-JP, P-LTEA7-EAL, P-5GS6-R16SA-GL
Cisco ESR 6300 Series	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	P-LTE-MNA, P-LTEA-EA, P-LTEA-LA, P-LTEAP18-GL

Guidelines

Circuit of last resort

Configure an interface as a circuit of last resort to ensure it remains dormant and is skipped during control connection calculations while primary interfaces are active. Use the **last-resort-circuit** command to enable this functionality on cellular or GigabitEthernet interfaces.

- Ensure that when primary interfaces establish BFD connections, the circuit of last resort shuts down to prevent unnecessary traffic.
- Recognize that the circuit of last resort activates only when all primary interfaces lose their connections, which triggers BFD TLOC Down and Control TLOC Down alarms.

Active circuit

Optimize bandwidth usage when using a cellular interface as an active circuit by adjusting control packet timers and prioritizing non-cellular interfaces for control traffic.

- Increase control packet timers using **omp timers advertisement-interval** and **bfd color hello-interval** to reduce the frequency of OMP update packets and BFD hello packets.
- Configure the **vmanage-connection-preference** command on tunnel interfaces to prioritize non-cellular paths for Cisco SD-WAN Manager control traffic, ensuring at least one interface maintains a non-zero preference value.

Configure cellular interface

A cellular interface is a network interface that enables wireless communication over a cellular network.

Use one of the methods to configure cellular interface.

- Configure cellular interfaces using a configuration group
- Configure cellular interfaces using the CLI
- Configure cellular interfaces using feature templates

Configure cellular interfaces using a configuration group

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.16.1a, Cisco Catalyst SD-WAN Manager Release 20.16.1

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups** .

Step 2 Create and configure a Transport VPN feature in a Transport & Management profile.

a. Configure the basic configuration parameters, such as the VPN.

Table 151: Basic Configuration

Field	Description
VPN	Enter the numeric identifier of the VPN.
Enhance ECMP Keying	Enable the use in the ECMP hash key of Layer 4 source and destination ports, in addition to the combination of the source IP address, destination IP address, protocol, and DSCP field, as the ECMP hash key. Default: Disabled

b. Configure DNS.

Table 152: DNS

Field	Description
Add DNS	
Primary DNS Address (IPv4)	Enter the IP address of the primary IPv4 DNS server in this VPN.
Secondary DNS Address (IPv4)	Enter the IP address of a secondary IPv4 DNS server in this VPN.
Add DNS IPv6	
Primary DNS Address (IPv6)	Enter the IP address of the primary IPv6 DNS server in this VPN.
Secondary DNS Address (IPv6)	Enter the IP address of a secondary IPv6 DNS server in this VPN.

c. Configure host mapping.

Table 153: Host Mapping

Field	Description
Add New Host Mapping	
Hostname*	Enter the hostname of the DNS server. The name can be up to 128 characters.
List of IP*	Enter up to 14 IP addresses to associate with the hostname. Separate the entries with commas.

d. Configure routes.

Table 154: Route

Field	Description
Add IPv4 Static Route	
Network address*	Enter the IPv4 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv4 static route to configure in the VPN.
Subnet Mask*	Enter the subnet mask.
Gateway*	Choose one of the following options to configure the next hop to reach the static route: • **nextHop**: When you choose this option and click **Add Next Hop**, the following fields appear: • **Address***: Enter the next-hop IPv4 address. • **Administrative distance***: Enter the administrative distance for the route. • **dhcp** • **null0**: When you choose this option, the following field appears: • **Administrative distance**: Enter the administrative distance for the route.
Add IPv6 Static Route	
Prefix*	Enter the IPv6 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv6 static route to configure in the VPN.
Next Hop/Null 0/NAT	Choose one of the following options to configure the next hop to reach the static route: • **Next Hop**: When you choose this option and click **Add Next Hop**, the following fields appear: • **Address***: Enter the next-hop IPv6 address. **Administrative distance***: Enter the administrative distance for the route. • **Null 0**: When you choose this option, the following field appears: • **IPv6 Route Null 0***: Enable this option to set the next hop to be the null interface. All packets sent to this interface are dropped without sending any ICMP messages. • **NAT**: When you choose this option, the following field appears: • **IPv6 NAT***: Choose NAT64 or NAT66.
Add BGP Routing	Choose a BGP route.

e. Configure services.

Table 155: Service

Field	Description
Add Service	
Service Type	Choose the service available in the VPN. Value: **TE**

Step 3 Configure a Cellular Interface feature to associate with the Transport VPN.

a. Adjacent to the Transport VPN feature, click + and add a Cellular Interface feature as a subfeature.

b. Configure the basic parameters.

Field	Description
Shutdown*	Enable or disable the interface.
Interface Name*	Enter the name of the interface.
Description*	Enter a description of the cellular interface.
DHCP Helper	Enter up to four IP addresses for DHCP servers in the network, separated by commas, to have the interface be a DHCP helper. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers.

c. Configure the tunnel parameters.

Field	Description
Tunnel Interface	Enable this option to create a tunnel interface.
Carrier	Choose the carrier name or private network identifier to associate with the tunnel. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default Default: default
Color	Choose a color for the TLOC.
Color Description	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enter a description associated to the TLOC color.
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 600000 milliseconds Default: 1000 milliseconds (1 second)

Field	Description
Hello Tolerance	Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down. Range: 12 through 6000 seconds Default: 12 seconds
Last-Resort Circuit	Enable this option to use the tunnel interface as the circuit of last resort.
Restrict	Enable this option to limit the remote TLOCs that the local TLOC can establish BFD sessions with. When a TLOC is marked as restricted, a TLOC on the local router establishes tunnel connections with a remote TLOC only if the remote TLOC has the same color.
Group	Enter a group number. Range: 1 through 4294967295
Border	Enable this option to set the TLOC as a border TLOC.
Maximum Control Connections	Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 100 Default: 2
NAT Refresh Interval	Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds Default: 5 seconds
Validator As Stun Server	Enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the Cisco IOS XE Catalyst SD-WAN device is located behind a NAT.
Exclude Controller Group List	Set the identifiers of one or more Cisco SD-WAN Controller groups that this tunnel is not allowed to connect to. Range: 1 through 100
Manager Connection Preference	Set the preference for using a tunnel interface to exchange control traffic with Cisco SD-WAN Manager. Range: 0 through 8 Default: 5

Field	Description
Full Port Hop	Minimum release: Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled
Port Hop	Enable port hopping. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. Default: Enabled Starting from Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, this field is deprecated. Instead use the **Full Port Hop** option. See the **Full Port Hop** field.
Low-Bandwidth Link	Enable the low-bandwidth feature.
Tunnel TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 500 to 1460 bytes Default: None
Clear-Dont-Fragment	Enable this option to clear the Don't Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than the MTU of the interface are fragmented before being sent.
Network Broadcast	Enable this option to accept and respond to network-prefix-directed broadcasts.

Field	Description
Allow Service	Allow or disallow the following services on the interface: • **All** • **BGP** • **DHCP** • **NTP** • **SSH** • **DNS** • **ICMP** • **HTTPS** • **OSPF** • **STUN** • **SNMP** • **NETCONF** • **BFD**
Encapsulation	
GRE	Use GRE encapsulation on the tunnel interface. By default, GRE is disabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
GRE Preference	Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0
GRE Weight	Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1
IPsec	Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.

Field	Description
IPsec Preference	Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0
IPsec Weight	Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1

d. Configure NAT.

Field	Description
NAT	Enable this option to have the interface act as a NAT device.
UDP Timeout*	Specify when NAT translations over UDP sessions time out. Range: 1 through 8947 minutes Default: 1 minutes
TCP Timeout*	Specify when NAT translations over TCP sessions time out. Range: 1 through 8947 minutes Default: 60 minutes (1 hour)

e. Configure ACL/QoS.

f. Configure the advanced parameters.

Field	Description
MAC Address	Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation.
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 through 9216 Default: 1500 bytes
Interface MTU	Enter the maximum transmission unit size for frames received and transmitted on the interface. Range: 1500 through 9216 Default: 1500 bytes

Field	Description
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 500 to 1460 bytes Default: None
TLOC Extension	Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN. **Note** TLOC extension over L3 is supported only for Cisco IOS XE Catalyst SD-WAN devices. If configuring TLOC extension over L3 for a Cisco IOS XE Catalyst SD-WAN device, enter the IP address of the L3 interface.
Tracker	Tracking the interface status is useful when you enable NAT on a transport interface in VPN 0 to allow data traffic from the router to exit directly to the internet rather than having to first go to a router in a data center. In this situation, enabling NAT on the transport interface splits the TLOC between the local router and the data center into two, with one going to the remote router and the other going to the internet. When you enable transport tunnel tracking, Cisco Catalyst SD-WAN periodically probes the path to the internet to determine whether it is up. If Cisco Catalyst SD-WAN detects that this path is down, it withdraws the route to the internet destination, and traffic destined to the internet is then routed through the data center router. When Cisco Catalyst SD-WAN detects that the path to the internet is again functioning, the route to the internet is reinstalled. Enter the name of a tracker to track the status of transport interfaces that connect to the internet.
IP Directed-Broadcast	An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet. A device that is not directly connected to its destination subnet forwards an IP directed broadcast in the same way it would forward unicast IP packets destined to a host on that subnet. When a directed broadcast packet reaches a device that is directly connected to its destination subnet, that packet is broadcast on the destination subnet. The destination address in the IP header of the packet is rewritten to the configured IP broadcast address for the subnet, and the packet is sent as a link-layer broadcast. If directed broadcast is enabled for an interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which that interface is attached are broadcast on that subnet.

Step 4 Click **Add New Feature** to create and configure a Cellular Controller feature.

Configure the basic parameters, mostly related to SIMs.

Table 156: Basic Settings

Field	Description
Type	Choose a feature from the drop-down list.
Feature Name	Enter a name for the feature. The name can be up to 128 characters and can contain only alphanumeric characters.
Description	Enter a description of the feature. The description can be up to 2048 characters and can contain only alphanumeric characters.
Cellular ID	Enter the interface slot and port number in which the cellular NIM card is installed. Currently, it can be 0/1/0 or 0/2/0.
Primary SIM slot	Enter the number of the primary SIM slot. It can be 0 or 1. The other slot is automatically set to be the secondary. If there is a single SIM slot, this parameter is not applicable.
SIM Failover Retries	Specify the maximum number of times to retry connecting to the secondary SIM when service on the primary SIM becomes unavailable. If there is a single SIM slot, this parameter is not applicable. Range: 0 through 65535 Default: 10
SIM Failover Timeout	Specify how long to wait before switching from the primary SIM to the secondary SIM if service on the primary SIM becomes unavailable. If there is a single SIM slot, this parameter is not applicable. Range: 3 to 7 minutes Default: 3 minutes
Firmware Auto Sim	By default, this option is enabled. AutoSIM analyzes any active SIM card and determines which service provider network is associated with that SIM. Based on that analysis, AutoSIM automatically loads the appropriate firmware.

Step 5 Configure a Cellular Profile feature to associate with the Cellular Controller.

a. Adjacent to the Cellular Controller feature, click + and add a Cellular Profile feature as a subfeature.

b. Configure the basic parameters.

Table 157: Basic Settings

Field	Description
Type	Choose a feature from the drop-down list.
Feature Name	Enter a name for the feature. The name can be up to 128 characters and can contain only alphanumeric characters.

Field	Description
Description	Enter a description of the feature. The description can be up to 2048 characters and can contain only alphanumeric characters.
Profile ID	Enter the identification number of the profile to use on the router. Range: 1 through 15
Access Point Name	Enter the name of the gateway between the service provider network and the public internet. It can be up to 32 characters long.
Authentication	Choose the authentication method used for the connection to the cellular network. It can be **none**, **pap**, **chap**, or **pap_chap**.
Profile Username	Enter the username to use when making cellular connections for web services. It can be 1 to 32 characters. It can contain any alphanumeric characters, including spaces.
Profile Password	Enter the user password to use when making cellular connections for web services. The password is case-sensitive and can be clear text, or an AES-encrypted key. From Cisco Catalyst SD-WAN Manager Release 20.15.1, when you enter the password as clear text, Cisco SD-WAN Manager encrypts the password. When you view the configuration preview, the password appears in its encrypted form.
Packet Data Network Type	Choose the packet data network (PDN) type of the cellular network. It can be IPv4, IPv6, or IPv4v6.
No Overwrite	Enable this option to overwrite the profile on the cellular modem. By default, this option is disabled.
Slot	Enter the associated SIM slot for the profile.

Step 6 If you need to configure specific cellular bands, do this:

a) In the **Cellular Controller** area, click + and choose **Cellular Band Select**.
b) Enable **Cellular Band Select**.
c) Configure the basic parameters.

Table 158: Cellular Band Select

Field	Description
Name	Specify the name of cellular band select.
Description (Optional)	Provide a description for the cellular band select.
Enable Cellular Band Select (Optional)	Enable/Disable cellular band.
All UMTS 3G only	Enable all UMTS3g bands in the cellular modem.
All LTE only	Enable all LTE bands in the cellular modem.

Field	Description
LTE 4G	Specify the LTE indices.
Indices	Enable/Disable cellular band indices.
UMTS 3G	Specify the 3G indices.
NR 5G	Specify the 5G SA indices.
NR 5G NSA	Specify the 5G NSA indices

Note
This sub-feature is applicable to both SD-Routing and SD-WAN modes.

What to do next

Also see Deploy a configuration group.

Configure cellular interfaces using CLI

The following example enables a cellular interface:

Procedure

Use the `interface Cellular` command to enable a cellular interface.

Example:

```
interface Cellular0/2/0
   description Cellular interface
   no shutdown
   ip address negotiated
   ip mtu 1428
   mtu 1500
  exit

  controller Cellular 0/2/0
   lte sim max-retry 1
   lte failovertimer 7
   profile id 1 apn Broadband authentication none pdn-type ipv4
```

Configure cellular interfaces using templates

To configure cellular interfaces using Cisco SD-WAN Manager templates:

1. Create a VPN Interface Cellular feature template to configure cellular module parameters
2. Create a Cellular Profile template to configure the profiles used by the cellular modem.

3. Create a VPN feature template to configure VPN parameters.

If your deployment includes devices with cellular interface, you must include cellular controller templates in Cisco SD-WAN Manager, even if these templates are not used.

If the device has the LTE or cellular controller module configured and the cellular controller feature template does not exist, then the device tries to remove the cellular controller template. For releases earlier than Cisco IOS XE Release 17.4.2, the following error message is displayed.

```
bad-cli - No controller Cellular 0/2/0, parser-context - No controller Cellular 0/2/0,
parser-response % Cannot remove controllers this way
```

For devices running on Cisco IOS XE Release 17.4.2 and later, the device will return an access-denied error message.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**.

In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

Step 3 Click **Add Template**.

Step 4 Select the type of device for which you are creating the template.

Step 5 Click **VPN Interface Cellular**.

Step 6 In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

Step 7 In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down list.

Step 8 Configure cellular interface.

a) Configure basic cellular interface functionality.

Table 159:

Parameter Name	Description
Shutdown*	Click **No** to enable the interface.
Interface Name*	Enter the name of the interface. It must be **cellular0**.
Description	Enter a description of the cellular interface.
DHCP Helper	Enter up to four IP addresses for DHCP servers in the network, separated by commas, to have the interface be a DHCP helper. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers.
Bandwidth Upstream	For transmitted traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32} / 2) – 1 kbps

Parameter Name	Description
Bandwidth Downstream	For received traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32} / 2) – 1 kbps
IP MTU*	Enter 1428 to set the MTU size, in bytes. This value must be 1428. You cannot use a different value.

b) Configure a tunnel interface on the cellular interface to configure an interface in VPN 0 to be a WAN transport connection. The tunnel, which provides security from attacks, is used to send the phone number. At a minimum, select **On** and select a color for the interface. You can generally accept the system defaults for the reminder of the tunnel interface settings.

Parameter Name	Description
Tunnel Interface*	From the drop-down, select **Global**. Click **On** to create a tunnel interface.
Per-tunnel QoS	From the drop-down, select **Global**. Click **On** to create per-tunnel QoS. You can apply a Quality of Service (QoS) policy on individual tunnels, and is only supported for hub-to-spoke network topologies.
Per-tunnel QoS Aggregrator	From the drop-down, select **Global**. Click **On** to create per-tunnel QoS. **Note** 'bandwidth downstream' is required for per-Tunnel QoS feature to take effect as spoke role.
Color*	From the drop-down, select **Global**. Select a color for the TLOC. The color typically used for cellular interface tunnels is **lte**.
Color Description	Minimum supported release: SD-WAN Manager 20.18.1 Enter a description associated to the TLOC color.
Groups	From the drop-down, select **Global**. Enter the list of groups in the field.
Border	From the drop-down, select **Global**. Click **On** to set TLOC as border TLOC.
Maximum Control Connections	Set the maximum number of Cisco SD-WAN Controller that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8 Default: 2
vBond As STUN Server	Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT.
Exclude Control Group List	Set the identifiers of one or more Cisco SD-WAN Controller groups that this tunnel is not allows to establish control connections with. Range: 0 through 100

Parameter Name	Description
vManage Connection Preference	Set the preference for using the tunnel to exchange control traffic with the Cisco SD-WAN Manager. Range: 0 through 9 Default: 5 If the edge device has two or more cellular interfaces, you can minimize the amount of traffic between the Cisco SD-WAN Manager and the cellular interfaces by setting one of the interfaces to be the preferred one to use when sending updates to the Cisco SD-WAN Manager and receiving configurations from the Cisco SD-WAN Manager. To have a tunnel interface never connect to the Cisco SD-WAN Manager, set the number to 0. At least one tunnel interface on the edge device must have a nonzero Cisco SD-WAN Manager connection preference.
Full Port Hop	Minimum release: SD-WAN Manager 20.18.1 Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled
Port Hop	From the drop-down, select **Global**. Click **Off** to allow port hopping on tunnel interface. Default: **On**, which disallows port hopping on tunnel interface. Starting from SD-WAN Manager 20.18.1, this field is deprecated. Instead use the **Full Port Hop** option. See the **Full Port Hop** field.
Low-Bandwidth Link	Click **On** to set the tunnel interface as a low-bandwidth link. Default: **Off**
Tunnel TCP MSS	TCP MSS affects any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS is examined against the MSS exchanged in the three-way handshake. The MSS in the header is lowered if the configured TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. If the TCP MSS is to be configured, it should be set at 40 bytes lower than the minimum path MTU. Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes. Default: None

Parameter Name	Description
Clear-Dont-Fragment	Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent. Click **On** to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, packets larger than the MTU of the interface are fragmented before being sent. **Note** **Clear-Dont-Fragment** clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected.
Network Broadcast	From the drop-down, select **Global**. Click **On** to accept and respond to network-prefix-directed broadcasts. Turn this **On** only if the **Directed Broadcast** is enabled on the LAN interface feature template. Default: **Off**
Allow Service	Click **On** or **Off** for each service to allow or disallow the service on the cellular interface.

To configure additional tunnel interface parameters, click **Advanced Options** and configure the following parameters:

Table 160:

Parameter Name	Description
GRE	From the drop-down, select **Global**. Click **On** to use GRE encapsulation on the tunnel interface. By default, GRE is disabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
GRE Preference	From the drop-down, select **Global**. Enter a value to set GRE preference for TLOC. Range: 0 to 4294967295
GRE Weight	From the drop-down, select **Global**. Enter a value to set GRE weight for TLOC. Default: 1
IPsec	From the drop-down, select **Global**. Click **On**to use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
IPsec Preference	From the drop-down, select **Global**. Enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295. Default: 0

Parameter Name	Description
IPsec Weight	From the drop-down, select **Global**. Enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255. Default: 1
Carrier	From the drop-down, select **Global**. From the **Carrier** drop-down, select the carrier name or private network identifier to associate with the tunnel. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default. Default: default
Bind Loopback Tunnel	Enter the name of a physical interface to bind to a loopback interface. The interface name has the format **ge** *slot*/*port*.
Last-Resort Circuit	From the drop-down, select **Global**. Click **On** to use the tunnel interface as the circuit of last resort. By default, it is disabled. **Note** An interface configured as a circuit of last resort is expected to be down and is skipped while calculating the number of control connections, the cellular modem becomes dormant, and no traffic is sent over the circuit. When the configurations are activated on the edge device with cellular interfaces, then all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down. Only when all the primary interfaces lose their connections to remote edges, then the circuit of last resort activates itself triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are used as backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode the radio interface is turned off, and no control or data connections exist over the cellular interface.
NAT Refresh Interval	Set the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds. Default: 5 seconds.
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 10000 milliseconds. Default: 1000 milliseconds (1 second).

Parameter Name	Description
Hello Tolerance	Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down. Range: 12 through 60 seconds. Default: 12 seconds. The default hello interval is 1000 milliseconds, and it can be a time in the range 100 through 600000 milliseconds (10 minutes). The default hello tolerance is 12 seconds, and it can be a time in the range 12 through 600 seconds (10 minutes). To reduce outgoing control packets on a TLOC, it is recommended that on the tunnel interface you set the hello interval to 60000 milliseconds (10 minutes) and the hello tolerance to 600 seconds (10 minutes) and include the **no track-transport disable** regular checking of the DTLS connection between the edge device and the controller. For a tunnel connection between a edge device and any controller device, the tunnel uses the hello interval and tolerance times configured on the edge device. This choice is made to minimize the traffic sent over the tunnel, to allow for situations where the cost of a link is a function of the amount of traffic traversing the link. The hello interval and tolerance times are chosen separately for each tunnel between a edge device and a controller device. Another step taken to minimize the amount of control plane traffic is to not send or receive OMP control traffic over a cellular interface when other interfaces are available. This behavior is inherent in the software and is not configurable.

c) Configure the cellular interface as a NAT device.

Table 161:

Parameter Name	Description
NAT	Click **On** to have the interface act as a NAT device.
Refresh Mode	Select how NAT mappings are refreshed, either outbound or bidirectional (outbound and inbound). Default: Outbound
UDP Timeout	Specify when NAT translations over UDP sessions time out. Range: 1 through 65536 minutes. Default: 1 minute
TCP Timeout	Specify when NAT translations over TCP sessions time out. Range: 1 through 65536 minutes. Default: 60 minutes (1 hour)
Block ICMP	Select **On** to block inbound ICMP error messages. By default, a router acting as a NAT device receives these error messages. Default: Off
Respond to Ping	Select **On** to have the router respond to ping requests to the NAT interface's IP address that are received from the public side of the connection.

To create a port forwarding rule, click **Add New Port Forwarding Rule** and configure the following parameters. You can define up to 128 port-forwarding rules to allow requests from an external network to reach devices on the internal network.

Table 162:

Parameter Name	Description
Port Start Range	Enter a port number to define the port or first port in the range of interest. Range: 0 through 65535
Port End Range	Enter the same port number to apply port forwarding to a single port, or enter a larger number to apply it to a range of ports. Range: 0 through 65535
Protocol	Select the protocol to which to apply the port-forwarding rule, either TCP or UDP. To match the same ports for both TCP and UDP traffic, configure two rules.
VPN	Specify the private VPN in which the internal server resides. This VPN is one of the VPN identifiers in the overlay network. Range: 0 through 65530
Private IP	Specify the IP address of the internal server to which to direct traffic that matches the port-forwarding rule.

d) Configure a shaping rate to a cellular interface and apply a QoS map, a rewrite rule, access lists, and policers to a router interface.

Table 163: Access Lists Parameters

Parameter Name	Description
Shaping rate	Configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).
QoS map	Specify the name of the QoS map to apply to packets being transmitted out the interface.
Rewrite rule	Click **On**, and specify the name of the rewrite rule to apply on the interface.
Ingress ACL – IPv4	Click **On**, and specify the name of an IPv4 access list to packets being received on the interface.
Egress ACL– IPv4	Click **On**, and specify the name of an IPv4 access list to packets being transmitted on the interface.
Ingress ACL – IPv6	Click **On**, and specify the name of an IPv6 access list to packets being received on the interface.
Egress ACL– IPv6	Click **On**, and specify the name of an IPv6 access list to packets being transmitted on the interface.
Ingress policer	Click **On**, and specify the name of the policer to apply to packets being received on the interface.
Egress policer	Click **On**, and specify the name of the policer to apply to packets being transmitted on the interface.

e) Add ARP table entries.

Table 164:

Parameter Name	Description
IP Address	Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name.
MAC Address	Enter the MAC address in colon-separated hexadecimal notation.

f) Configure other interface properties.

Table 165: Cellular Interfaces Advanced Parameters

Parameter Name	Description
PMTU Discovery	Click **On** to enable path MTU discovery on the interface, to allow the router to determine the largest MTU size supported without requiring packet fragmentation.
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes. Default: None.
Clear-Dont-Fragment	Click **On** to clear the Don't Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent.
Static Ingress QoS	Select a queue number to use for incoming traffic. Range: 0 through 7
Autonegotiate	Click **Off** to turn off autonegotiation. By default, an interface runs in autonegotiation mode.
TLOC Extension	Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.
Tracker	Enter the name of a tracker to track the status of transport interfaces that connect to the internet.
IP Directed-Broadcast	From the drop-down, select **Global**. Click **On** for IP directed-broadcast. Default: **Off**

Step 9 Click **Save**.

Reset the profile configuration of a cellular modem

From Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, when you need to switch from one cellular provider to another, you can reset the cellular modem to clear existing profile configurations and apply new settings using the **cellular** slot **lte profile reset** command.

Resetting the profile configuration of a modem prevents remnants of previous carrier settings (such as Access Point Name (APN) or authentication details) from interfering with new configurations, which is vital for successful network attachment and operation.

Procedure

For routers, use the command with a 3-tuple slot identifier. For cellular gateways, the `slot` variable is 1.

Example:

Routers:

```
CellularGateway# cellular 0/2/0 profile-reset
```

Cellular gateways:

```
CellularGateway# cellular 1 profile-reset
```

Troubleshoot LTE modem crash

In the event that an LTE modem crashes, `crash dump` is the information stored in the device bootflash that:

- makes troubleshooting easier by appearing in the admin-tech file
- helps diagnose the cause of the crash

When enabled, this command instructs the device to automatically collect a crash dump from the LTE modem upon a crash event. This dump contains various diagnostic logs and memory states that are essential for analyzing why the modem crashed.

Before you begin

Ensure that the device has sufficient bootflash storage available to accommodate the large amount of data collected.

Procedure

Use the **lte modem crash-action auto-collect** command to automatically gather and store detailed operational data in the event of an LTE modem crash.

What to do next

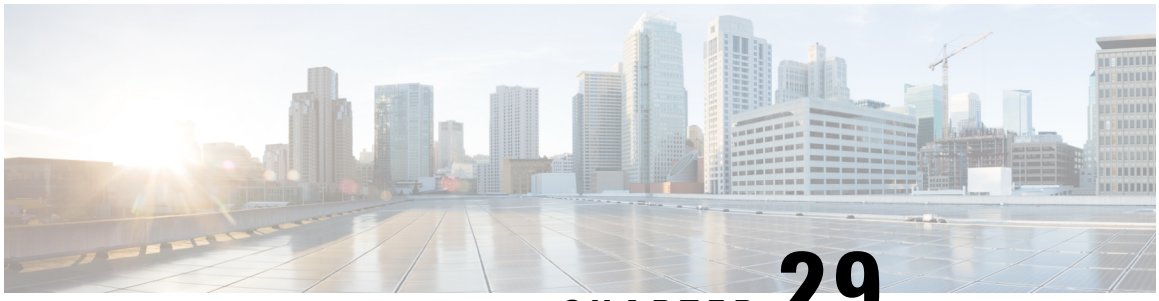
Use the following command to verify the crash-dump progress.

```
Device#show cellular 0/2/0 logs modem-crashdump
Modem crashdump logging = off
Device#
```

When a crash-dump is in progress, it is displayed as follows:

```
Router#show cellular 0/3/0 logs modem-crashdump
Modem crashdump logging = on
Progress = 44%
Router#
Router#show cellular 0/3/0 logs modem-crashdump
Modem crashdump logging = on
Progress = 98%
Router#show cellular 0/3/0 logs modem-crashdump
Modem crashdump logging = off
```

Once the collection is complete, the status will return to off.



CHAPTER 29

VRRP Interface Tracking

- Feature history for VRRP interface tracking, on page 531
- VRRP, on page 532
- Restrictions for VRRP interface tracking, on page 533
- VRRP tracking use cases, on page 533
- Configure VRRP, on page 534
- Configure VRRP tracking using CLI templates, on page 542
- Configure VRRP tracking, on page 544
- Monitor VRRP configuration, on page 546
- Verify VRRP tracking, on page 547

Feature history for VRRP interface tracking

Table 166: Feature History

Feature Name	Release Information	Description
Support for Multiple VRRP Groups on the Same LAN Interface or Sub-interface	Cisco SD-WAN Release 20.3.1	This feature increases support from one VRRP group per interface to five VRRP groups per interface. Multiple VRRP groups are useful for providing redundancy and for load balancing.

Feature Name	Release Information	Description
VRRP interface tracking for Cisco IOS XE Catalyst SD-WAN devices	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco SD-WAN Release 20.7.1	This feature enables VRRP to set the Cisco IOS XE Catalyst SD-WAN device as active or standby based on the WAN Interface or SIG tracker events. It increases the TLOC preference value on a new VRRP active device to ensure traffic symmetry. From this release, you can configure VRRP interface tracking using the Cisco SD-WAN Manager feature template and the CLI template on Cisco IOS XE Catalyst SD-WAN devices.

VRRP

A Virtual Router Redundancy Protocol (VRRP) is a LAN-side protocol that

- provides redundant gateway service for switches and IP end stations,
- allows configuration on interfaces and subinterfaces using templates, and
- supports failover and election of a new primary router based on interface state, OMP session, or remote prefix reachability.

In Cisco Catalyst SD-WAN, VRRP is configured on service-side VPN interfaces or subinterfaces (excluding reserved VPNs 0 and 512), with each group identified by a unique number and assigned an IP address.

The protocol enables up to 512 groups per router, with priority values determining primary router election. Failover can be triggered by interface status, three consecutive advertisements missed, OMP session loss, or loss of prefix reachability, ensuring continuous gateway service.

For VRRP to function with IEEE 802.1Q tagging, MTU adjustments may be necessary.

This is not applicable from Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and later, where physical and subinterfaces can share the same MTU.

- If the primary VRRP goes down, traffic is redirected to the secondary VRRP, which then becomes the primary gateway.
- VRRP is configured per interface or subinterface within a service-side VPN; reserved VPNs (0, 512) are not supported except for physical interface configuration.
- Each VRRP group requires a unique group number and IP address, with a maximum of 512 groups per router.
- Routers in the same VRRP group act as a single virtual router; the router with the highest priority (1–254, default 100) becomes primary.
- Advertisement messages are sent by the primary every 1–3600 seconds (default: every second).

- The x710 NIC must have the `t->system-> vrrp-advt-with-phymac` command configured, for VRRP to function.

Restrictions for VRRP interface tracking

- Use VRRP only with service-side VPNs.
- Configure VRRP physical interfaces with VPN 0 when you use subinterfaces.
- Enable VRRP tracking only on a physical uplink interface or a logical tunnel interface (IPSEC, GRE, or both).
- Do not use IP prefix as an object for the VRRP Tracking feature.
- Apply the same tracker to multiple VRRP groups or VPNs.
- Do not track multiple VRRP interfaces using the same track object.
- Group a maximum of 16 track objects under a list track object.
- Do not configure **tloc-change** or **increase-preference** on more than one VRRP group.

VRRP tracking use cases

The VRRP state is determined based on the tunnel link status. If the tunnel or interface is down on the primary VRRP, then the traffic is directed to the secondary VRRP. The secondary VRRP router in the LAN segment becomes primary VRRP to provide gateway for the service-side traffic.

Zscaler Tunnel Use Case 1—Primary VRRP, Single Internet Provider

The primary and secondary Zscaler tunnels are connected through a single internet provider to the primary VRRP. The primary and secondary VRRP routers are connected using TLOC extension. In this scenario, the VRRP state transitions occurs if the primary and secondary tunnels go down on the primary VRRP. The predetermined priority value decrements when the tracking object is down, which triggers the VRRP state transition. To avoid asymmetric routing, VRRP notifies this change to the Overlay through OMP.

Zscaler Tunnel Use Case 2—VRRP Routers in TLOC Extension, Dual Internet Providers

The primary and secondary VRRP routers are configured in TLOC extension high availability mode. The primary and secondary Zscaler tunnels are directly connected with primary and secondary VRRP routers, respectively, using dual internet providers. In this scenario too, the VRRP state transition occurs if the primary and secondary tunnels go down on the primary VRRP. The predetermined priority value decrements when the tracking object is down, which triggers the VRRP state transition. VRRP notifies this change to the overlay through OMP.

TLOC Preference

Transport Locators (TLOCs) connect an OMP route to a physical location. A TLOC is directly reachable using an entry in the routing table of the physical network, or represented by a prefix beyond a NAT device.

In Cisco IOS XE Catalyst SD-WAN devices, the TLOC change increase preference value increases based on the configured value. You can configure the TLOC change increase preference value on both the active and the backup nodes.

Configure VRRP

- Configure VRRP using Cisco Catalyst SD-WAN Manager
- Configure a prefix list for VRRP using configuration groups
- Configure a prefix list for VRRP using a feature template
- Configure a prefix list for VRRP using a device template
- Configure VRRP using CLI commands

Configuring VRRP using Cisco Catalyst SD-WAN Manager

Procedure

To have an interface run the Virtual Router Redundancy Protocol (VRRP), which allows multiple routers to share a common virtual IP address for default gateway redundancy, select the VRRP tab. Then click **Add New VRRP** and configure the following parameters:

Parameter Name	Description
Group ID	Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups. Range: 1 through 255
Priority	Enter the priority level of the router. There router with the highest priority is elected as primary VRRP router. If two routers have the same priority, the one with the higher IP address is elected as primary VRRP router. Range: 1 through 254 Default: 100
Timer (milliseconds)	Specify how often the primary VRRP router sends VRRP advertisement messages. If subordinate routers miss three consecutive VRRP advertisements, they elect a new primary VRRP routers. Range: 100 through 40950 milliseconds Default: 100 msecs **Note** When the timer is 100 ms for the VRRP feature template on Cisco IOS XE Catalyst SD-WAN devices, the VRRP fails if the traffic is high on LAN interface.

Parameter Name	Description
Track OMP Track Prefix List	By default, VRRP uses of the state of the service (LAN) interface on which it is running to determine which router is the primary virtual router. if a router loses all its WAN control connections, the LAN interface still indicates that it is up even though the router is functionally unable to participate in VRRP. To take WAN side connectivity into account for VRRP, configure one of the following: **Track OMP**: Click **On** for VRRP to track the Overlay Management Protocol (OMP) session running on the WAN connection. If the primary VRRP router loses all its OMP sessions, VRRP elects a new default gateway from those that have at least one active OMP session. **Note** From Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, enabling **Track OMP** changes the device CLI command from **vrrp track omp shutdown** to **vrrp track omp decrement 10** . **Track Prefix List**: Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the primary VRRP router loses all its OMP sessions, VRRP failover occurs as described for the Track OMP option. In addition, if reachability to all of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic is dropped while the routers determine the primary VRRP router.
IP Address	Enter the IP address of the virtual router. This address must be different from the configured interface IP addresses of both the local router and the peer running VRRP.

Configure a prefix list for VRRP using Configuration Groups

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure Prefix List for VRRP in a Policy Object Profile.

a) Choose the **Prefix** policy object from the **Select Policy Object** drop-down list.
b) Enter the **Prefix List Name**.
c) In the **Internet Protocol field**, click **IPv4** or **IPv6**.
d) Under **Add Prefix**, enter the prefix for the list. Optionally, click the **Choose a file** link to import a prefix list.
e) Click **Save** The following table describe the options for configuring the prefix.

Table 167: Prefix List

Field	Description
Prefix List Name	Enter a name for the prefix list.

Field	Description
Internet Protocol	Specifies the internet protocol. The options are IPv4 and IPv6.

What to do next

Also see Deploy a configuration group.

Configure a prefix list for VRRP using a feature template

To configure a prefix list,

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy** > **Localized Policy**.

Step 2 From the **Custom Options** drop-down list, click **Lists**.

a) Click **Prefix** from the left pane, and click **New Prefix List**.
b) In **Prefix List Name,** enter a name for the prefix list.
c) Choose **IPv4** as the **Internet Protocol**.
d) In **Add Prefix**, enter the prefix entries separated by commas.
e) Click **Add**.

Step 3 Click **Next** and configure **Forwarding Classes/QoS**.

Step 4 Click **Next** and configure **Access Control Lists**.

Step 5 Click **Next** and in **Route Policy** pane, select a relevant route policy and click **…** , and click **Edit** to add the newly added prefix list.

Step 6 From the **Match** pane, click **AS Path List** and in the **Address**, choose the newly added prefix list.

Step 7 Click **Save Match and Actions**.

Step 8 Click **Next** and enter the **Policy Name** and **Policy Description** in the **Policy Overview** screen.

Step 9 Click **Save Policy**.

Configure a prefix list for VRRP using a device template

To configure the Prefix List to the VRRP using a device template,

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Device Templates**.

In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

Step 2 Select a relevant device template and click **…**, then click **Edit** to edit the template details.

Step 3 From **Policy**, select the policy with the newly added prefix list and click **Update**.

Step 4 Click **Feature Templates**.

Step 5 Select a relevant device template and click **…** and click **Edit** to edit the template details.

Step 6 Click **VRRP**.

Step 7 Select a relevant group ID and click the pen icon to associate the new prefix-list to the VRRP details and click the **Track Prefix List** drop-down to enter the newly added prefix-list name.

Step 8 Click **Save Changes** and then **Update**. Click **Device Templates** and select the policy with the newly added prefix list.

Step 9 Click **…** and click **Attach Devices**. From **Available Devices,** double-click the relevant device to move it to **Selected Devices**, and then click **Attach**.

Configure VRRP using CLI commands

To provide redundant gateway service on Cisco Catalyst SD-WAN devices by configuring VRRP on service-side interfaces using CLI commands.

Before you begin

- VRRP must be configured on service-side VPNs (not on VPN 0 or 512, except for the physical interface when using subinterfaces).
- Ensure required interfaces and subinterfaces are created and enabled.
- Adjust MTU for 802.1Q tagging if needed (not required for Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and later).

Procedure

Step 1 Enter the target VPN .

Example:

```
vpn <vpn-id>
```

Step 2 Select and enable the interface (or subinterface). Select and enable the interface (or subinterface).

Example:

```
interface <irbnumber>[.<subinterface>]
no shutdown
```

Step 3 Assign an IP address to the interface.

Example:

```
ipv4 ip-address
```

Step 4 Within each VRRP group, the router with the higher priority value is elected as primary VRRP. By default, each virtual router IP address has a default primary election priority of 100, so the router with the higher IP address is elected as primary. You can modify the priority value, setting it to a value from 1 through 254.

Example:

```
priority number
```

Step 5 The primary VRRP periodically sends advertisement messages, indicating that it is still operating. If backup routers miss three consecutive VRRP advertisements, they assume that the primary VRRP is down and elect a new primary VRRP. By default, these messages are sent every second. You can change the VRRP advertisement time to be a value from 1 through 3600 seconds.

Example:

```
timer seconds
```

Step 6 By default, VRRP uses the state of the interface on which it is running, to determine which router is the primary virtual router. This interface is on the service (LAN) side of the router. When the interface for the primary VRRP goes down, a new primary VRRP virtual router is elected based on the VRRP priority value. Because VRRP runs on a LAN interface, if a router loses all its WAN control connections, the LAN interface still indicates that it is up even though the router is functionally unable to participate in VRRP. To take WAN side connectivity into account for VRRP, you can configure one of the following:

a) Track the Overlay Management Protocol (OMP) session running on the WAN connection when determining the primary VRRP virtual router.

Example:

```
track-omp
```

If all OMP sessions are lost on the primary VRRP router, VRRP elects a new default gateway from among all the gateways that have one or more active OMP sessions even if the gateway chosen has a lower VRRP priority than the current primary VRRP router. With this option, VRRP failover occurs once the OMP state changes from up to down, which occurs when the OMP hold timer expires. Until the hold timer expires and a new primary VRRP is elected, all overlay traffic is dropped. When the OMP session recovers, the local VRRP interface claims itself as primary VRRP even before it learns and installs OMP routes from the Cisco Catalyst SD-WAN Controllers. Until the routers are learned, traffic is also dropped.

b) Track both the OMP session and a list of remote prefixes. *list-name* is the name of a prefix list configured with the policy lists **prefix-list** command on the Cisco vEdge device :

Example:

```
track-prefix-list list-name
```

If all OMP sessions are lost, VRRP failover occurs as described for the **track-omp**option. In addition, if reachability to all the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic is dropped while the router determines the primary VRRP.

As discussed above, the IEEE 802.1Q protocol adds 4 bytes to each packet's length. Hence, for packets to be transmitted, either increase the MTU size on the physical interface in VPN 0 (the default MTU is 1500 bytes) or decrease the MTU size on the VRRP interface.

For devices running on Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and later, adjusting the MTU size is not required, both the physical interface and sub interface can have the same MTU size.

Here is an example of configuring VRRP on redundant physical interfaces. For subinterface 2, vEdge1 is configured to act as the primary VRRP, and for subinterface 3, vEdge2 acts as the primary VRRP.

```
vEdge1# show running-config vpn 1
vpn 1
```

```
 interface ge0/6.2
  ip address 10.2.2.3/24
  mtu      1496
  no shutdown
  vrrp 2
   ipv4 10.2.2.1
   track-prefix-list vrrp-prefix-list1
  !
 !
 interface ge0/6.3
  ip address 10.2.3.5/24
  mtu      1496
  shutdown
  vrrp 3
   ipv4 10.2.3.11
   track-prefix-list vrrp-prefix-list1
  !
 !
!

vEdge2# show running-config vpn 1
vpn 1
 interface ge0/1.2
  ip address 10.2.2.4/24
  mtu      1496
  no shutdown
  vrrp 2
   ipv4 10.2.2.1
   track-prefix-list vrrp-prefix-list2
  !
 !
 interface ge0/1.3
  ip address 10.2.3.6/24
  mtu      1496
  no shutdown
  vrrp 3
   ipv4 10.2.3.11
   track-prefix-list vrrp-prefix-list2
  !
 !
!

vEdge1# show interface vpn 1

                             IF      IF
          TCP
                            ADMIN   OPER    ENCAP  PORT                              SPEED
         MSS                  RX       TX
VPN  INTERFACE  IP ADDRESS   STATUS  STATUS  TYPE   TYPE     MTU   HWADDR             MBPS
   DUPLEX  ADJUST  UPTIME      PACKETS  PACKETS
-------------------------------------------------------------------------------------------
1    ge0/6.2    10.2.2.3/24  Up      Up      vlan   service  1496  00:0c:29:ab:b7:94  10
   full    0       0:00:05:52  0        357
1    ge0/6.3    10.2.3.5/24  Down    Down    vlan   service  1496  00:0c:29:ab:b7:94  -
   -       0       -           0        0

vEdge1# show vrrp interfaces


 MASTER                              TRACK   PREFIX
              GROUP  VIRTUAL                                VRRP    OMP    ADVERTISEMENT
 DOWN                                PREFIX  LIST
VPN  IF NAME  ID     IP          VIRTUAL MAC        PRIORITY  STATE   STATE  TIMER
 TIMER   LAST STATE CHANGE TIME     LIST    STATE
```

```
1    ge0/6.2  2      10.2.2.1   00:0c:29:ab:b7:94  100       master  down   1
 3       2015-05-01T20:09:37+00:00  -       -
     ge0/6.3  3      10.2.3.11  00:00:00:00:00:00  100       init    down   1
 3       0000-00-00T00:00:00+00:00  -       -
```

In the following example, Router-1 is the primary VRRP, because it has a higher priority value than Router 2:

```
Router-1# show running-config vpn 1
vpn 1
!
 interface ge0/1.15
  ip address 10.10.1.2/24
  mtu         1496
  no shutdown
  vrrp 15
   priority  110
   track-omp
   ipv4 10.20.23.1
  !
 !
!

Router-1# show vrrp vpn 1

      MASTER                                TRACK   PREFIX
               GROUP                                                VRRP    OMP    ADVERTISEMENT
  DOWN                                    PREFIX  LIST
VPN  IF NAME   ID     VIRTUAL IP     VIRTUAL MAC        PRIORITY  STATE   STATE  TIMER
      TIMER   LAST STATE CHANGE TIME     LIST    STATE
-------------------------------------------------------------------------------------------
1    ge0/1.1   1      10.20.22.1     00:0c:bd:08:79:a4  100       backup  up     1
      3       2016-01-13T03:10:55+00:00  -       -
     ge0/1.5   5      10.20.22.193   00:0c:bd:08:79:a4  100       backup  up     1
      3       2016-01-13T03:10:55+00:00  -       -
     ge0/1.10  10     10.20.22.225   00:0c:bd:08:79:a4  100       backup  up     1
      3       2016-01-13T03:10:55+00:00  -       -
     ge0/1.15  15     10.20.23.1     00:0c:bd:08:79:a4  110       master  up     1
      3       2016-01-13T03:10:56+00:00  -       -
     ge0/1.20  20     10.20.24.1     00:0c:bd:08:79:a4  100       backup  up     1
      3       2016-01-13T03:10:56+00:00  -       -
     ge0/1.25  25     10.20.25.1     00:0c:bd:08:79:a4  110       master  up     1
      3       2016-01-13T03:10:56+00:00  -       -
     ge0/1.30  30     10.20.25.129   00:0c:bd:08:79:a4  100       backup  up     1
      3       2016-01-13T03:10:56+00:00  -       -


Router-1# show vrrp vpn 1 interfaces ge0/1.15 groups 15

                                                                                  MASTER
                        TRACK   PREFIX
GROUP                                          VRRP    OMP    ADVERTISEMENT  DOWN
                        PREFIX  LIST
ID     VIRTUAL IP   VIRTUAL MAC        PRIORITY  STATE   STATE  TIMER          TIMER   LAST
 STATE CHANGE TIME     LIST    STATE
-------------------------------------------------------------------------------------------
1      10.20.33.1  00:0c:bd:08:79:a4  110       master  up     1              3
2016-01-13T03:10:56+00:00  -       -

Router-2# show running-config vpn 1
vpn 1
!
 interface ge0/1.15
```

```
  ip address 10.10.1.3/24
  mtu         1496
  no shutdown
  vrrp 15
   track-omp
   ipv4 10.20.23.1
  !
 !
!

Router-2# show vrrp vpn 1 interfaces groups


 MASTER                              TRACK   PREFIX
          GROUP                                                VRRP    OMP    ADVERTISEMENT
 DOWN                                PREFIX  LIST
IF NAME    ID     VIRTUAL IP     VIRTUAL MAC        PRIORITY  STATE   STATE  TIMER
 TIMER    LAST STATE CHANGE TIME     LIST    STATE
-------------------------------------------------------------------------------------------
ge0/1.1    1      10.20.32.1     00:0c:bd:08:2b:a5  110       master  up     1
 3       2016-01-13T00:22:15+00:00  -       -
ge0/1.5    5      10.20.32.193   00:0c:bd:08:2b:a5  110       master  up     1
 3       2016-01-13T00:22:15+00:00  -       -
ge0/1.10   10     10.20.32.225   00:0c:bd:08:2b:a5  110       master  up     1
 3       2016-01-13T00:22:15+00:00  -       -
ge0/1.15   15     10.20.33.1     00:0c:bd:08:2b:a5  100       backup  up     1
 3       2016-01-13T03:10:56+00:00  -       -
ge0/1.20   20     10.20.34.1     00:0c:bd:08:2b:a5  110       master  up     1
 3       2016-01-13T00:22:16+00:00  -       -
ge0/1.25   25     10.20.35.1     00:0c:bd:08:2b:a5  100       backup  up     1
 3       2016-01-13T03:10:56+00:00  -       -
ge0/1.30   30     10.20.35.129   00:0c:bd:08:2b:a5  100       master  up     1
 3       2016-01-13T00:22:16+00:00  -       -

Router-2# show vrrp vpn 100 interfaces groups 15


MASTER                              TRACK   PREFIX
          GROUP                                                VRRP    OMP    ADVERTISEMENT
DOWN                                PREFIX  LIST
IF NAME    ID     VIRTUAL IP     VIRTUAL MAC        PRIORITY  STATE   STATE  TIMER
TIMER    LAST STATE CHANGE TIME     LIST    STATE
-------------------------------------------------------------------------------------------
ge0/0.15   15     10.20.33.1     00:0c:bd:08:2b:a5  100       backup  up     1              3
       2016-01-13T03:10:56+00:00  -       -
```

Cisco SD-WAN supports configuring multiple VRRP groups on an interface. A use case for configuring this is where primary and secondary IP addresses have been assigned to a single interface. On one interface, you can configure:

- One primary IP address
- Up to four secondary IP addresses

To support each of these IP addresses, you can configure up to 5 VRRP groups (each with a unique group ID) on an interface, subinterface, or integrated routing and bridging (IRB) interface that supports VRRP groups.

The following is an example of configuring 5 VRRP groups on 1 interface.

```
vpn 2
 interface ge0/4.2
  ip address 10.0.1.10/24
```

```
  ip secondary-address 10.0.2.10/24
  ip secondary-address 10.0.3.10/24
  ip secondary-address 10.0.4.10/24
  mtu 1496
  no shutdown
  vrrp 1
   priority 101
    ipv4 10.0.1.1
!
  vrrp 2
   ipv4 10.0.1.2
!
  vrrp 3
   priority 101
    ipv4 10.0.2.1
!
  vrrp 4
   ipv4 10.0.3.1
!
  vrrp 5
   ipv4 10.0.4.1
  !
 !
!
```

Configure VRRP tracking using CLI templates

You can configure VRRP tracking using the CLI add-on feature templates and CLI device templates. For more information, see CLI Templates.

- VRRP object tracking using CLI
- SIG container tracking

VRRP object tracking using CLI

Procedure

Use the following configuration to add an interface to a track list using the Cisco SD-WAN Manager device CLI template:

```
Device(config)# track <object-id1> interface <interface-type-number> [line-protocol]
Device(config-tracker)# exit
Device(config)# track < object-id2> interface <interface-type-number> [line-protocol]
Device(config-tracker)# exit
Device(config)# track <group-object-id> list boolean [and | Or]
Device(config-tracker)# object <object-id1>
Device(config-tracker)# object <object-id2>
Device(config-tracker)# exit
Device(config)# interface GigabitEthernet2


Device(config-if)# vrf forwarding <vrf-number>

Device(config-if)# ipv4 address <ip-address> <subnet-mask>
Device(config-if)# negotiation auto
```

```
Device(config-if)# vrrp <vrrp-number> address-family ipv4
Device(config-if-vrrp)# address <ipv4-address> [primary | secondary]
Device(config-if-vrrp)# track <object-id> [decrement <dec-value> | shutdown]
Device(config-if-vrrp)# tloc-change increase-preference <value>
Device(config-if-vrrp)# exit
```

Example:

Interface Object Tracking Using CLI

```
config-transaction
  track 100 interface Tunnel123 line-protocol
   exit
 track 200 interface GigabitEthernet5 line-protocol
  exit
track 400 list boolean and
  object 100
  object 200
  exit

interface GigabitEthernet2
 vrf forwarding 1
 ip address 10.10.1.1 255.255.255.0
 negotiation auto
vrrp 1 address-family ipv4
  address 10.10.1.10 primary
  track 400 decrement 10
  tloc-change increase-preference 333
  exit
```

SIG container tracking

Procedure

Use the following example to configure a track list and tracking for SIG containers using the Cisco SD-WAN Manager device CLI template.

```
Device(config)# track <object-id1> service global

Device(config-tracker)# exit
Device(config)# track <object-id2> service global
Device(config-tracker)# exit
Device(config)# track <group-object-id> list boolean [and | Or]
Device(config-tracker)# object <object-id1>
Device(config-tracker)# object <object-id2>
Device(config-tracker)# exit

Device(config)# interface GigabitEthernet2

Device(config-if)# vrf forwarding <vrf-number>

Device(config-if)# ip address <ip-address> <subnet-mask>
Device(config-if)# negotiation auto
Device(config-if)# vrrp <vrrp-number> address-family ipv4
Device(config-if-vrrp)# address <ipv4-address> [primary | secondary]
Device(config-if-vrrp)# track <object-id> [decrement <dec-value> | shutdown]
Device(config-if-vrrp)# tloc-change increase-preference <value>
Device(config-if-vrrp)#exit
```

Example:

SIG Object Tracking Using CLI

```
config-transaction
  track 1 service global
  exit
  exit
  track 2 service global
track 3 list boolean and
  object 1
  object 2
  exit

interface GigabitEthernet2
 vrf forwarding 1
 ip address 10.10.1.1 255.255.255.0
 negotiation auto
vrrp 1 address-family ipv4
  address 10.10.1.10 primary
  track 3 decrement 10
  tloc-change increase-preference 333
  exit
```

Configure VRRP tracking

1. Configure an object tracker using a feature template.
2. Configure VRRP for a VPN Interface template and associate the object tracker with the template.

Configure an object tracker using a feature template

Use the **Cisco System** template to configure an object tracker.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **ConfigurationTemplates**.

Step 2 Click **Feature Templates**.

Note
In Cisco SD-WAN Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

Step 3 Navigate to the **Cisco System** template for the device.

Step 4 Click **Tracker** and choose **New Object Tracker** to configure the tracker parameters.

Table 168: Tracker Parameters

Field	Description
Tracker Type	Choose **Interface** or **SIG** or **Route** to configure the object tracker.
Object ID	Enter the object ID number.
Interface	Choose global or device-specific tracker interface name.
Route IP	Enter the IP route prefix to track the state of an IP route.
Route IP Mask	Enter the prefix mask.
VPN	Enter the VPN number.

Step 5 Click **Add**.

Step 6 Optionally, to create a tracker group, click **Tracker**, and click **Tracker Groups** > **New Object Tracker Groups** to configure the tracker parameters.

Note
Ensure that you have created two trackers to create a track group.

Table 169: Object Tracker Group Parameters

Field	Description
Group Tracker ID	Enter the name of the tracker group.
Tracker ID	Enter the name of the object tracker that you want to group.
Criteria	Choose **AND** or **OR** explicitly. **OR** ensures that the transport interface status is reported as active if either one of the associated trackers of the tracker group reports that the route is active. If you choose **AND** operation, the transport interface status is reported as active if both the associated trackers of the tracker group report that the route is active.

Note
Provide information in all the mandatory fields before you save the template.

Step 7 Click **Add**.

Step 8 Click **Save**.

Configure VRRP for a VPN interface template and associate interface object tracker

To configure VRRP for a **Cisco VPN** template, do the following:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** .

Step 2 Click **Feature Templates**.

Note
In Cisco SD-WAN Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

Step 3 Navigate to the **Cisco VPN Interface Ethernet** template for the device.

Note
For information about creating a new **Cisco VPN Interface Ethernet** template, see *Configure VPN Ethernet Interface*.

Step 4 Click **VRRP** and choose **IPv4**.

Step 5 Click **New VRRP** to create a new VRRP or edit the existing VRRP and configure the following parameters:

Parameter Name	Description
TLOC Preference Change	(Optional) Choose **On** or **Off** to set whether the TLOC preference can be changed or not.
TLOC Preference Change Value	(Optional) Enter the TLOC preference change. Range: 1 to 4294967295.

Step 6 Click the **Add Tracking Object** link, and in the **Tracking Object** dialog box that is displayed, click **Add Tracking Object**.

Step 7 In the **Tracker ID** field, enter the Interface Object ID or Object Group Tracker ID.

Step 8 From the **Action** drop-down list, choose **Decrement** and enter the **Decrement Value** as 1. Cisco vEdge Devices support decrement value of 1.

Or

Choose **Shutdown**

Step 9 Click **Add** to save the VRRP details, then click **Save** to save the configuration.

Monitor VRRP configuration

To view information about VRRP configuration:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

For Cisco SD-WAN Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

Step 2 Choose a device from the list of devices.

Step 3 Click **Real Time**.

Step 4 From the **Device Options** drop-down list, choose **VRRP Information**.

Note
You can view the status of the VRRP configuration in **Track State**.

Verify VRRP tracking

View the summary of the VRRP configuration

The following is a sample output for the **show vrrp** command:

```
Device# show vrrp
GigabitEthernet2 - Group 1 - Address-Family IPv4
State is MASTER
State duration 37 mins 52.978 secs
Virtual IP address is 10.10.1.10
Virtual MAC address is 0000.5E00.0101
Advertisement interval is 1000 msec
Preemption enabled
Priority is 100
State change reason is VRRP_TRACK_UP
Tloc preference configured, value 333
Track object 400 state UP decrement 10
Master Router is 10.10.1.1 (local), priority is 100
Master Advertisement interval is 1000 msec (expires in 607 msec)
Master Down interval is unknown
FLAGS: 1/1
```

View the summary of tracked objects

The following is a sample output for the **show track brief** command:

```
Device# show track brief
Track Type      Instance           Parameter     State      Last Change
100   interface Tunnel123 l        line-protocol Up         00:12:48
200   interface GigabitEthernet5   line-protocol Up         00:49:57
400   list                         boolean       Up         00:12:47
```

View the state of the tracked list

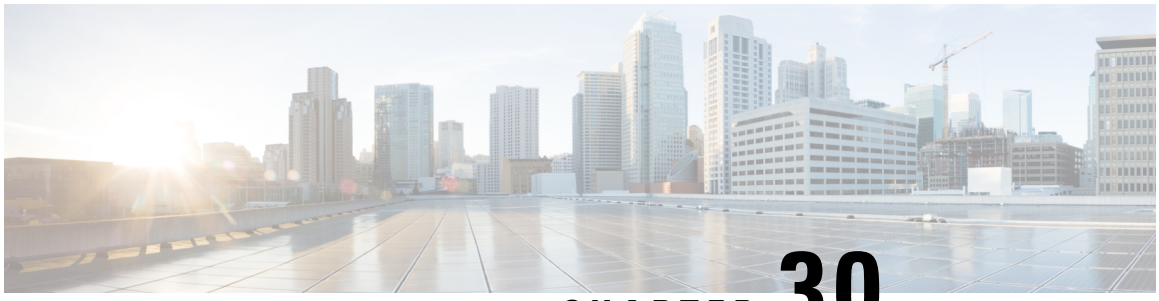
The following is a sample output for the **show track list** command:

```
Device# show track list
Track 400
  List boolean and
  Boolean AND is Up
    6 changes, last change 00:12:58
    object 100 Up
    object 200 Up
  Tracked by:
    VRRPv3 GigabitEthernet2 IPv4 group 1
```

View a brief summary state of the tracked list

The following is a sample output for the **show track list brief** command:

```
Track  Type        Instance        Parameter        State  Last Change
         400    list                          boolean          Up    00:13:02
```



CHAPTER 30

VPN Interface Bridge

• Configure VPN interface bridge, on page 549

Configure VPN interface bridge

To configure a bridge interface using Cisco SD-WAN Manager templates:

1. Create a VPN Interface Bridge feature template to configure parameters for logical IRB interfaces.
2. Create a Bridge feature template for each bridging domain, to configure the bridging domain parameters.

Integrated routing and bridging (IRB) allows Cisco IOS XE Catalyst SD-WAN devices in different bridge domains to communicate with each other. To enable IRB, create logical IRB interfaces to connect a bridge domain to a VPN. The VPN provides the Layer 3 routing services necessary so that traffic can be exchanged between different VLANs. Each bridge domain can have a single IRB interface and can connect to a single VPN, and a single VPN can connect to multiple bridge domains on a Cisco IOS XE Catalyst SD-WAN device.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Device Templates**.

In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

a) From the **Create Template** drop-down list, select **From Feature Template**.
b) From the **Device Model** drop-down list, select the type of device for which you are creating the template.
c) Click **Service VPN** or scroll to the **Service VPN** section.
d) Click the **Service VPN** drop-down list.
e) From **Additional VPN Templates**, click **VPN Interface Bridge**.
f) From the **VPN Interface Bridge** drop-down list, click **Create Template**.

The VPN Interface Bridge template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface Bridge parameters.

g) In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

h) In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

Step 3 Configure an interface to use for bridging servers.

Table 170:

Parameter Name	Description
Shutdown*	Click **No** to enable the interface.
Interface name*	Enter the name of the interface, in the format **irb** *number*. The IRB interface number can be from 1 through 63, and must be the same as the VPN identifier configured in the Bridge feature template for the bridging domain that the IRB is connected to.
Description	Enter a description for the interface.
IPv4 Address*	Enter the IPv4 address of the router.
DHCP Helper	Enter up to eight IP addresses for DHCP servers in the network, separated by commas, to have the interface be a DHCP helper. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers.
Block Non-Source IP	Click **Yes** to have the interface forward traffic only if the source IP address of the traffic matches the interface's IP prefix range.
Secondary IP Address (on Cisco IOS XE Catalyst SD-WAN devices)	Click **Add** to configure up to four secondary IPv4 addresses for a service-side interface.

Step 4 Apply access lists to IRB interfaces, select the ACL tab and configure the following parameters. The ACL filter determines what is allowed in or out of a bridging domain.

Table 171:

Parameter Name	Description
Ingress ACL – IPv4	Click **On**, and specify the name of an IPv4 access list to packets being received on the interface.
Egress ACL– IPv4	Click **On**, and specify the name of an IPv4 access list to packets being transmitted on the interface.

Step 5 To have an interface run the Virtual Router Redundancy Protocol (VRRP), which allows multiple routers to share a common virtual IP address for default gateway redundancy, choose **VRRP**. Then click **Add New VRRP** and configure the following parameters:

Table 172:

Parameter Name	Description
Group ID	Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups. Range: 1 through 255

Parameter Name	Description
Priority	Enter the priority level of the router. There router with the highest priority is elected as primary VRRP router. If two Cisco IOS XE Catalyst SD-WAN devices have the same priority, the one with the higher IP address is elected as primary VRRP router. Range: 1 through 254 Default: 100
Timer (milliseconds)	Specify how often the primary VRRP router sends VRRP advertisement messages. If subordinate routers miss three consecutive VRRP advertisements, they elect a new primary VRRP router. Range: 100 through 40950 milliseconds Default: 1000 msecs **Note** When the timer is 100 ms for the VRRP feature template on Cisco IOS XE Catalyst SD-WAN devices, the VRRP fails if the traffic is high on LAN interface. Use the 100 msec timer only if the Cisco IOS XE Catalyst SD-WAN device platform supports it, and if there are fewer tunnel groups.
Track OMP Track Prefix List	By default, VRRP uses of the state of the service (LAN) interface on which it is running to determine which Cisco IOS XE Catalyst SD-WAN device is the primary virtual router. if a Cisco IOS XE Catalyst SD-WAN device loses all its WAN control connections, the LAN interface still indicates that it is up even though the router is functionally unable to participate in VRRP. To take WAN side connectivity into account for VRRP, configure one of the following: Track OMP—Click **On** for VRRP to track the Overlay Management Protocol (OMP) session running on the WAN connection. If the primary VRRP router loses all its OMP sessions, VRRP elects a new default gateway from those that have at least one active OMP session. Track Prefix List—Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the primary VRRP router loses all its OMP sessions, VRRP failover occurs as described for the Track OMP option. In addition, if reachability to all of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic is dropped while the Cisco IOS XE Catalyst SD-WAN devices determine the primary VRRP router.
IP Address	Enter the IP address of the virtual router. This address must be different from the configured interface IP addresses of both the local Cisco IOS XE Catalyst SD-WAN device and the peer running VRRP.

Step 6 Configure static Address Resolution Protocol (ARP) table entries on the interface.

Table 173:

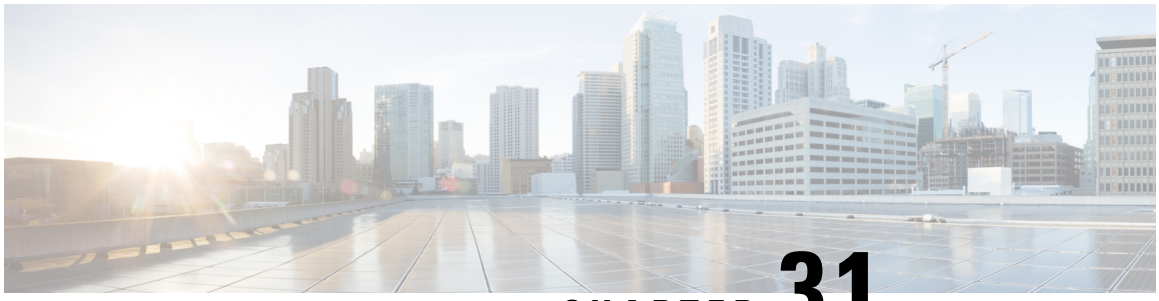
Parameter Name	Description
IP Address	Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name.
MAC Address	Enter the MAC address in colon-separated hexadecimal notation.

Step 7 Configure other interface properties.

Table 174:

Parameter Name	Description
MAC Address	MAC addresses can be static or dynamic. A static MAC address is manually configured as opposed to a dynamic MAC address that is one learned via an ARP request. You can configure a static MAC on a router's interface or indicate a static MAC that identifies a router's interface. Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation.
IP MTU	Similar to MTU, IP MTU only affects IP packets. If an IP packet exceeds the IP MTU, then the packet will be fragmented. Specify the maximum MTU size of packets on the interface. Range: 576 through 1804 Default: 1500 bytes
TCP MSS	TCP MSS will affect any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS will be examined against the MSS exchanged in the three-way handshake. The MSS in the header will be lowered if the configured setting is lower than what is in the header. If the header value is already lower, it will flow through unmodified. The end hosts will use the lower setting of the two hosts. If the TCP MSS is to be configured, it should be set it at 40 bytes lower than the minimum path MTU. Specify the maximum segment size (MSS) of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes Default: None
Clear-Dont-Fragment	Configure Clear-Dont-Fragment if there are packets arriving on an interface with the DF bit set. If these packets are larger than the MTU will allow, they are dropped. If you clear the df-bit, the packets will be fragmented and sent. Click **On** to clear the Dont Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent. **Note** Clear-Dont-Fragment clears the DF bit when there is fragmentation needed and the DF bit is set. For packets not requiring fragmentation, the DF bit is not affected.
ARP Timeout	ARP Timeout controls how long we maintain the ARP cache on a router. Specify how long it takes for a dynamically learned ARP entry to time out. Range: 0 through 2678400 seconds (744 hours) Default: 1200 seconds (20 minutes)

Parameter Name	Description
ICMP Redirect	ICMP Redirects are sent by a router to the sender of an IP packet when a packet is being routed sub-optimally. The ICMP Redirect informs the sending host to forward subsequent packets to that same destination through a different gateway. To disable ICMP redirect messages on the interface, click **Disable**. By default, an interface allows ICMP redirect messages.



CHAPTER 31

DSL IPoE

- Configure DSL IPoE, on page 555

Configure DSL IPoE

Guides the configuration of DSL IPoE, detailing step-by-step procedures for using configuration groups and templates to deploy and manage broadband access efficiently.

Use one of these methods to configure DSL IPoE:

- Configuration group
- Feature template

Configure DSL IPoE using a configuration group

Follow these steps to configure DSL IPoE using a configuration group.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure the DSL IPoE parameters in a Transport and Management Profile.

a. Configure basic configuration.

Table 175: Basic Configuration

Parameter Name	Description
Controller Slot*	Enter the slot number of the controller, in the following format: *slot*/*subslot*/*port* (for example, 0/2/0)

Parameter Name	Description
Controller Mode	Select the operating mode of the DSL controller from the drop-down list: • **ADSL1**: Use ITU G.992.1 Annex A full-rate mode, which provides a downstream rate of 1.3 Mbps and an upstream rate of 1.8 Mbps. • **ADSL2**: Use ITU G.992.3 Annex A, Annex L, and Annex M, which provides a downstream rate of 12 Mbps and an upstream rate of 1.3 Mbps. • **ADSL2+**: Use ITU G.992.5 Annex A and Annex M, which provides a downstream rate of 24 Mbps and an upstream rate of 3.3 Mbps. • **ANSI**: Operating in ADSL2/2+ mode, as defined in ITU G.991.1, G.992.3, and G992.5, Annex A and Annex M, and in VDSL2 mode, as defined in ITU-T G993.2. • **VDSL2**: Operate in VDSL2 mode, as defined in ITU-T G.993.2, which uses frequencies of up to 30 MHz to provide a downstream rate of 200 Mbps and an upstream rate of 100 Mbps.
SRA	Enabled by default. Click **No** to disable seamless rate adaptation on the interface. SRA adjusts the line rate based on current line conditions.

b. Configure Ethernet.

Table 176: Ethernet

Parameter Name	Description
Ethernet Interface Name *	Enter the name of an ethernet interface. For IOS XE routers, you must spell out the interface names completely (for example, **GigabitEthernet0/0/0**).
Description	Enter a description for the interface.
VLAN ID	Enter the VLAN identifier of the Ethernet interface.

c. Configure Tunnel.

Table 177: Tunnel

Parameter Name	Description
Tunnel Interface	
Per Tunnel QoS	Enable per tunnel QoS and choose from the following values to configure hub-to-spoke network topologies: • **Spoke** • **Hub**
Color	Select a color for the TLOC.

Parameter Name	Description
Color Description	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enter a description associated to the TLOC color.
Groups	Enter the list of groups in the field.
Exclude Controller Group List	Set the Cisco SD-WAN Controllers that the tunnel interface is not allowed to connect to. Range: 0 through 100
Maximum Control Connections	Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8 Default: 2
Cisco SD-WAN Manager Connection Preference	Set the preference for using a tunnel interface to exchange control traffic with Cisco SD-WAN Manager. Range: 0 through 8 Default: 5
Tunnel TCP MSS	TCP MSS affects any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS is examined against the MSS exchanged in the three-way handshake. The MSS in the header is lowered if the configured TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. To configure TCP MSS, provide a value that is 40 bytes lower than the minimum path MTU. Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: None
Border	From the drop-down list, select **Global**. Click **On** to set TLOC as border TLOC.
Validator As Stun Server	Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT.
Full Port Hop	Minimum release: Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled
Port Hop	From the drop-down list, select **Global**. Click **Off** to allow port hopping on tunnel interface. Default: **On**, which disallows port hopping on tunnel interface. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, this field is deprecated. Instead use the **Full Port Hop** option. See the **Full Port Hop** field.

Parameter Name	Description
Low-Bandwidth Link	Click **On** to set the tunnel interface as a low-bandwidth link. Default: **Off**
Clear-Dont-Fragment	Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent. Click **On** to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, the router fragments packets larger than the MTU of the interface before sending the packets. **Note** **Clear-Dont-Fragment** clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected.
Network Broadcast	From the drop-down list, select **Global**. Click **On** to accept and respond to network-prefix-directed broadcasts. Enable this parameter only if the **Directed Broadcast** is enabled on the LAN interface feature template. Default: **Off**
Carrier	From the drop-down list, select **Global**and select the carrier name or private network identifier to associate with the tunnel. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default. Default: default
Bind Loopback Tunnel	Enter the name of a physical interface to bind to a loopback interface. The interface name has the following format: **ge** *slot*/*port*
NAT Refresh Interval	Set the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds Default: 5 seconds
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 10000 milliseconds Default: 1000 milliseconds (1 second)

Parameter Name	Description
Hello Tolerance	Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down. Range: 12 through 60 seconds. Default: 12 seconds. The default hello interval is 1000 milliseconds, and it can be a time in the range 100 through 600000 milliseconds (10 minutes). The default hello tolerance is 12 seconds, and it can be a time in the range 12 through 600 seconds (10 minutes). To reduce outgoing control packets on a TLOC, it is recommended that on the tunnel interface you set the hello interval to 60000 milliseconds (10 minutes) and the hello tolerance to 600 seconds (10 minutes) and include the **no track-transport disable** regular checking of the DTLS connection between the edge device and the controller. For a tunnel connection between a edge device and any controller device, the tunnel uses the hello interval and tolerance times configured on the edge device. This choice is made to minimize the traffic sent over the tunnel, to allow for situations where the cost of a link is a function of the amount of traffic traversing the link. The hello interval and tolerance times are chosen separately for each tunnel between a edge device and a controller device. Another step taken to minimize the amount of control plane traffic is to not send or receive OMP control traffic over a cellular interface when other interfaces are available. This behavior is inherent in the software and is not configurable.
Last Resort Circuit	Select to use the tunnel interface as the circuit of last resort. **Note** It is assumed that an interface configured as a circuit of last resort is unavailable and is skipped while calculating the number of control connections. As a result, the cellular modem becomes dormant, and no traffic is sent over the circuit. When the configurations are activated on the edge device with cellular interfaces, all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down. If the primary interfaces lose their connections to remote edges, the circuit of last resort activates itself, triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are a backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode, the radio interface is turned off, and no control or data connections exist over the cellular interface.
Allow Services	Click **On** or **Off** for each service to enable or disable the service on the cellular interface.
Encapsulation	

Parameter Name	Description
Encapsulation	Enable atleast one of the following encapsulation methods: • **IPsec**: Enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 • **IPsec Preference**: From the drop-down list, select **Global** and enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 • **IPsec Weight**: From the drop-down list, select **Global** and enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1 • **GRE**: Enter a value to set GRE preference for TLOC. Range: 0 through 4294967295 • **GRE Preference**: From the drop-down list, select **Global** and enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 • **GRE Weight**: From the drop-down list, select **Global** and enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1

d. Configure NAT.

Table 178: NAT

Parameter Name	Description
UDP Timeout (Minutes)	Specify when NAT translations over UDP sessions time out. Range: 1 through 65536 minutes Default: 1 minute

Parameter Name	Description
TCP Timeout (Minutes)	Specify when NAT translations over TCP sessions time out. Range: 1 through 65536 minutes Default: 60 minutes (1 hour)

e. Configure QoS.

Table 179: QoS

Parameter Name	Description
Adaptive QoS	Enter adaptive QoS parameters. You can leave the additional details at as default or specify your values. • **Adapt Period (Minutes)**: Choose **Global** from the drop-down list, click **On**, and enter the period in minutes. • **Shaping Rate Upstream**: Choose **Global** from the drop-down list, click **On**, and enter the minimum, maximum, and default upstream bandwidth in Kbps. • **Shaping Rate Downstream**: Choose **Global** from the drop-down list, click **On**, and enter the minimum, maximum, downstream, and upstream bandwidth in Kbps.
Shaping Rate (kbps)	Choose **Global** from the drop-down list and configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps). Range: 8 through 100000000

f. Configure ACL.

Table 180: ACL

Parameter Name	Description
IPv4 Ingress Access List	Enter the name of an IPv4 access list to packets being received on the interface.
IPv4 Egress Access List	Enter the name of an IPv4 access list to packets being transmitted on the interface.
IPv6 Ingress Access List	Enter the name of an IPv6 access list to packets being received on the interface.
IPv6 Egress Access List	Enter the name of an IPv6 access list to packets being transmitted on the interface.

g. Configure advanced parameters.

Table 181: Advanced

Parameter Name	Description
Shutdown	Click **No** to enable the interface.

Parameter Name	Description
Tracker / Tracker Group	Enter the name of a tracker or tracker group to track the status of transport interfaces that connect to the internet.
Service Provider	Specify the details of the service provider.
Bandwidth Upstream (Kbps)	Specify the bandwidth value to generate notifications when the bandwidth of traffic transmitted on a physical interface exceeds the value.
Bandwidth Downstream (Kbps)	Specify the bandwidth value to generate notifications when the bandwidth of traffic transmitted on a physical interface exceeds the value.
IP MTU	Enter the maximum MTU size of packets on the interface. Range: 576 through 1804 Default: 1500
TCP MSS	Enter the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: 1500
TLOC Extension	Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration binds the service-side interface to the WAN transport by enabling a device to access the opposite WAN transport connected to the neighbouring device using a TLOC-extension interface.
IP Directed Broadcast	From the drop-down list, select **Global** to enable IP Directed Broadcast. An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet.

What to do next

Also see *Deploy a configuration group*.

Configure DSL IPoE using templates

Follow these steps to configure DSL IPoE using a feature template.

You configure IPoE on routers with DSL interfaces, to provide support for service provider digital subscriber line (DSL) functionality.

To configure DSL interfaces on Cisco IOS XE Catalyst SD-WAN devices using Cisco SD-WAN Manager templates:

1. Create a VPN Interface DSL IPoE feature template to configure IP-over-Ethernet interface parameters, as described in this article.
2. Create a VPN feature template to configure VPN parameters. See the VPN help topic.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Device Templates**, and click **Create Template**.

In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

a) From the **Create Template** drop-down list, choose **From Feature Template**.
b) From the **Device Model** drop-down list, select the type of device for which you are creating the template.
c) Click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.
d) Under **Additional VPN 0 Templates**, click **VPN Interface DSL IPoE**.
e) From the **VPN Interface DSL IPoE** drop-down list, choose **Create Template**. The **VPN Interface DSL IPoE** template form is displayed.

This form contains fields for naming the template, fields for defining the IPoE Interface parameters. 

In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

Step 3 Configure the basic IPoE functionality.

Table 182:

Parameter Name	Description
Shutdown*	Click **No** to enable the VDSL controller interface.
Controller VDSL Slot*	Enter the slot number of the controller VDSL interface, in the format *slot*/*subslot*/*port* (for example, 0/2/0).

Parameter Name	Description
Mode*	Select the operating mode of the VDSL controller from the drop-down: • Auto—Default mode. • ADSL1—Use ITU G.992.1 Annex A full-rate mode, which provides a downstream rate of 1.3 Mbps and an upstream rate of 1.8 Mbps. • ADSL2—Use ITU G.992.3 Annex A, Annex L, and Annex M, which provides a downstream rate of 12 Mbps and an upstream rate of 1.3 Mbps. • ADSL2+— Use ITU G.992.5 Annex A and Annex M, which provides a downstream rate of 24 Mbps and an upstream rate of 3.3 Mbps. • ANSI—Operating in ADSL2/2+ mode, as defined in ITU G.991.1, G.992.3, and G992.5, Annex A and Annex M, and in VDSL2 mode, as defined in ITU-T G993.2. • VDSL2—Operate in VDSL2 mode, as defined in ITU-T G.993.2, which uses frequencies of up to 30 MHz to provide a downstream rate of 200 Mbps and an upstream rate of 100 Mbps..
VDSL Modem Configuration	Enter a command to send to the DSL modem in the NIM module. If the command is valid, it is executed and the results are returned to the Cisco SD-WAN Manager NMS. If the command is not valid, it is not executed.
SRA	Click **Yes** to enable seamless rate adaptation on the interface. SRA adjusts the line rate based on current line conditions.

Step 4 Configure an Ethernet interface on the VDSL controller.

Table 183:

Parameter Name	Description
Ethernet Interface Name	Enter a name for the Ethernet interface, in the format *subslot*/*port* (for example 2/0). You do not need to enter the slot number, because it must always be 0.
VLAN ID	Enter the VLAN identifier of the Ethernet interface.
Description	Enter a description for the interface.
Dynamic/Static	Assign a dynamic or static IPv4 address to the Ethernet interface.
IPv4 Address	Enter the static IPv4 address of the Ethernet interface.
DHCP Helper	Enter up to eight IP addresses for DHCP servers in the network, separated by commas, to have the interface be a DHCP helper. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers.

Step 5 Configure a tunnel interface for the multilink interface.

Table 184:

Parameter Name	Description
Tunnel Interface	Click **On** to create a tunnel interface.
Color	Select a color for the TLOC.
Color Description	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.x Enter a description associated to the TLOC color.
Control Connection	By default, Control Conection is set to **On**, which establishes a control connection for the TLOC. If the router has multiple TLOCs, click **No** to have the tunnel not establish control connection for the TLOC. **Note** We recommend a minimum of 650-700 Kbps bandwidth with default 10 msec hello-interval and 12 sec hello-tolerance parameters configured to avoid any data/packet loss in connection traffic. For each BFD session, an additional average sized BFD packet of 175 Bytes consumes 1.4 Kbps of bandwidth. A sample calculation of the required bandwidth for bidirectional BFD packet flow is given below: • 650 – 700 Kbps per device for control connections. • 175 Bytes (or 1.4 Kbps) per BFD session on the device (request) • 175 Bytes (or 1.4 Kbps) per BFD session on the device (response) If the path MTU discovery (PMTUD) is enabled, bandwidth for send/receive BFD packets per tunnel for every 30 secs: A 1500 Bytes BFD request packet is sent per tunnel every 30 secs: 1500 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 400 bps (request) A 147 Bytes BFD packet is sent in response: 147 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 40 bps (response) Therefore, a device with 775 BFD sessions (for example) requires a bandwidth of: 700k + (1.4k*775) + (400 *775) + (1.4k*775) + (40 *775) = ~3,5 MBps
Maximum Control Connections	Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8. Default: 2
Cisco SD-WAN Validator As STUN Server	Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT.

Parameter Name	Description
Exclude Controller Group List	Set the Cisco SD-WAN Controllers that the tunnel interface is not allowed to connect to. Range: 0 through 100
Cisco SD-WAN Manager Connection Preference	Set the preference for using a tunnel interface to exchange control traffic with the Cisco SD-WAN Manager NMS. Range: 0 through 8. Default: 5
Full Port Hop	Minimum release: Cisco Catalyst SD-WAN Manager Release 20.18.x Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled
Port Hop	Click **On** to enable port hopping, or click Off to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. Default: Enabled Starting from Cisco Catalyst SD-WAN Manager Release 20.18.x, this field is deprecated. Instead use the **Full Port Hop** option. See the **Full Port Hop** field.
Low-Bandwidth Link	Select to characterize the tunnel interface as a low-bandwidth link.
TCP MSS	TCP MSS affects any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS is examined against the MSS exchanged in the three-way handshake. The MSS in the header is lowered if the configured TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. If the TCP MSS is to be configured, it should be set at 40 bytes lower than the minimum path MTU. Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes Default: None

Parameter Name	Description
Clear-Dont-Fragment	Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent. Click **On** to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, packets larger than the MTU of the interface are fragmented before being sent. **Note** **Clear-Dont-Fragment** clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected.
Allow Service	Choose **On** or **Off** for each service to allow or disallow the service on the interface.

To configure additional tunnel interface parameters, click **Advanced Options** and configure the following parameters:

Table 185:

Parameter Name	Description
GRE	Use GRE encapsulation on the tunnel interface. By default, GRE is disabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
IPsec	Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
IPsec Preference	Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0
IPsec Weight	Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1
Carrier	Select the carrier name or private network identifier to associate with the tunnel. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default Default: default
Bind Loopback Tunnel	Enter the name of a physical interface to bind to a loopback interface.

Parameter Name	Description
Last-Resort Circuit	Select to use the tunnel interface as the circuit of last resort. **Note** An interface configured as a circuit of last resort is expected to be down and is skipped while calculating the number of control connections, the cellular modem becomes dormant, and no traffic is sent over the circuit. When the configurations are activated on the edge device with cellular interfaces, then all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down. Only when all the primary interfaces lose their connections to remote edges, then the circuit of last resort activates itself triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are used as backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode the radio interface is turned off, and no control or data connections exist over the cellular interface.
NAT Refresh Interval	Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds Default: 5 seconds
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 10000 milliseconds Default: 1000 milliseconds (1 second)
Hello Tolerance	Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down. Range: 12 through 60 seconds Default: 12 seconds

Step 6 Configure an interface to act as a NAT device for applications such as port forwarding.

Table 186:

Parameter Name	Description
NAT	Click **On** to have the interface act as a NAT device.
Refresh Mode	Select how NAT mappings are refreshed, either outbound or bidirectional (outbound and inbound). Default: Outbound
UDP Timeout	Specify when NAT translations over UDP sessions time out. Range: 1 through 65536 minutes Default: 1 minutes

TCP Timeout	Specify when NAT translations over TCP sessions time out. Range: 1 through 65536 minutes Default: 60 minutes (1 hour)
Block ICMP	Select **On** to block inbound ICMP error messages. By default, a router acting as a NAT device receives these error messages. Default: Off
Respond to Ping	Select **On** to have the router respond to ping requests to the NAT interface's IP address that are received from the public side of the connection.

To create a port forwarding rule, click **Add New Port Forwarding Rule** and configure the following parameters. You can define up to 128 port-forwarding rules to allow requests from an external network to reach devices on the internal network.

Table 187:

Parameter Name	Description
Port Start Range	Enter a port number to define the port or first port in the range of interest. Range: 0 through 65535
Port End Range	Enter the same port number to apply port forwarding to a single port, or enter a larger number to apply it to a range of ports. Range: 0 through 65535
Protocol	Select the protocol to which to apply the port-forwarding rule, either TCP or UDP. To match the same ports for both TCP and UDP traffic, configure two rules.
VPN	Specify the private VPN in which the internal server resides. This VPN is one of the VPN identifiers in the overlay network. Range: 0 through 65527
Private IP	Specify the IP address of the internal server to which to direct traffic that matches the port-forwarding rule.

Step 7 Configure ACLs to selectively indicate what traffic will enjoy the benefits of QoS

Table 188:

Parameter Name	Description
Shaping rate	Configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).
QoS map	Specify the name of the QoS map to apply to packets being transmitted out the interface.
Rewrite Rule	Click **On**, and specify the name of the rewrite rule to apply on the interface.

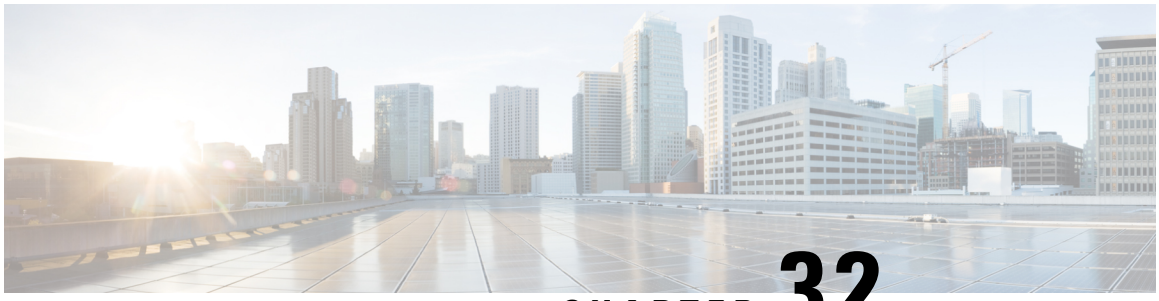
Parameter Name	Description
Ingress ACL – IPv4	Click **On**, and specify the name of the access list to apply to IPv4 packets being received on the interface.
Egress ACL – IPv4	Click **On**, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface.
Ingress ACL – IPv6	Click **On**, and specify the name of the access list to apply to IPv6 packets being received on the interface.
Egress ACL – IPv6	Click **On**, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface.
Ingress Policer	Click **On**, and specify the name of the policer to apply to packets being received on the interface.
Egress Policer	Click **On**, and specify the name of the policer to apply to packets being transmitted on the interface.

Step 8 Configure other interface properties.

Table 189:

Parameter Name	Description
Bandwidth Upstream	When the bandwidth of traffic transmitted on a physical interface in the WAN transport VPN (VPN 0) exceeds a specific limit by 85 percent (on Cisco IOS XE Catalyst SD-WAN devices and Cisco SD-WAN Manager NMSs only), BW Uptream issues notifications. For transmitted traffic, set the bandwidth above which to generate notifications. Range: 1 through $(2^{32} / 2) – 1$ kbps
Bandwidth Downstream	When the bandwidth of traffic received on a physical interface in the WAN transport VPN (VPN 0) exceeds a specific limit by 85 percent (on Cisco IOS XE Catalyst SD-WAN devices and Cisco SD-WAN Manager NMSs only), BW Downtream issues notifications. For received traffic, set the bandwidth above which to generate notifications. Range: 1 through $(2^{32} / 2) – 1$ kbps
IP MTU	IP MTU affects IP packets. If an IP packet exceeds the IP MTU, then the packet will be fragmented. Specify the maximum MTU size of packets on the interface. Range: 576 through 1804 Default: 1500 bytes

Parameter Name	Description
TCP MSS	In a single TCP/IPv4 datagram, the TCP Maximum Segment Size (MSS) defines the maximum data that a host will accept. This TCP/IPv4 datagram might be fragmented at the IPv4 layer. The MSS value is sent as a TCP header option only in TCP SYN segments. Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes Default: None
TLOC Extension	Use a TLOC Extension to bind an interface and connect another Cisco IOS XE Catalyst SD-WAN device at the same physical site to the local router's WAN transport interface (on Cisco IOS XE Catalyst SD-WAN devices only). Enter the name of the physical interface on the same router that connects to the WAN transport circuit. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.
Tracker	Tracking the interface status is useful when you enable NAT on a transport interface in VPN 0 to allow data traffic from the router to exit directly to the internet rather than having to first go to a router in a data center. In this situation, enabling NAT on the transport interface splits the TLOC between the local router and the data center into two, with one going to the remote router and the other going to the internet. When you enable transport tunnel tracking, the software periodically probes the path to the internet to determine whether it is up. If the software detects that this path is down, it withdraws the route to the internet destination, and traffic destined to the internet is then routed through the data center router. When the software detects that the path to the internet is again functioning, the route to the internet is reinstalled. Enter the name of a tracker to track the status of transport interfaces that connect to the internet.
IP Directed-Broadcast	An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet. A device that is not directly connected to its destination subnet forwards an IP directed broadcast in the same way it would forward unicast IP packets destined to a host on that subnet. When a directed broadcast packet reaches a device that is directly connected to its destination subnet, that packet is broadcast on the destination subnet. The destination address in the IP header of the packet is rewritten to the configured IP broadcast address for the subnet, and the packet is sent as a link-layer broadcast. If directed broadcast is enabled for an interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which that interface is attached are broadcast on that subnet.



CHAPTER 32

DSL PPPoA

- Configure DSL PPPoA, on page 573

Configure DSL PPPoA

Outlines configuration procedures for DSL PPPoA, offering task-based guidance to set up PPPoA using configuration groups and templates to streamline deployment and management.

Use one of these methods to configure DSL PPPoA:

- Configuration group
- Feature template

Configure DSL PPPoA using a configuration group

Follow these steps to configure DSL PPPoA using a configuration group.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure the DSL PPPoA parameters in a Transport and Management Profile.

a. Configure basic configuration.

Table 190: Basic Configuration

Parameter Name	Description
Controller Slot*	Enter the slot number of the DSL controller, in the following format: *slot*/*subslot*/*port* (for example, 0/2/0)

Parameter Name	Description
Controller Mode	Select the operating mode of the DSL controller from the drop-down list: • **ADSL1**: Use ITU G.992.1 Annex A full-rate mode, which provides a downstream rate of 1.3 Mbps and an upstream rate of 1.8 Mbps. • **ADSL2**: Use ITU G.992.3 Annex A, Annex L, and Annex M, which provides a downstream rate of 12 Mbps and an upstream rate of 1.3 Mbps. • **ADSL2+**: Use ITU G.992.5 Annex A and Annex M, which provides a downstream rate of 24 Mbps and an upstream rate of 3.3 Mbps. • **ANSI**: Operating in ADSL2/2+ mode, as defined in ITU G.991.1, G.992.3, and G992.5, Annex A and Annex M, and in VDSL2 mode, as defined in ITU-T G993.2. • **VDSL2**: Operate in VDSL2 mode, as defined in ITU-T G.993.2, which uses frequencies of up to 30 MHz to provide a downstream rate of 200 Mbps and an upstream rate of 100 Mbps.
SRA	Disabled by default. Enable SRA to disable seamless rate adaptation on the interface. SRA adjusts the line rate based on current line conditions.
Dialer Pool Member*	Enter the number of the dialer pool to which the interface belongs. Range: 1 through 255

b. Configure ATM.

Table 191: ATM

Parameter Name	Description
ATM Sub Interface Name*	The ATM Sub interface name is auto populated based on the controller slot. Enter a value for the ATM sub interface, in the format *subslot*/*port* (for example ATM0/2/0.100). In this example, ".100" is the sub interface value.
Sub Interface Description	Enter a description for the interface.
VPI/VCI*	Create an ATM permanent virtual circuit (PVC), in the following format: *vpi*/*vci* Enter values for the virtual path identifier (VPI) and the virtual channel identifier (VCI).
Encapsulation	Select the encapsulation type to use on the ATM PVC from the drop-down list: • AAL5 NLPID: Use NLPID multiplexing. • AAL5 SNAP: Multiplex two or more protocols on the same PVC. • AAL5 MUX: Dedicate the PVC to a single protocol.
PVC Mode	

Parameter Name	Description
VBR-NRT	Configure variable bit rate non-real-time parameters: • Peak Cell Rate: Enter a value from 48 through 1015 Kbps. • Sustainable Cell Rate: Enter the sustainable cell rate, in Kbps. • Maximum Burst Size: This size can be 1 through 65535.
VBR-RT	Configure variable bit rate real-time parameters: • Peak Cell Rate: Enter a value from 48 through 25000 Kbps. • Average Cell Rate: Enter the average cell rate, in Kpbs. • Maximum Burst Size: This size can be 1 through 65535.
None	Don't configure variable bit rate parameters

c. Configure PPP.

Table 192: PPP

Parameter Name	Description
PPP Authentication Protocol	Select the authentication protocol used by the MLP: • **PAP**: Enter the username and password that are provided by your ISP. *username* can be up to 254 characters. • **CHAP**: Enter the hostname and password provided by your Internet Service Provider (ISP). *hostname* can be up to 254 characters. • **PAP** and **CHAP**: Configure both authentication protocols. Enter the login credentials for each protocol.
Authentication Type	Select the type authentication from one of the following options.: • **Unidirectional**: Only the side receiving the call (NAS) authenticates the remote side (client). The remote client does not authenticate the server. • **Bidirectional**: Each side independently sends an Authenticate-Request (AUTH-REQ) and receives either an Authenticate-Acknowledge (AUTH-ACK) or Authenticate-Not Acknowledged (AUTH-NAK).
CHAP Hostname*	Enter the CHAP hostname.
CHAP Password*	Enter the CHAP password.
PAP Hostname*	Enter the PAP hostname.
PAP Password*	Enter the PAP password.

d. Configure Tunnel.

Table 193: Tunnel

Parameter Name	Description
Tunnel Interface	
Per Tunnel QoS	Enable per tunnel QoS and choose from the following values to configure hub-to-spoke network topologies: • **Spoke** • **Hub** If you select hub topology, the following option appears: • **Bandwidth Percentage**: Enter a value for the bandwidth percentage. Default: 50
Color	Choose a color for the TLOC.
Color Description	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enter a description associated to the TLOC color.
Groups	Enter the list of groups in the field.
Exclude Controller Group List	Set the Cisco SD-WAN Controllers that the tunnel interface is not allowed to connect to. Range: 0 through 100
Maximum Control Connections	Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8 Default: 2
Cisco SD-WAN Manager Connection Preference	Set the preference for using a tunnel interface to exchange control traffic with Cisco SD-WAN Manager. Range: 0 through 8 Default: 5
Tunnel TCP MSS	TCP MSS affects any packet containing an initial TCP header that flows through the router. When configured, TCP MSS is examined against the MSS exchanged in the three-way handshake. The MSS in the header is lowered if the configured TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. To configure TCP MSS, provide a value that is 40 bytes lower than the minimum path MTU. Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes

Parameter Name	Description
Border	From the drop-down list, select **Global**. Click **On** to set TLOC as border TLOC.
Validator As Stun Server	Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT.
Full Port Hop	Minimum release: Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled
Port Hop	From the drop-down list, select **Global**. Click **Off** to allow port hopping on tunnel interface. Default: **On**, which disallows port hopping on a tunnel interface Starting from Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, this field is deprecated. Instead use the **Full Port Hop** option. See the **Full Port Hop** field.
Low-Bandwidth Link	Click **On** to set the tunnel interface as a low-bandwidth link. Default: **Off**
Clear-Dont-Fragment	Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent. Click **On** to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, the router fragments packets larger than the MTU of the interface before sending the packets. the router fragments packets larger than the MTU of the interface before sending the packets. **Note** **Clear-Dont-Fragment** clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected.
Network Broadcast	From the drop-down list, select **Global**. Click **On** to accept and respond to network-prefix-directed broadcasts. Enable this parameter only if the **Directed Broadcast** is enabled on the LAN interface feature template. Default: **Off**
Carrier	From the drop-down list, select **Global** and select the carrier name or private network identifier to associate with the tunnel. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default. Default: default
Bind Loopback Tunnel	Enter the name of a physical interface to bind to a loopback interface. The interface name has the following format: **ge** *slot*/*port*

Parameter Name	Description
NAT Refresh Interval	Set the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds Default: 5 seconds
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 10000 milliseconds Default: 1000 milliseconds (1 second)
Hello Tolerance	Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down. Range: 12 through 60 seconds Default: 12 seconds The default hello interval is 1000 milliseconds, and it can be a time in the range 100 through 600000 milliseconds (10 minutes). The default hello tolerance is 12 seconds, and it can be a time in the range 12 through 600 seconds (10 minutes). To reduce outgoing control packets on a TLOC, it is recommended that on the tunnel interface you set the hello interval to 60000 milliseconds (10 minutes) and the hello tolerance to 600 seconds (10 minutes) and include the **no track-transport disable** regular checking of the DTLS connection between the edge device and the controller. For a tunnel connection between a edge device and any controller device, the tunnel uses the hello interval and tolerance times configured on the edge device. This choice is made to minimize the traffic sent over the tunnel, to allow for situations where the cost of a link is a function of the amount of traffic traversing the link. The hello interval and tolerance times are chosen separately for each tunnel between a edge device and a controller device. Another step taken to minimize the amount of control plane traffic is to not send or receive OMP control traffic over a cellular interface when other interfaces are available. This behavior is inherent in the software and is not configurable.
Last Resort Circuit	Select to use the tunnel interface as the circuit of last resort. **Note** It is assumed that an interface configured as a circuit of last resort is unavailable and is skipped while calculating the number of control connections. As a result, the cellular modem becomes dormant, and no traffic is sent over the circuit. When the configurations are activated on the edge device with cellular interfaces, all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down. If the primary interfaces lose their connections to remote edges, the circuit of last resort activates itself, triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are a backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode, the radio interface is turned off, and no control or data connections exist over the cellular interface.
Allow Services	Click **On** or **Off** for each service to anable or disable the service on the cellular interface.

Parameter Name	Description
Encapsulation	
Encapsulation	Enable at least one of the following encapsulation methods: • **IPsec**: Enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 • **IPsec Preference**: From the drop-down list, select **Global** and enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 • **IPsec Weight**: From the drop-down list, select **Global** and enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1 • **GRE**: Enter a value to set GRE preference for TLOC. Range: 0 through 4294967295 • **GRE Preference**: From the drop-down list, select **Global** and enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 • **GRE Weight**: From the drop-down list, select **Global** and enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1

e. Configure NAT.

Table 194: NAT

Parameter Name	Description
UDP Timeout (Minutes)	Specify when NAT translations over UDP sessions time out. Range: 1 through 8947 minutes Default: 1 minute
TCP Timeout (Minutes)	Specify when NAT translations over TCP sessions time out. Range: 1 through 8947 minutes Default: 60 minutes (1 hour)

f. Configure QoS.

Table 195: QoS

Parameter Name	Description
Adaptive QoS	Enter adaptive QoS parameters. You can leave the additional details at as default or specify your values. • **Adapt Period (Minutes)**: Choose **Global** from the drop-down list, click **On**, and enter the period in minutes. • **Shaping Rate Upstream**: Choose **Global** from the drop-down list, click **On**, and enter the minimum, maximum, and default upstream bandwidth in Kbps. • **Shaping Rate Downstream**: Choose **Global** from the drop-down list, click **On**, and enter the minimum, maximum, downstream, and upstream bandwidth in Kbps.
Shaping Rate (kbps)	Choose **Global** from the drop-down list and configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps). Range: 8 through 100000000

g. Configure ACL.

Table 196: ACL

Parameter Name	Description
IPv4 Ingress Access List	Enter the name of an IPv4 access list to packets being received on the interface.
IPv4 Egress Access List	Enter the name of an IPv4 access list to packets being transmitted on the interface.
IPv6 Ingress Access List	Enter the name of an IPv6 access list to packets being received on the interface.
IPv6 Egress Access List	Enter the name of an IPv6 access list to packets being transmitted on the interface.

h. Configure advanced parameters.

Table 197: Advanced

Parameter Name	Description
Shutdown	Click **No** to enable the interface.
Tracker / Tracker Group	Enter the name of a tracker or tracker group to track the status of transport interfaces that connect to the internet.
Service Provider	Specify the details of the service provider.
Bandwidth Upstream (Kbps)	Specify the bandwidth value to generate notifications when the bandwidth of traffic transmitted on a physical interface exceeds the value.
Bandwidth Downstream (Kbps)	Specify the bandwidth value to generate notifications when the bandwidth of traffic transmitted on a physical interface exceeds the value.
IP MTU	Enter the maximum MTU size of packets on the interface. Range: 576 through 1804 Default: 1500
TCP MSS	Enter the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: 1500
TLOC Extension	Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration binds the service-side interface to the WAN transport by enabling a device to access the opposite WAN transport connected to the neighbouring device using a TLOC-extension interface.
IP Directed Broadcast	From the drop-down list, select **Global** to enable IP Directed Broadcast. An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet.

What to do next

Also see Deploy a configuration group.

Configure DSL PPPoA using templates

To configure DSL interfaces on Cisco routers using Cisco SD-WAN Manager templates:

1. Create a VPN Interface DSL PPPoA feature template to configure ATM interface parameters.
2. Create a VPN feature template to configure VPN parameters.

Follow these steps to configure DSL PPPoA using a feature template.

To provide support for service provider digital subscriber line (DSL) functionality, configure PPP-over-ATM interfaces on routers with DSL NIM modules.

Use the VPN Interface DSL PPPoA template for Cisco IOS XE Catalyst SD-WAN devices.

You configure PPP-over-ATM interfaces on routers with DSL NIM modules, to provide support for service provider digital subscriber line (DSL) functionality.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Device Templates**.

In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

Step 3 From the **Create Template** drop-down list, select **From Feature Template**.

a) From the **Device Model** drop-down list, select the type of device for which you are creating the template.
b) Click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.
c) Under **Additional VPN 0 Templates**, click **VPN Interface DSL PPPoA**.
d) From the **VPN Interface DSL PPPoA** drop-down list, click **Create Template**. The VPN Interface DSL PPPoA template form is displayed. This form contains fields for naming the template, and fields for defining VPN Interface PPP parameters.
e) In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
f) In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

Step 4 Configure basic VDSL controller functionality in a VPN.

Table 198:

Parameter Name	Description
Shutdown*	Click **No** to enable the VDSL controller interface.
Controller VDSL Slot*	Enter the slot number of the controller VDSL interface, in the format *slot*/*subslot*/*port* (for example, 0/2/0).

Parameter Name	Description
Mode*	Select the operating mode of the VDSL controller from the drop-down: • **Auto**—Default mode. • **ADSL1**—Use ITU G.992.1 Annex A full-rate mode, which provides a downstream rate of 1.3 Mbps and an upstream rate of 1.8 Mbps. • **ADSL2**—Use ITU G.992.3 Annex A, Annex L, and Annex M, which provides a downstream rate of 12 Mbps and an upstream rate of 1.3 Mbps. • **ADSL2+**— Use ITU G.992.5 Annex A and Annex M, which provides a downstream rate of 24 Mbps and an upstream rate of 3.3 Mbps. • **ANSI**—Operate in ADSL2/2+ mode, as defined in ITU G.991.1, G.992.3, and G992.5, Annex A and Annex M, and in VDSL2 mode, as defined in ITU-T G993.2. • **VDSL2**—Operate in VDSL2 mode, as defined in ITU-T G.993.2, which uses frequencies of up to 30 MHz to provide a downstream rate of 200 Mbps and an upstream rate of 100 Mbps.
VDSL Modem Configuration	Enter a command to send to the DSL modem in the NIM module. If the command is valid, it is executed and the results are returned to the Cisco SD-WAN Manager. If the command is not valid, it is not executed.
SRA	Enabled by default. Click **No** to disable seamless rate adaptation on the interface. SRA adjusts the line rate based on current line conditions.

Step 5 Configure an ATM interface on the VDSL controller.

Table 199:

Parameter Name	Description
ATM Interface Name	Enter a name for the ATM interface, in the format *subslot*/*port* (for example 2/0). You do not need to enter the slot number, because it must always be 0.
Description	Enter a description for the interface.
VPI and VCI	Create an ATM permanent virtual circuit (PVC), in the format *vpi*/*vci*, Enter values for the virtual path identifier (VPI) and the virtual channel identifier (VCI).
Encapsulation	Select the ATM adaptation layer (AAL) and encapsulation type to use on the ATM PVC from the drop-down list: • AAL5 MUX—Dedicate the PVC to a single protocol. • AAL5 NLPID—Use NLPID multiplexing. • AAL5 SNAP—Multiplex two or more protocols on the same PVC.
Dialer Pool Member	Enter the number of the dialer pool to which the interface belongs. It can be a value from 1 through 255.

Parameter Name	Description
VBR-NRT	Configure variable bit rate non-real-time parameters: • Peak Cell Rate—Enter a value from 48 through 25000 Kbps. • Sustainable Cell Rate—Enter the sustainable cell rate, in Kbps. • Maximum Burst Size—This size can be 1 cell.
VBR-RT	Configure variable bit rate real-time parameters: • Peak Cell Rate—Enter a value from 48 through 25000 Kbps. • Average Cell Rate—Enter the average cell rate, in Kpbs. • Maximum Burst Size—This size can be 1 cell.

Step 6 Configure the PPP authentication protocol.

Table 200:

Parameter Name	Description
Authentication Protocol	Select the authentication protocol used by the MLP: • **CHAP**—Enter the hostname and password provided by your Internet Service Provider (ISP). *hostname* can be up to 254 characters. • **PAP**—Enter the username and password provided by your ISP. *username* can be up to 254 characters. • **PAP** and **CHAP**—Configure both authentication protocols. Enter the login credentials for each protocol. To use the same username and password for both, click Same Credentials for PAP and CHAP.

Step 7 Configure a tunnel interface for the multilink interface.

Table 201:

Parameter Name	Description
Tunnel Interface	Click **On** to create a tunnel interface.
Color	Select a color for the TLOC.
Color Description	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enter a description associated to the TLOC color.

Parameter Name	Description
Control Connection	If the Cisco IOS XE Catalyst SD-WAN device has multiple TLOCs, click No to have the tunnel not establish a TLOC. The default is On, which establishes a control connection for the TLOC. **Note** For control connection traffic without dropping any data, a minimum of 650-700 kbps bandwidth is recommended with default parameters configured for hello-interval (10) and hello-tolerance (12).
Maximum Control Connections	Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8 Default: 2
Cisco SD-WAN Validator As STUN Server	Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the Cisco IOS XE Catalyst SD-WAN device is located behind a NAT.
Exclude Controller Group List	Set the Cisco SD-WAN Controllers that the tunnel interface is not allowed to connect to. Range: 0 through 100
Cisco SD-WAN Manager Connection Preference	Set the preference for using a tunnel interface to exchange control traffic with the Cisco SD-WAN Manager NMS. Range: 0 through 8 Default: 5
Full Port Hop	Minimum release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled
Port Hop	Click **On** to enable port hopping, or click Off to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. Default: Enabled Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, this field is deprecated. Instead use the **Full Port Hop** option. See the **Full Port Hop** field.
Low-Bandwidth Link	Select to characterize the tunnel interface as a low-bandwidth link.

Parameter Name	Description
Tunnel TCP MSS	TCP MSS affects any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS is examined against the MSS exchanged in the three-way handshake. The MSS in the header is lowered if the configured TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. If the TCP MSS is to be configured, it should be set at 40 bytes lower than the minimum path MTU. Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes Default: None
Clear-Dont-Fragment	Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent. Click **On** to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, packets larger than the MTU of the interface are fragmented before being sent. **Note** **Clear-Dont-Fragment** clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected.
Allow Service	Select **On** or **Off** for each service to allow or disallow the service on the interface.

To configure additional tunnel interface parameters, click **Advanced Options** and configure the following parameters:

Table 202:

Parameter Name	Description
GRE	Use GRE encapsulation on the tunnel interface. By default, GRE is disabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
IPsec	Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
IPsec Preference	Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295. Default: 0

Parameter Name	Description
IPsec Weight	Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255. Default: 1
Carrier	Select the carrier name or private network identifier to associate with the tunnel. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default. Default: default
Bind Loopback Tunnel	Enter the name of a physical interface to bind to a loopback interface.
Last-Resort Circuit	Select to use the tunnel interface as the circuit of last resort. **Note** An interface configured as a circuit of last resort is expected to be down and is skipped while calculating the number of control connections, the cellular modem becomes dormant, and no traffic is sent over the circuit. When the configurations are activated on the edge device with cellular interfaces, then all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down. Only when all the primary interfaces lose their connections to remote edges, then the circuit of last resort activates itself triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are used as backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode the radio interface is turned off, and no control or data connections exist over the cellular interface.
NAT Refresh Interval	Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds. Default: 5 seconds.
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 10000 milliseconds. Default: 1000 milliseconds (1 second).
Hello Tolerance	Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down. Range: 12 through 60 seconds. Default: 12 seconds.

Step 8 Apply a rewrite rule, access lists, and policers to a router interface.

Table 203:

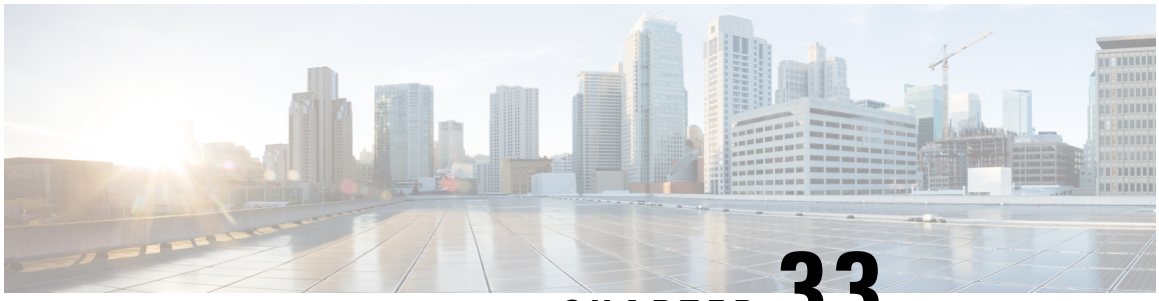
Parameter Name	Description
Shaping rate	Configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).
QoS map	Specify the name of the QoS map to apply to packets being transmitted out the interface.
Rewrite Rule	Click **On**, and specify the name of the rewrite rule to apply on the interface.
Ingress ACL – IPv4	Click **On**, and specify the name of the access list to apply to IPv4 packets being received on the interface.
Egress ACL – IPv4	Click **On**, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface.
Ingress ACL – IPv6	Click **On**, and specify the name of the access list to apply to IPv6 packets being received on the interface.
Egress ACL – IPv6	Click **On**, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface.
Ingress Policer	Click **On**, and specify the name of the policer to apply to packets being received on the interface.
Egress Policer	Click **On**, and specify the name of the policer to apply to packets being transmitted on the interface.

Step 9 Configure other interface properties.

Table 204:

Parameter Name	Description
PMTU Discovery	Click **On** to enable path MTU discovery on the interface, to allow the router to determine the largest MTU size supported without requiring packet fragmentation.
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes. Default: None.
Clear Dont Fragment	Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent.
Static Ingress QoS	Select a queue number to use for incoming traffic. Range:0 through 7
Autonegotiate	Click **Off** to turn off autonegotiation. By default, an interface runs in autonegotiation mode.

Parameter Name	Description
TLOC Extension	Enter the name of the physical interface on the same router that connects to the WAN transport circuit. This configuration then binds this service-side interface to the WAN transport. A second Cisco IOS XE Catalyst SD-WAN device at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.



CHAPTER 33

DSL PPPoE

- Feature history for DSL PPPoe, on page 591
- Configure DSL PPPoE, on page 591

Feature history for DSL PPPoe

Table 205: Feature History

Feature Name	Release Information	Description
Support for Dialer Interface in DSL	Cisco IOS XE Release 17.3.2 Cisco vManage Release 20.3.1	This feature enables tracking of a Point-to-Point Protocol (PPP) session over a dialer interface on Cisco IOS XE Catalyst SD-WAN devices. Dialer interface is used in Digital Subscriber Line (DSL) in the deployments of Point-to-Point Protocol over Ethernet (PPPoE), Point-to-Point Protocol over Asynchronous Transfer Mode (PPPoA). Dialer interface always stay up irrespective of the PPP session status. This helps to avoid the need for additional configuration such as IP SLA and tracking for routing failover to work while using dialer interfaces. The following command is added to configure dialer down-with-vInterface which brings the dialer interface down when the PPP session goes down.

Configure DSL PPPoE

Use one of these methods to configure DSL PPPoE:

- Configuration group
- Feature template

Configure DSL PPPoE using a configuration group

Follow these steps to configure DSL PPPoE using a configuration group.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure the DSL PPPoE parameters in a Transport and Management Profile.

a. Configure basic configuration.

Table 206: Basic Configuration

Parameter Name	Description
Controller Slot*	Enter the slot number of the controller, in the following format: *slot*/*subslot*/*port* (for example, 0/2/0)
Controller Mode	Select the operating mode of the DSL controller from the drop-down list: • **ADSL1**: Use ITU G.992.1 Annex A full-rate mode, which provides a downstream rate of 1.3 Mbps and an upstream rate of 1.8 Mbps. • **ADSL2**: Use ITU G.992.3 Annex A, Annex L, and Annex M, which provides a downstream rate of 12 Mbps and an upstream rate of 1.3 Mbps. • **ADSL2+**: Use ITU G.992.5 Annex A and Annex M, which provides a downstream rate of 24 Mbps and an upstream rate of 3.3 Mbps. • **ANSI**: Operating in ADSL2/2+ mode, as defined in ITU G.991.1, G.992.3, and G992.5, Annex A and Annex M, and in VDSL2 mode, as defined in ITU-T G993.2. • **VDSL2**: Operate in VDSL2 mode, as defined in ITU-T G.993.2, which uses frequencies of up to 30 MHz to provide a downstream rate of 200 Mbps and an upstream rate of 100 Mbps.
SRA	Disabled by default. Enable SRA to disable seamless rate adaptation on the interface. SRA adjusts the line rate based on current line conditions.
Dialer Pool Member*	Enter the number of the dialer pool to which the interface belongs. Range: 1 through 255

b. Configure Ethernet.

Table 207: Ethernet

Parameter Name	Description
Ethernet Interface Name *	Enter the name of an ethernet interface. For IOS XE routers, you must spell out the interface names completely (for example, **GigabitEthernet0/0/0**).
Description	Enter a description for the interface.
VLAN ID	Enter the VLAN identifier of the Ethernet interface.

c. Configure PPP.

Table 208: PPP

Parameter Name	Description
PPP Authentication Protocol	Select the authentication protocol used by the MLP: • **PAP**: Enter the username and password that are provided by your ISP. *username* can be up to 254 characters. • **CHAP**: Enter the hostname and password provided by your Internet Service Provider (ISP). *hostname* can be up to 254 characters. • **PAP** and **CHAP**: Configure both authentication protocols. Enter the login credentials for each protocol.
Authentication Type	Select the type authentication from one of the following options: • **Unidirectional**: Only the side receiving the call (NAS) authenticates the remote side (client). The remote client does not authenticate the server. • **Bidirectional**: Each side independently sends an Authenticate-Request (AUTH-REQ) and receives either an Authenticate-Acknowledge (AUTH-ACK) or Authenticate-Not Acknowledged (AUTH-NAK).
CHAP Hostname*	Enter the CHAP hostname.
CHAP Password*	Enter the CHAP password.
PAP Hostname*	Enter the PAP hostname.
PAP Password*	Enter the PAP password.

d. Configure Tunnel.

Table 209: Tunnel

Parameter Name	Description
Tunnel Interface	

Parameter Name	Description
Per Tunnel QoS	Enable per tunnel QoS and choose from the following values to configure hub-to-spoke network topologies: • **Spoke** • **Hub**
Color	Select a color for the TLOC.
Color Description	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enter a description associated to the TLOC color.
Groups	Enter the list of groups in the field.
Exclude Controller Group List	Set the Cisco SD-WAN Controllers that the tunnel interface is not allowed to connect to. Range: 0 through 100
Maximum Control Connections	Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8 Default: 2
Cisco SD-WAN Manager Connection Preference	Set the preference for using a tunnel interface to exchange control traffic with Cisco SD-WAN Manager. Range: 0 through 8 Default: 5
Tunnel TCP MSS	TCP MSS affects any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS is examined against the MSS exchanged in the three-way handshake. The MSS in the header is lowered if the configured TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. To configure TCP MSS, provide a value that is 40 bytes lower than the minimum path MTU. Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: None
Border	From the drop-down list, select **Global**. Click **On** to set TLOC as border TLOC.
Validator As Stun Server	Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT.

Parameter Name	Description
Full Port Hop	Minimum release: Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled
Port Hop	From the drop-down list, select **Global**. Click **Off** to allow port hopping on tunnel interface. Default: **On**, which disallows port hopping on tunnel interface. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, tthis field is deprecated. Instead use the **Full Port Hop** option. See the **Full Port Hop** field.
Low-Bandwidth Link	Click **On** to set the tunnel interface as a low-bandwidth link. Default: **Off**
Clear-Dont-Fragment	Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent. Click **On** to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, the router fragments packets larger than the MTU of the interface before sending the packets. **Note** **Clear-Dont-Fragment** clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected.
Network Broadcast	From the drop-down list, select **Global**. Click **On** to accept and respond to network-prefix-directed broadcasts. Enable this parameter only if the **Directed Broadcast** is enabled on the LAN interface feature template. Default: **Off**
Carrier	From the drop-down list, select **Global**and select the carrier name or private network identifier to associate with the tunnel. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default. Default: default
Bind Loopback Tunnel	Enter the name of a physical interface to bind to a loopback interface. The interface name has the following format: **ge***slot*/*port*
NAT Refresh Interval	Set the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds Default: 5 seconds

Parameter Name	Description
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 10000 milliseconds Default: 1000 milliseconds (1 second)
Hello Tolerance	Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down. Range: 12 through 60 seconds Default: 12 seconds The default hello interval is 1000 milliseconds, and it can be a time in the range 100 through 600000 milliseconds (10 minutes). The default hello tolerance is 12 seconds, and it can be a time in the range 12 through 600 seconds (10 minutes). To reduce outgoing control packets on a TLOC, it is recommended that on the tunnel interface you set the hello interval to 60000 milliseconds (10 minutes) and the hello tolerance to 600 seconds (10 minutes) and include the **no track-transport disable** regular checking of the DTLS connection between the edge device and the controller. For a tunnel connection between a edge device and any controller device, the tunnel uses the hello interval and tolerance times configured on the edge device. This choice is made to minimize the traffic sent over the tunnel, to allow for situations where the cost of a link is a function of the amount of traffic traversing the link. The hello interval and tolerance times are chosen separately for each tunnel between a edge device and a controller device. Another step taken to minimize the amount of control plane traffic is to not send or receive OMP control traffic over a cellular interface when other interfaces are available. This behavior is inherent in the software and is not configurable.
Last Resort Circuit	Select to use the tunnel interface as the circuit of last resort. **Note** It is assumed that an interface configured as a circuit of last resort is unavailable and is skipped while calculating the number of control connections. As a result, the cellular modem becomes dormant, and no traffic is sent over the circuit. When the configurations are activated on the edge device with cellular interfaces, all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down. If the primary interfaces lose their connections to remote edges, the circuit of last resort activates itself, triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are a backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode, the radio interface is turned off, and no control or data connections exist over the cellular interface.
Allow Services	Click **On** or **Off** for each service to allow or disallow the service on the cellular interface.
Encapsulation	

Parameter Name	Description
Encapsulation	Enable atleast one of the following encapsulation methods: • **IPsec**: Enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 • **IPsec Preference**: From the drop-down list, select **Global** and enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 • **IPsec Weight**: From the drop-down list, select **Global** and enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1 • **GRE**: Enter a value to set GRE preference for TLOC. Range: 0 through 4294967295 • **GRE Preference**: From the drop-down list, select **Global** and enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 • **GRE Weight**: From the drop-down list, select **Global** and enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1

e. Configure NAT.

Table 210: NAT

Parameter Name	Description
UDP Timeout (Minutes)	Specify when NAT translations over UDP sessions time out. Range: 1 through 65536 minutes Default: 1 minute

Parameter Name	Description
TCP Timeout (Minutes)	Specify when NAT translations over TCP sessions time out. Range: 1 through 65536 minutes Default: 60 minutes (1 hour)

f. Configure QoS.

Table 211: QoS

Parameter Name	Description
Adaptive QoS	Enter adaptive QoS parameters. You can leave the additional details at as default or specify your values. • **Adapt Period (Minutes)**: Choose **Global** from the drop-down list, click **On**, and enter the period in minutes. • **Shaping Rate Upstream**: Choose **Global** from the drop-down list, click **On**, and enter the minimum, maximum, and default upstream bandwidth in Kbps. • **Shaping Rate Downstream**: Choose **Global** from the drop-down list, click **On**, and enter the minimum, maximum, downstream, and upstream bandwidth in Kbps.
Shaping Rate (kbps)	Choose **Global** from the drop-down list and configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps). Range: 8 through 100000000

g. Configure ACL.

Table 212: ACL

Parameter Name	Description
IPv4 Ingress Access List	Enter the name of an IPv4 access list to packets being received on the interface.
IPv4 Egress Access List	Enter the name of an IPv4 access list to packets being transmitted on the interface.
IPv6 Ingress Access List	Enter the name of an IPv6 access list to packets being received on the interface.
IPv6 Egress Access List	Enter the name of an IPv6 access list to packets being transmitted on the interface.

h. Configure advanced parameters.

Table 213: Advanced

Parameter Name	Description
Shutdown	Click **No** to enable the interface.

Parameter Name	Description
Tracker / Tracker Group	Enter the name of a tracker or tracker group to track the status of transport interfaces that connect to the internet.
PPP Maximum Payload	Enter the maximum receive unit (MRU) value to be negotiated during PPP-over-Ethernet negotiation. Range: 64 through 1792 bytes
Service Provider	Specify the details of the service provider.
Bandwidth Upstream (Kbps)	Specify the bandwidth value to generate notifications when the bandwidth of traffic transmitted on a physical interface exceeds the value.
Bandwidth Downstream (Kbps)	Specify the bandwidth value to generate notifications when the bandwidth of traffic transmitted on a physical interface exceeds the value.
IP MTU	Enter the maximum MTU size of packets on the interface. Range: 576 through 1804 Default: 1500.
TCP MSS	Enter the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: 1500
TLOC Extension	Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration binds the service-side interface to the WAN transport by enabling a device to access the opposite WAN transport connected to the neighbouring device using a TLOC-extension interface.
IP Directed Broadcast	From the drop-down list, select **Global** to enable IP Directed Broadcast. An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet.
Tracker / Tracker Group	Enter the name of a tracker or tracker group to track the status of transport interfaces that connect to the internet.

What to do next

Also see Deploy a configuration group.

Configure DSL PPPoE using templates

Follow these steps to confgure DSL PPPoE using a feature template.

You configure PPP-over-Ethernet interfaces on routers with DSL NIM modules, to provide support for service provider digital subscriber line (DSL) functionality.

Use the VPN Interface DSL PPPoE template for Cisco IOS XE Catalyst SD-WAN devices.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Device Templates**.

In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

Step 3 From the **Create Template** drop-down list, select **From Feature Template**.

a) From the **Device Model** drop-down list, select the type of device for which you are creating the template.
b) Click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.
c) Under **Additional VPN 0 Templates**, click **VPN Interface DSL PPPoE**.
d) From the **VPN Interface DSL PPPoE** drop-down list, click **Create Template**. The VPN Interface DSL PPPoA template form is displayed. This form contains fields for naming the template, and fields for defining VPN Interface PPP parameters.
e) In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
f) In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

Step 4 Configure the following VPN Interface DSL PPPoE parameters.

a) Configure basic VDSL controller functionality in a VPN.

If your deployment includes devices with DSL, you must include DSL interface templates in Cisco SD-WAN Manager, even if these templates are not used.

Table 214:

Parameter Name	Description
Shutdown*	Click **No** to enable the VDSL controller interface.
Controller VDSL Slot*	Enter the slot number of the controller VDSL interface, in the format *slot*/*subslot*/*port* (for example, 0/2/0).

Parameter Name	Description
Mode*	Select the operating mode of the VDSL controller from the drop-down: • **Auto**—Default mode. • **ADSL1**—Use ITU G.992.1 Annex A full-rate mode, which provides a downstream rate of 1.3 Mbps and an upstream rate of 1.8 Mbps. • **ADSL2**—Use ITU G.992.3 Annex A, Annex L, and Annex M, which provides a downstream rate of 12 Mbps and an upstream rate of 1.3 Mbps. • **ADSL2+**— Use ITU G.992.5 Annex A and Annex M, which provides a downstream rate of 24 Mbps and an upstream rate of 3.3 Mbps. • **ANSI**—Operating in ADSL2/2+ mode, as defined in ITU G.991.1, G.992.3, and G992.5, Annex A and Annex M, and in VDSL2 mode, as defined in ITU-T G993.2. • **VDSL2**—Operate in VDSL2 mode, as defined in ITU-T G.993.2, which uses frequencies of up to 30 MHz to provide a downstream rate of 200 Mbps and an upstream rate of 100 Mbps..
VDSL Modem Configuration	Enter a command to send to the DSL modem in the NIM module. If the command is valid, it is executed and the results are returned to the Cisco SD-WAN Manager NMS. If the command is not valid, it is not executed.
SRA	Click **Yes** to enable seamless rate adaptation on the interface. SRA adjusts the line rate based on current line conditions.

b) Configure an Ethernet interface on the VDSL controller.

Table 215:

Parameter Name	Description
Ethernet Interface Name	Enter a name for the Ethernet interface, in the format *subslot*/*port* (for example 2/0). You do not need to enter the slot number, because it must always be 0.
VLAN ID	Enter the VLAN identifier of the Ethernet interface.
Description	Enter a description for the interface.
Dialer Pool Member	Enter the number of the dialer pool to which the interface belongs. It can be a value from 1 through 255.
PPP Max Payload	Enter the maximum receive unit (MRU) value to be negotiated during PPP Link Control Protocol (LCP) negotiation. Range: 64 through 1792 bytes
Dialer IP	Configure the IP prefix of the dialer interface. This prefix is that of the node in the destination that the interface calls. • Negotiated—Use the address that is obtained during IPCP negotiation.

c) Configure the PPP authentication protocol.

Table 216:

Parameter Name	Description
Authentication Protocol	Select the authentication protocol used by the MLP: • **CHAP**—Enter the hostname and password provided by your Internet Service Provider (ISP). *hostname* can be up to 254 characters. • **PAP**—Enter the username and password that are provided by your ISP. *username* can be up to 254 characters. • **PAP** and **CHAP**—Configure both authentication protocols. Enter the login credentials for each protocol. To use the same username and password for both, click Same Credentials for PAP and CHAP.

d) Configure a tunnel interface for the multilink interface.

Table 217:

Parameter Name	Description
Tunnel Interface	Click **On** to create a tunnel interface.
Color	Select a color for the TLOC.
Color Description	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enter a description associated to the TLOC color.

Parameter Name	Description
Control Connection	By default, Control Conection is set to **On**, which establishes a control connection for the TLOC. If the router has multiple TLOCs, click **No** to have the tunnel not establish control connection for the TLOC. **Note** We recommend a minimum of 650-700 Kbps bandwidth with default 1 sec hello-interval and 12 sec hello-tolerance parameters configured to avoid any data/packet loss in connection traffic. For each BFD session, an additional average sized BFD packet of 175 Bytes consumes 1.4 Kbps of bandwidth. A sample calculation of the required bandwidth for bidirectional BFD packet flow is given below: • 650 – 700 Kbps per device for control connections. • 175 Bytes (or 1.4 Kbps) per BFD session on the device (request) • 175 Bytes (or 1.4 Kbps) per BFD session on the device (response) If the path MTU discovery (PMTUD) is enabled, bandwidth for send/receive BFD packets per tunnel for every 30 secs: A 1500 Bytes BFD request packet is sent per tunnel every 30 secs: 1500 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 400 bps (request) A 147 Bytes BFD packet is sent in response: 147 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 40 bps (response) Therefore, a device with 775 BFD sessions (for example) requires a bandwidth of: 700k + (1.4k*775) + (400 *775) + (1.4k*775) + (40 *775) = ~3,5 MBps • STATE—specifies the vdaemon control state. Last Connection—If no control connection on that WAN interface, the uptime of the device is lifted. SPI Time Remaining—countdown to the next change in SPI for IPSec. The countdown starts at half of the rekey time.
Maximum Control Connections	Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8 Default: 2
Cisco SD-WAN Validator As STUN Server	Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT.
Exclude Controller Group List	Set the Cisco SD-WAN Controllers that the tunnel interface is not allowed to connect to. Range: 0 through 100

Parameter Name	Description
Cisco SD-WAN Manager Connection Preference	Set the preference for using a tunnel interface to exchange control traffic with the Cisco SD-WAN Manager NMS. Range: 0 through 8 Default: 5
Full Port Hop	Minimum release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled
Port Hop	Click **On** to enable port hopping, or click Off to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. Default: Enabled. Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, this field is deprecated. Instead use the **Full Port Hop** option. See the **Full Port Hop** field.
Low-Bandwidth Link	Select to characterize the tunnel interface as a low-bandwidth link.
Tunnel TCP MSS	TCP MSS affects any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS is examined against the MSS exchanged in the three-way handshake. The MSS in the header is lowered if the configured TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. If the TCP MSS is to be configured, it should be set at 40 bytes lower than the minimum path MTU. Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes Default: None
Clear-Dont-Fragment	Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent. Click **On** to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, packets larger than the MTU of the interface are fragmented before being sent. **Note** **Clear-Dont-Fragment** clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected.
Allow Service	Select **On** or **On** for each service to allow or disallow the service on the interface.

To configure additional tunnel interface parameters, click **Advanced Options** and configure the following parameters:

Table 218:

Parameter Name	Description
GRE	Use GRE encapsulation on the tunnel interface. By default, GRE is disabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
IPsec	Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
IPsec Preference	Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0
IPsec Weight	Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1
Carrier	Select the carrier name or private network identifier to associate with the tunnel. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default Default: default
Bind Loopback Tunnel	Enter the name of a physical interface to bind to a loopback interface.
Last-Resort Circuit	Select to use the tunnel interface as the circuit of last resort. **Note** An interface configured as a circuit of last resort is expected to be down and is skipped while calculating the number of control connections, the cellular modem becomes dormant, and no traffic is sent over the circuit. When the configurations are activated on the edge device with cellular interfaces, then all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down. Only when all the primary interfaces lose their connections to remote edges, then the circuit of last resort activates itself triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are used as backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode the radio interface is turned off, and no control or data connections exist over the cellular interface.

Parameter Name	Description
NAT Refresh Interval	Enter the interval between NAT refresh packets that are sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds. Default: 5 seconds.
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 10000 milliseconds. Default: 1000 milliseconds (1 second).
Hello Tolerance	Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down. Range: 12 through 60 seconds. Default: 12 seconds.

e) Configure an interface to act as a NAT device for applications such as port forwarding.

Parameter Name	Description
NAT	Click **On** to have the interface act as a NAT device.
Refresh Mode	Select how NAT mappings are refreshed, either outbound or bidirectional (outbound and inbound). Default: Outbound
UDP Timeout	Specify when NAT translations over UDP sessions time out. Range: 1 through 65536 minutes Default: 1 minutes
TCP Timeout	Specify when NAT translations over TCP sessions time out. Range: 1 through 65536 minutes Default: 60 minutes (1 hour)
Block ICMP	Select **On** to block inbound ICMP error messages. By default, a router acting as a NAT device receives these error messages. Default: Off
Respond to Ping	Select **On** to have the router respond to ping requests to the NAT interface's IP address that are received from the public side of the connection.

To create a port forwarding rule, click **Add New Port Forwarding Rule** and configure the following parameters. You can define up to 128 port-forwarding rules to allow requests from an external network to reach devices on the internal network.

Table 219:

Parameter Name	Description
Port Start Range	Enter a port number to define the port or first port in the range of interest. Range: 0 through 65535
Port End Range	Enter the same port number to apply port forwarding to a single port, or enter a larger number to apply it to a range of ports. Range: 0 through 65535
Protocol	Select the protocol to which to apply the port-forwarding rule, either TCP or UDP. To match the same ports for both TCP and UDP traffic, configure two rules.
VPN	Specify the private VPN in which the internal server resides. This VPN is one of the VPN identifiers in the overlay network. Range: 0 through 65527
Private IP	Specify the IP address of the internal server to which to direct traffic that matches the port-forwarding rule.

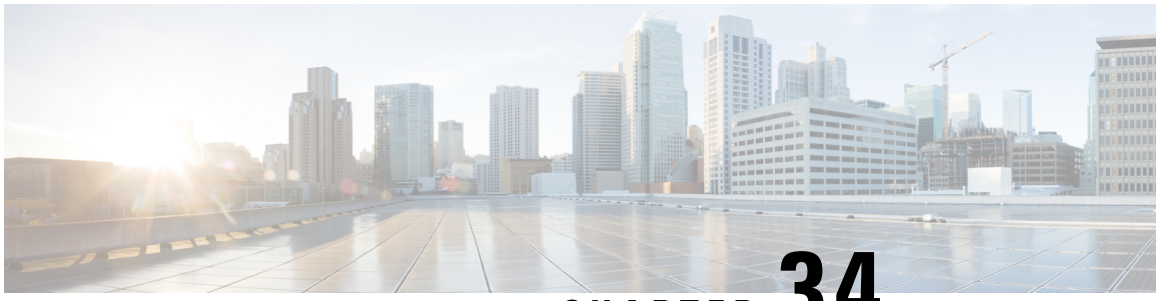
f) Apply a rewrite rule, access lists, and policers to a router interface.

Table 220:

Parameter Name	Description
Shaping rate	Configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).
QoS map	Specify the name of the QoS map to apply to packets being transmitted out the interface.
Rewrite Rule	Click **On**, and specify the name of the rewrite rule to apply on the interface.
Ingress ACL – IPv4	Click **On**, and specify the name of the access list to apply to IPv4 packets being received on the interface.
Egress ACL – IPv4	Click **On**, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface.
Ingress ACL – IPv6	Click **On**, and specify the name of the access list to apply to IPv6 packets being received on the interface.
Egress ACL – IPv6	Click **On**, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface.
Ingress Policer	Click **On**, and specify the name of the policer to apply to packets being received on the interface.
Egress Policer	Click **On**, and specify the name of the policer to apply to packets being transmitted on the interface.

g) Configure other interface properties.

Parameter Name	Description
Bandwidth Upstream	For transmitted traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32} / 2) – 1 kbps
Bandwidth Downstream	For received traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32} / 2) – 1 kbps
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 through 1804. Default: 1500 bytes.
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes. Default: None.
Clear Dont Fragment	Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent.
TLOC Extension	Enter the name of the physical interface on the same router that connects to the WAN transport circuit. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.
Tracker	Enter the name of a tracker to track the status of transport interfaces that connect to the internet.



CHAPTER 34

VPN Interface Ethernet PPPoE

- Configure VPN interface ethernet PPPoE, on page 609

Configure VPN interface ethernet PPPoE

Use one of these methods to configure VPN interface ethernet PPPoE:

- Configuration group
- Feature template

Configure VPN interface ethernet PPPoE using a configuration group

Follow these steps to configure VPN interface ethernet PPPoE using a configuration group.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure a Ethernet PPPoE feature under Transport VPN in a Transport and Management profile.

a) Configure basic PPPoE functionality.

Parameter Name	Description
Ethernet Interface Name *	Enter the name of an ethernet interface. For IOS XE routers, you must spell out the interface names completely (for example, **GigabitEthernet0/0/0**).
Description	Enter a description for the ethernet interface.
VLAN ID	Enter the VLAN identifier of the Ethernet interface.

Parameter Name	Description
Dialer Pool Member *	Enter the number of the dialer pool to which the interface belongs. Range: 1 through 255

b) Configure the PPP Authentication Protocol.

Parameter Name	Description
PPP Authentication Protocol*	Select the authentication protocol used by the MLP: • **PAP**: Enter the username and password that are provided by your ISP. *username* can be up to 254 characters. • **CHAP**: Enter the hostname and password provided by your Internet Service Provider (ISP). *hostname* can be up to 254 characters. • **PAP** and **CHAP**: Configure both authentication protocols. Enter the login credentials for each protocol.
Authentication Type	Select the type authentication from one of the following options.: • **Unidirectional**: Only the side receiving the call (NAS) authenticates the remote side (client). The remote client does not authenticate the server. • **Bidirectional**: Each side independently sends an Authenticate-Request (AUTH-REQ) and receives either an Authenticate-Acknowledge (AUTH-ACK) or Authenticate-Not Acknowledged (AUTH-NAK).
CHAP Hostname*	Enter the CHAP hostname.
CHAP Password*	Enter the CHAP password.
PAP Hostname*	Enter the PAP hostname.
PAP Password*	Enter the PAP password.

c) Configure a tunnel interface for the multilink interface.

Parameter Name	Description
Tunnel Interface	
Per Tunnel QoS	Enable per tunnel QoS and choose **Spoke** to configure the spoke network topology
Color	Select a color for the TLOC.
Color Description	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enter a description associated to the TLOC color.
Groups	Enter the list of groups in the field.

Parameter Name	Description
Exclude Controller Group List	Set the Cisco SD-WAN Controllers that the tunnel interface is not allowed to connect to. Range: 0 through 100
Maximum Control Connections	Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8
Cisco SD-WAN Manager Connection Preference	Set the preference for using a tunnel interface to exchange control traffic with Cisco SD-WAN Manager. Range: 0 through 8 Default: 5
Tunnel TCP MSS	TCP MSS affects any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS is examined against the MSS exchanged in the three-way handshake. The MSS in the header is lowered if the configured TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. To configure TCP MSS, provide a value that is 40 bytes lower than the minimum path MTU. Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: None
Border	From the drop-down list, select **Global**. Click **On** to set TLOC as border TLOC.
Validator As Stun Server	Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT.
Full Port Hop	Minimum release: Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled
Port Hop	From the drop-down list, select **Global**. Click **Off** to allow port hopping on tunnel interface. Default: **On**, which disallows port hopping on tunnel interface. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, this field is deprecated. Instead use the **Full Port Hop** option. See the **Full Port Hop** field.
Low-Bandwidth Link	Click **On** to set the tunnel interface as a low-bandwidth link. Default: **Off**

Parameter Name	Description
Clear-Dont-Fragment	Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent. Click **On** to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, the router fragments packets larger than the MTU of the interface before sending the packets. **Note** **Clear-Dont-Fragment** clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected.
Network Broadcast	From the drop-down list, select **Global**. Click **On** to accept and respond to network-prefix-directed broadcasts. Enable this parameter only if the **Directed Broadcast** is enabled on the LAN interface feature template. Default: **Off**
Carrier	From the drop-down list, select **Global**and select the carrier name or private network identifier to associate with the tunnel. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default. Default: default
Bind Loopback Tunnel	Enter the name of a physical interface to bind to a loopback interface. The interface name has the following format: **ge** *slot*/*port*
NAT Refresh Interval	Set the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds Default: 5 seconds
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 10000 milliseconds Default: 1000 milliseconds (1 second)

Parameter Name	Description
Hello Tolerance	Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down. Range: 12 through 60 seconds Default: 12 seconds The default hello interval is 1000 milliseconds, and it can be a time in the range 100 through 600000 milliseconds (10 minutes). The default hello tolerance is 12 seconds, and it can be a time in the range 12 through 600 seconds (10 minutes). To reduce outgoing control packets on a TLOC, it is recommended that on the tunnel interface you set the hello interval to 60000 milliseconds (10 minutes) and the hello tolerance to 600 seconds (10 minutes) and include the **no track-transport disable** regular checking of the DTLS connection between the edge device and the controller. For a tunnel connection between a edge device and any controller device, the tunnel uses the hello interval and tolerance times configured on the edge device. This choice is made to minimize the traffic sent over the tunnel, to allow for situations where the cost of a link is a function of the amount of traffic traversing the link. The hello interval and tolerance times are chosen separately for each tunnel between a edge device and a controller device. Another step taken to minimize the amount of control plane traffic is to not send or receive OMP control traffic over a cellular interface when other interfaces are available. This behavior is inherent in the software and is not configurable.
Last Resort Circuit	Select to use the tunnel interface as the circuit of last resort. **Note** It is assumed that an interface configured as a circuit of last resort is unavailable and is skipped while calculating the number of control connections. As a result, the cellular modem becomes dormant, and no traffic is sent over the circuit. When the configurations are activated on the edge device with cellular interfaces, all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down. If the primary interfaces lose their connections to remote edges, the circuit of last resort activates itself, triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are a backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode, the radio interface is turned off, and no control or data connections exist over the cellular interface.
Allow Services	Click **On** or **Off** for each service to allow or disallow the service on the cellular interface.
Encapsulation	

Parameter Name	Description
Encapsulation	Enable at least one of the following encapsulation methods: • **IPsec**: Enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 • **IPsec Preference**: From the drop-down list, select **Global** and enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 • **IPsec Weight**: From the drop-down list, select **Global** and enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1 • **GRE**: Enter a value to set GRE preference for TLOC. Range: 0 through 4294967295 • **GRE Preference**: From the drop-down list, select **Global** and enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 • **GRE Weight**: From the drop-down list, select **Global** and enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1

d) Configure an interface to act as a NAT device for applications such as port forwarding.

Parameter Name	Description
UDP Timeout (Minutes)	Specify when NAT translations over UDP sessions time out. Range: 1 through 8947 minutes Default: 1 minute

Parameter Name	Description
TCP Timeout (Minutes)	Specify when NAT translations over TCP sessions time out. Range: 1 through 8947 minutes Default: 60 minutes (1 hour)

e) Configure QoS.

Parameter Name	Description
Adaptive QoS	Enter adaptive QoS parameters. You can leave the additional details at as default or specify your values. • **Adapt Period (Minutes)**: Choose **Global** from the drop-down list, click **On**, and enter the period in minutes. • **Shaping Rate Upstream**: Choose **Global** from the drop-down list, click **On**, and enter the minimum, maximum, and default upstream bandwidth in Kbps. • **Shaping Rate Downstream**: Choose **Global** from the drop-down list, click **On**, and enter the minimum, maximum, downstream, and upstream bandwidth in Kbps.
Shaping Rate (kbps)	Choose **Global** from the drop-down list and configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps). Range: 8 through 100000000

f) Configure ACL.

Parameter Name	Description
IPv4 Ingress Access List	Enter the name of an IPv4 access list to packets being received on the interface.
IPv4 Egress Access List	Enter the name of an IPv4 access list to packets being transmitted on the interface.
IPv6 Ingress Access List	Enter the name of an IPv6 access list to packets being received on the interface.
IPv6 Egress Access List	Enter the name of an IPv6 access list to packets being transmitted on the interface.

g) Configure additional tunnel interface parameters.

Parameter Name	Description
Shutdown	Choose **No** to enable the interface.
Tracker / Tracker Group	Enter the name of a tracker or tracker group to track the status of transport interfaces that connect to the internet.
Maximum Payload	Enter the maximum receive unit (MRU) value to be negotiated during PPP-over-Ethernet negotiation. Range: 64 through 1792 bytes

Parameter Name	Description
IP MTU	Enter the maximum MTU size of packets on the interface. Range: 576 through 1804 Default: 1500
TCP MSS	Enter the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: 1500
TLOC Extension	Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration binds the service-side interface to the WAN transport by enabling a device to access the opposite WAN transport connected to the neighbouring device using a TLOC-extension interface.
IP Directed Broadcast	From the drop-down list, select **Global** to enable IP Directed Broadcast. An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet.
Tracker / Tracker Group	Enter the name of a tracker or tracker group to track the status of transport interfaces that connect to the internet.

What to do next

Also see Deploy a configuration group.

Configure VPN interface ethernet PPPoE using templates

Follow these steps to configure VPN interface ethernet PPPoE using a feature template.

You configure PPPoE over GigabitEthernet interfaces on Cisco IOS XE routers, to provide PPPoE client support.

Use the PPPoE template for Cisco IOS XE Catalyst SD-WAN devices.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Device Templates**.

In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

Step 3 From the **Create Template** drop-down list, select **From Feature Template**.

a) From the **Device Model** drop-down list, select the type of device for which you are creating the template.
b) Click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.
c) Under **Additional VPN 0 Templates**, click **VPN Interface Ethernet PPPoE**.
d) From the **VPN Interface Ethernet PPPoE** drop-down list, click **Create Template**. The VPN Interface Ethernet PPPoE template form is displayed.
e) In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
f) In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

Step 4 Configure the following parameters in the VPN interface ethernet PPPoE template.

a) Configure the basic PPPoE functionality.

Table 221:

Parameter Name	Description
Shutdown*	Click **No** to enable the GigabitEthernet interface.
Ethernet Interface Name	Enter the name of a GigabitEthernet interface. For IOS XE routers, you must spell out the interface names completely (for example, **GigabitEthernet0/0/0**).
VLAN ID	VLAN tag of the sub-interface.
Description	Enter a description of the Ethernet-PPPoE-enabled interface.
Dialer Pool Member	Enter the number of the dialer pool to which the interface belongs. Range: 100 to 255.
PPP Maximum Payload	Enter the maximum receive unit (MRU) value to be negotiated during PPP Link Control Protocol (LCP) negotiation. Range: 64 through 1792 bytes

b) Configure the PPP Authentication Protocol.

Table 222:

Parameter Name	Description
PPP Authentication Protocol	Select the authentication protocol used by the MLP: • **CHAP**—Enter the hostname and password provided by your Internet Service Provider (ISP). *hostname* can be up to 254 characters. • **PAP**—Enter the username and password provided by your ISP. *username* can be up to 254 characters. • **PAP** and **CHAP**—Configure both authentication protocols. Enter the login credentials for each protocol. To use the same username and password for both, click Same Credentials for PAP and CHAP.

c) Configure a tunnel interface for the multilink interface.

Table 223:

Parameter Name	Description
Tunnel Interface	Click **On** to create a tunnel interface.
Color	Select a color for the TLOC.
Color Description	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enter a description associated to the TLOC color.
Control Connection	By default, Control Conection is set to **On**, which establishes a control connection for the TLOC. If the router has multiple TLOCs, click **No** to have the tunnel not establish control connection for the TLOC. **Note** We recommend a minimum of 650-700 Kbps bandwidth with default 1 sec hello-interval and 12 sec hello-tolerance parameters configured to avoid any data/packet loss in connection traffic. For each BFD session, an additional average sized BFD packet of 175 Bytes consumes 1.4 Kbps of bandwidth. A sample calculation of the required bandwidth for bidirectional BFD packet flow is given below: • 650 – 700 Kbps per device for control connections. • 175 Bytes (or 1.4 Kbps) per BFD session on the device (request) • 175 Bytes (or 1.4 Kbps) per BFD session on the device (response) If the path MTU discovery (PMTUD) is enabled, bandwidth for send/receive BFD packets per tunnel for every 30 secs: A 1500 Bytes BFD request packet is sent per tunnel every 30 secs: 1500 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 400 bps (request) A 147 Bytes BFD packet is sent in response: 147 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 40 bps (response) Therefore, a device with 775 BFD sessions (for example) requires a bandwidth of: 700k + (1.4k*775) + (400 *775) + (1.4k*775) + (40 *775) = ~3,5 MBps
Maximum Control Connections	Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8 Default: 2

Parameter Name	Description
Cisco SD-WAN Validator As STUN Server	Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT.
Exclude Controller Group List	Set the Cisco SD-WAN Controllers that the tunnel interface is not allowed to connect to. Range: 0 through 100
Cisco SD-WAN Manager Connection Preference	Set the preference for using a tunnel interface to exchange control traffic with the Cisco SD-WAN Manager NMS. Range: 0 through 8 Default: 5
Full Port Hop	Minimum release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled
Port Hop	Click **On** to enable port hopping, or click **Off** to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. Default: Enabled Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, this field is deprecated. Instead use the **Full Port Hop** option. See the **Full Port Hop** field.
Low-Bandwidth Link	Select to characterize the tunnel interface as a low-bandwidth link.
Allow Service	Select **On** or **Off** for each service to allow or disallow the service on the interface.

To configure additional tunnel interface parameters, click **Advanced Options** and configure the following parameters:

Table 224:

Parameter Name	Description
GRE	Use GRE encapsulation on the tunnel interface. By default, GRE is disabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
IPsec	Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.

Parameter Name	Description
IPsec Preference	Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295. Default: 0
IPsec Weight	Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255. Default: 1
Carrier	Select the carrier name or private network identifier to associate with the tunnel. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default. Default: default
Bind Loopback Tunnel	Enter the name of a physical interface to bind to a loopback interface.
Last-Resort Circuit	Select to use the tunnel interface as the circuit of last resort. **Note** An interface configured as a circuit of last resort is expected to be down and is skipped while calculating the number of control connections, the cellular modem becomes dormant, and no traffic is sent over the circuit. When the configurations are activated on the edge device with cellular interfaces, then all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down. Only when all the primary interfaces lose their connections to remote edges, then the circuit of last resort activates itself triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are used as backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode the radio interface is turned off, and no control or data connections exist over the cellular interface. **Note** Configuring administrative distance values on primary interface routes is not supported.
NAT Refresh Interval	Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds. Default: 5 seconds
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 10000 milliseconds. Default: 1000 milliseconds (1 second)

Parameter Name	Description
Hello Tolerance	Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down. Range: 12 through 60 seconds. Default: 12 seconds

d) Configure an interface to act as a NAT device for applications such as port forwarding.

Table 225:

Parameter Name	Description
NAT	Click **On** to have the interface act as a NAT device.
Refresh Mode	Select how NAT mappings are refreshed, either outbound or bidirectional (outbound and inbound). Default: Outbound
UDP Timeout	Specify when NAT translations over UDP sessions time out. Range: 1 through 65536 minutes. Default: 1 minutes
TCP Timeout	Specify when NAT translations over TCP sessions time out. Range: 1 through 65536 minutes. Default: 60 minutes (1 hour)
Block ICMP	Select **On** to block inbound ICMP error messages. By default, a router acting as a NAT device receives these error messages. Default: Off
Respond to Ping	Select **On** to have the router respond to ping requests to the NAT interface's IP address that are received from the public side of the connection.

To create a port forwarding rule, click **Add New Port Forwarding Rule** and configure the following parameters. You can define up to 128 port-forwarding rules to allow requests from an external network to reach devices on the internal network.

Table 226:

Parameter Name	Description
Port Start Range	Enter a port number to define the port or first port in the range of interest. Range: 0 through 65535

Parameter Name	Description
Port End Range	Enter the same port number to apply port forwarding to a single port, or enter a larger number to apply it to a range of ports. Range: 0 through 65535
Protocol	Select the protocol to which to apply the port-forwarding rule, either TCP or UDP. To match the same ports for both TCP and UDP traffic, configure two rules.
VPN	Specify the private VPN in which the internal server resides. This VPN is one of the VPN identifiers in the overlay network. Range: 0 through 65527
Private IP	Specify the IP address of the internal server to which to direct traffic that matches the port-forwarding rule.

e) Apply a rewrite rule, access lists, and policers to a router interface.

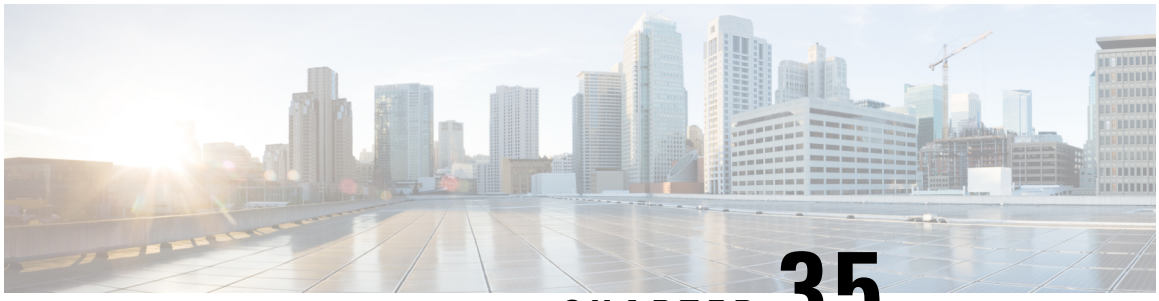
Table 227:

Parameter Name	Description
Shaping rate	Configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).
QoS map	Specify the name of the QoS map to apply to packets being transmitted out the interface.
Rewrite Rule	Click **On**, and specify the name of the rewrite rule to apply on the interface.
Ingress ACL – IPv4	Click **On**, and specify the name of the access list to apply to IPv4 packets being received on the interface.
Egress ACL – IPv4	Click **On**, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface.
Ingress ACL – IPv6	Click **On**, and specify the name of the access list to apply to IPv6 packets being received on the interface.
Egress ACL – IPv6	Click **On**, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface.
Ingress Policer	Click **On**, and specify the name of the policer to apply to packets being received on the interface.
Egress Policer	Click **On**, and specify the name of the policer to apply to packets being transmitted on the interface.

f) Configure other interface properties.

Table 228:

Parameter Name	Description
Bandwidth Upstream	For transmitted traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32} / 2) – 1 kbps
Bandwidth Downstream	For received traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32} / 2) – 1 kbps
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 through 1804. Default: 1500 bytes
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes. Default: None
TLOC Extension	Enter the name of the physical interface on the same router that connects to the WAN transport circuit. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.
Tracker	Enter the name of a tracker to track the status of transport interfaces that connect to the internet.
IP Directed-Broadcast	Enables translation of a directed broadcast to physical broadcasts. An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet.



CHAPTER 35

VPN Interface GRE

- Configure VPN interface GRE, on page 625

Configure VPN interface GRE

Use one of these methods to configure VPN interface GRE:

- Configuration group
- Feature template

Note Some configurations and protocols are identified as insecure and is a security risk for Cisco devices. Existing deployments continue to function, but new installations require intentional enablement. For more information on remediation, refer to Resilient Infrastructure: Cisco Catalyst SD-WAN and Routing

Configure VPN interface GRE on transport VPN using a configuration group

Follow these steps to configure VPN interface GRE on transport VPN using a configuration group.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure the GRE feature.

a) Configure GRE parameters.

Table 229: Basic Configuration

Field	Description
Interface Name (1..255)*	Enter the name of the GRE interface. Range: 1 through 255.
Interface Description	Enter a description of the GRE interface.
Tunnel Mode	Choose from one of the following GRE tunnel modes: • **ipv4 underlay**: GRE tunnel with IPv4 underlay. IPv4 underlay is the default value. • **ipv6 underlay**: GRE tunnel with IPv6 underlay.
Multiplexing	Choose **Yes** to enable multiplexing, in case of a tunnel in the transport VPN. Default: No
Preshared Key for IKE	Enter the preshared key (PSK) for authentication.

b) Configure Tunnel fields.

Table 230: Tunnel

Field	Description
Source	Enter the source of the GRE interface: • **IP Address**: Enter the source IP address of the GRE tunnel interface. Based on the option you selected in the **Tunnel Mode** drop-down list, enter an IPv4 or an IPv6 address. This address is on the local router. • **Interface**: Enter the egress interface name for the GRE tunnel. • **Tunnel Route Via***: Specify the tunnel route details to steer the GRE tunnel traffic through. **Note** If the Tunnel Source Interface type is a loopback interface, enter the interface for traffic to be routed to. You cannot use the tunnel route via option to configure IPSec tunnels on a cellular interface because cellular interfaces do not include a next hop IP address for the default route.
Destination	Enter the source of the GRE interface: • **GRE Destination IP Address***: Enter the destination IP address of the GRE tunnel interface. This address is on a remote device. • **IP Address**: Based on the option you selected in the **Tunnel Mode** drop-down list, enter an IPv4 or an IPv6 address for the GRE tunnel. • **Mask***: Enter the subnet mask. • **IPv6 Address**: Enter the destination IPv6 or address for the GRE tunnel.

c) Configure IKE fields.

Table 231: IKE

Field	Description
IKE Version	Enter 1 to choose IKEv1. Enter 2 to choose IKEv2. Default: IKEv1
IKE Integrity Protocol	Choose one of the following modes for the exchange of keying information and setting up IKE security associations: • **Main**: Establishes an IKE SA session before starting IPsec negotiations. • **Aggressive**: Negotiation is quicker, and the initiator and responder ID pass in the clear. Aggressive mode does not provide identity protection for communicating parties. Default: Main mode
IKE Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 14400 seconds (4 hours)
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Values: aes128-cbc-sha1, aes128-cbc-sha2, aes256-cbc-sha1, aes256-cbc-sha2 Default: aes256-cbc-sha1
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchanges. Values: 2, 14, 15, 16, 19, 20, 21, 24 Default: 16
IKE ID for Local End Point	If the remote IKE peer requires a local endpoint identifier, specify it. Range: 1 through 64 characters Default: Source IP address of the tunnel
IKE ID for Remote End Point	If the remote IKE peer requires a remote end point identifier, specify it. Range: 1 through 64 characters Default: Destination IP address of the tunnel There is no default option if you have chosen IKEv2.

d) Configure IPSEC fields.

Table 232: IPSEC

Field	Description
IPsec Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 3600 seconds
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. Values: 64, 128, 256, 512, 1024, 2048, 4096, 8192 bytes Default: 512 bytes
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Values: **aes256-cbc-sha1**, **aes256-gcm**, **null-sha1** Default: **aes256-gcm**
Perfect Forward Secrecy	Specify the PFS settings to use on the IPsec tunnel by choosing one of the following values: • **group-2**: Use the 1024-bit Diffie-Hellman prime modulus group • **group-14**: Use the 2048-bit Diffie-Hellman prime modulus group • **group-15**: Use the 3072-bit Diffie-Hellman prime modulus group • **group-16**: Use the 4096-bit Diffie-Hellman prime modulus group • **none**: Disable PFS Default: **group-16**
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. Range: 10 through 3600 seconds (1 hour) Default: 10 seconds
DPD Retries	Specify how many unacknowledged packets to accept before declaring an IKE peer to be dead and then removing the tunnel to the peer. Range: 2 through 60 Default: 3
Application	Choose an application from the drop-down list: • None • Sig

e) Configure advanced fields.

Table 233: Advanced

Field	Description
Shutdown	Click **Off** to enable the interface.
IP MTU	Based on your choice in the **Tunnel Mode** option, specify the maximum MTU size of the IPv6 packets on the interface. Range: 576 through 9216 Default: 1500 bytes
TCP MSS	Based on your choice in the **Tunnel Mode** option, specify the maximum segment size (MSS) of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: None
Clear-Dont-Fragment	Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface.
Tunnel Protection	Choose **Yes** to enable tunnel protection. Default: No

What to do next

Also see Deploy a configuration group.

Configure GRE on service VPN using a configuration group

Follow these steps to configure GRE on service VPN using a configuration group.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure GRE in Service Profile.

a) Configure Basic Configuration fields.

Table 234: Basic Configuration

Field	Description
Interface Name (1..255)*	Enter the name of the GRE interface, in the format **grenumber**. The value for **number** can be from 1 through 255.
Interface Description	Enter a description of the GRE interface.
Tunnel Mode	Choose from one of the following GRE tunnel modes: • **ipv4 underlay**: GRE tunnel with IPv4 underlay. IPv4 underlay is the default value. • **ipv6 underlay**: GRE tunnel with IPv6 underlay.
Preshared Key for IKE	Enter the preshared key (PSK) for authentication.

b) Configure Tunnel Fields.

Table 235: Tunnel

Field	Description
Source	Enter the source of the GRE interface: • **IP Address**: Enter the source IP address of the GRE tunnel interface. Based on the option you selected in the **Tunnel Mode** drop-down list, enter an IPv4 or an IPv6 address. This address is on the local router. • **Interface**: Enter the egress interface name for the GRE tunnel. • **Tunnel Route Via***: Specify the tunnel route details to steer the GRE tunnel traffic through. **Note** If the Tunnel Source Interface type is a loopback interface, enter the interface for traffic to be routed to. You cannot use the tunnel route via option to configure IPSec tunnels on a cellular interface because cellular interfaces do not include a next hop IP address for the default route.
Destination	Enter the source of the GRE interface: • **GRE Destination IP Address***: Enter the destination IP address of the GRE tunnel interface. This address is on a remote device. • **IP Address**: Based on the option you selected in the **Tunnel Mode** drop-down list, enter an IPv4 or an IPv6 address for the GRE tunnel. • **Mask***: Enter the subnet mask. • **IPv6 Address**: Enter the destination IPv6 or address for the GRE tunnel.

c) Configure IKE fields.

Table 236: IKE

Field	Description
IKE Version	Enter 1 to choose IKEv1. Enter 2 to choose IKEv2. Default: IKEv1
IKE Integrity Protocol	Choose one of the following modes for the exchange of keying information and setting up IKE security associations: • **Main**: Establishes an IKE SA session before starting IPsec negotiations. • **Aggressive**: Negotiation is quicker, and the initiator and responder ID pass in the clear. Aggressive mode does not provide identity protection for communicating parties. Default: Main mode
IKE Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 14400 seconds (4 hours)
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Values: aes128-cbc-sha1, aes128-cbc-sha2, aes256-cbc-sha1, aes256-cbc-sha2 Default: aes256-cbc-sha1
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchanges. Values: 2, 14, 15, 16, 19, 20, 21, 24 Default: 16
IKE ID for Local End Point	If the remote IKE peer requires a local endpoint identifier, specify it. Range: 1 through 64 characters Default: Source IP address of the tunnel
IKE ID for Remote End Point	If the remote IKE peer requires a remote end point identifier, specify it. Range: 1 through 64 characters Default: Destination IP address of the tunnel There is no default option if you have chosen IKEv2.

d) Configure IPSEC fields.

Table 237: IPSEC

Field	Description
IPsec Rekey Interval (Seconds)	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 3600 seconds
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. Values: 64, 128, 256, 512, 1024, 2048, 4096, 8192 bytes Default: 512 bytes
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Values: **aes256-cbc-sha1**, **aes256-gcm**, **null-sha1** Default: **aes256-gcm**
Perfect Forward Secrecy	Specify the PFS settings to use on the IPsec tunnel by choosing one of the following values: • **group-2**: Use the 1024-bit Diffie-Hellman prime modulus group • **group-14**: Use the 2048-bit Diffie-Hellman prime modulus group • **group-15**: Use the 3072-bit Diffie-Hellman prime modulus group • **group-16**: Use the 4096-bit Diffie-Hellman prime modulus group • **none**: Disable PFS Default: **group-16**
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. Range: 10 through 3600 seconds (1 hour) Default: 10 seconds
DPD Retries	Specify how many unacknowledged packets to accept before declaring an IKE peer to be dead and then removing the tunnel to the peer. Range: 2 through 60 Default: 3
Application	Choose an application from the drop-down list: • None • Sig

e) Configure advanced fields.

Table 238: Advanced

Field	Description
Shutdown	Click **Off** to enable the interface.
IP MTU	Based on your choice in the **Tunnel Mode** option, specify the maximum MTU size of the IPv4 or IPv6 packets on the interface. Range: 576 through 9216 Default: 1500 bytes
TCP MSS	Specify the maximum segment size (MSS) of the IPv4 TPC SYN packets passing through the Cisco vEdge device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: None
IPv6 TCP MSS	Specify the maximum segment size (MSS) of the IPv6 TPC SYN packets passing through the Cisco vEdge device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: None
Clear-Dont-Fragment	Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface.
Tunnel Protection	Choose **Yes** to enable tunnel protection. Default: No

What to do next

Also see Deploy a configuration group.

Configure VPN Interface GRE using templates

Follow these steps to configure VPN interface GRE using a feature template.

To configure GRE interfaces using Cisco SD-WAN Manager templates:

1. Create a Cisco VPN Interface GRE feature template to configure a GRE interface.
2. Create a Cisco VPN feature template to advertise a service that is reachable via a GRE tunnel, to configure GRE-specific static routes, and to configure other VPN parameters.
3. Create a data policy on the Cisco SD-WAN Controller that applies to the service VPN, including a **set-service** *service-name* **local** command.

When a service, such as a firewall, is available on a device that supports only GRE tunnels, you can configure a GRE tunnel on the device to connect to the remote device by configuring a logical GRE interface. You then advertise that the service is available via a GRE tunnel, and you can create data policies to direct the appropriate traffic to the tunnel. GRE interfaces come up as soon as they are configured, and they stay up as long as the physical tunnel interface is up.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Device Templates**.

In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

Step 3 From the **Create Template** drop-down list, select **From Feature Template**.

a) From the **Device Model** drop-down list, select the type of device for which you are creating the template.
b) Click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.
c) Under **Additional VPN 0 Templates**, click **VPN Interface GRE**.
d) From the **VPN Interface GRE** drop-down list, click **Create Template**. The VPN Interface GRE template form is displayed.
e) In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
f) In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

Step 4 Configure the following VPN interface GRE parameters:

a) Configure a basic GRE interface.

Table 239:

Parameter Name	Description
Shutdown*	Click **Off** to enable the interface.
Interface Name*	Enter the name of the GRE interface, in the format **gre** *number*. *number* can be from 1 through 255.
Description	Enter a description of the GRE interface.
Source*	Enter the source of the GRE interface: • GRE Source IP Address—Enter the source IP address of the GRE tunnel interface. This address is on the local router. This address is on the local router. GRE keepalives can not be configured when source configured as IP address. • Tunnel Source Interface—Enter the physical interface that is the source of the GRE tunnel. GRE keepalives can not be configured when source configured as loopback interface. • If you selected the Source as **Interface**, enter the name of the source interface. If you enter a loopback interface, an additional field **Tunnel Route-via Interface** displays where you enter the egress interface name.

Parameter Name	Description
Destination*	Enter the destination IP address of the GRE tunnel interface. This address is on a remote device. If this tunnel connects to a Secure Internet Gateway (SIG), specify the URL for the SIG.
GRE Destination IP Address*	Enter the destination IP address of the GRE tunnel interface. This address is on a remote device
IPv4 Address	Enter an IPv4 address for the GRE tunnel.
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 through 1804 Default: 1500 bytes
Clear-Dont-Fragment	Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface.
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes Default: None

b) Configure access lists on a GRE interface.

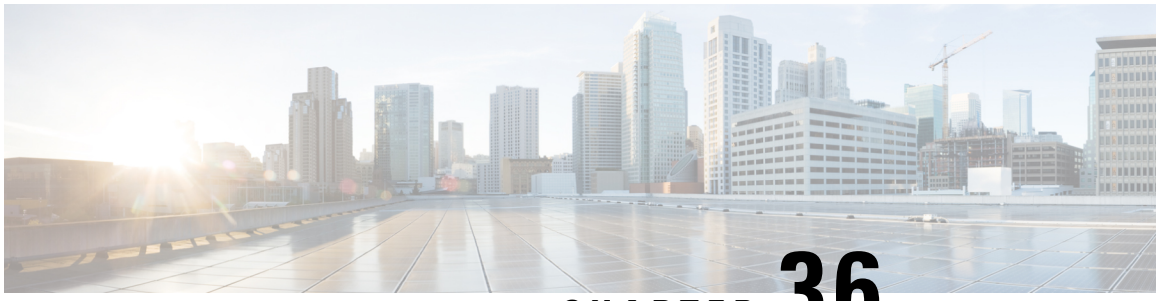
Table 240:

Parameter Name	Description
Rewrite Rule	Click **On**, and specify the name of the rewrite rule to apply on the interface.
Ingress ACL – IPv4	Click **On**, and specify the name of the access list to apply to IPv4 packets being received on the interface.
Egress ACL – IPv4	Click **On**, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface.

c) Configure a tracker interface to track the status of a GRE interface.

Table 241:

Parameter Name	Description
Tracker	Enter the name of a tracker to track the status of GRE interfaces that connect to the Internet.



CHAPTER 36

VPN Interface IPsec

- Feature history for VPN interface IPsec, on page 637
- Configure VPN interface IPsec, on page 637
- CLI configuration examples for VPN interface IPsec, on page 652

Feature history for VPN interface IPsec

Table 242: Feature History

Feature Name	Release Information	Description
SHA256 Support for IPSec Tunnels	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This feature adds support for `HMAC_SHA256` algorithms for enhanced security.

Configure VPN interface IPsec

Use one of these methods to configure geofencing:

- Configuration group
- Feature template

Note Some configurations and protocols are identified as insecure and is a security risk for Cisco devices. Existing deployments continue to function, but new installations require intentional enablement. For more information on remediation, refer to Resilient Infrastructure: Cisco Catalyst SD-WAN and Routing

Configure IPsec on the transport VPN using a configuration group

Follow these steps to configure IPSEC on the transport VPN using a configuration group.

If...

- you are running Cisco SD-WAN Manager releases from SD-WAN Manager 20.15.1 to SD-WAN Manager 20.15.3, and
- you are using the IPSEC feature to configure an edge device using Cisco IOS XE Catalyst SD-WAN Release 17.12.x or earlier,

then you must also configure a command using a CLI add-on profile. This command provides backward compatibility for edge devices using Cisco IOS XE Catalyst SD-WAN Release 17.12.x or earlier. Without this, the tunnel does not operate correctly.

To do this, create the CLI add-on profile and add it to the configuration group that you are using the configure the device. In the profile, include the **tunnel mode ipsec ipv4-old** command.

Using the CLI add-on profile with the **tunnel mode ipsec ipv4-old** command is not necessary in these releases:

- SD-WAN Manager 20.15.4 and later releases of 20.15.x
- SD-WAN Manager 20.18.1 and later releases

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure the basic IPSEC.

a) Configure a basic IPsec tunnel interface.

Table 243: Basic Configuration

Field	Description
Interface Name	Enter the name of the IPsec interface.
Description	Enter a description of the IPsec interface.
Tunnel Mode	Choose from one of the following IPsec tunnel modes: • **ipv4**: IPsec tunnel with IPv4 overlay and IPv4 underlay. IPv4 underlay is the default value. • **ipv6**: IPsec tunnel with IPv6 overlay and IPv6 underlay. • **ipv4-v6overlay**: IPsec tunnel with IPv6 overlay and IPv4 underlay.
Multiplexing	Choose **Yes** to enable multiplexing, if there is a tunnel in the transport VPN. Default: No
Interface Address	Enter the IPv4 or IPv6 address of the IPsec interface, based on your choice from the **Tunnel Mode** drop-down list.
Mask	Enter the subnet mask.

Field	Description
Preshared Key for IKE	Enter the preshared key (PSK) for authentication.
Associated Tracker / Tracker Group	Choose a tracker or a tracker group from the drop-down list to associate with the IPsec tunnel.
Tunnel Source	Enter the source of the IPsec interface: • **IP Address**: Enter the source IP address of the IPsec tunnel interface. Enter an IPv4 or IPv6 address that is based on your selection in the **Tunnel Mode** option. This address is on the local router. • **Interface**: Enter the physical interface in the **IPsec Source Interface** field, which is the source of the IPsec tunnel.
Tunnel Destination	Enter the destination IP address of the IPsec tunnel interface. This address is on a remote device. • **Address**: Enter the destination IP address of the IPsec tunnel interface. Enter an IPv4 or IPv6 address based on your selection in the **Tunnel Mode** option. • **Application**: Choose an application from the drop-down list. • **None** • **Sig**

b) Configure Internet Key Exchange fields.

Table 244: Internet Key Exchange

Field	Description
IKE Version	Enter 1 to choose IKEv1. Enter 2 to choose IKEv2. Default: IKEv1
IKE Integrity Protocol	Choose one of the following modes for the exchange of keying information and setting up IKE security associations: • **Main**: Establishes an IKE SA session before starting IPsec negotiations. • **Aggressive**: Negotiation is quicker, and the initiator and responder ID pass in the clear. Aggressive mode does not provide identity protection for communicating parties. Default: Main mode
IPsec Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 14400 seconds (4 hours)

Field	Description
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Values: aes128-cbc-sha1, aes128-cbc-sha2, aes256-cbc-sha1, aes256-cbc-sha2 Default: aes256-cbc-sha1
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchanges. Values: 2, 14, 15, 16, 19, 20, 21, 24 Default: 16
IKE ID for Local End Point	If the remote IKE peer requires a local endpoint identifier, specify it. Range: 1 through 64 characters Default: Source IP address of the tunnel
IKE ID for Remote End Point	If the remote IKE peer requires a remote endpoint identifier, specify it. Range: 1 through 64 characters Default: Destination IP address of the tunnel There is no default option if you choose IKEv2.

c) Configure IPSEC fields.

Table 245: IPSEC

Field	Description
IPsec Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 3600 seconds (1 hour)
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. Values: 64, 128, 256, 512, 1024, 2048, 4096, 8192 bytes Default: 512 bytes
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Values: **aes256-cbc-sha1**, **aes256-gcm**, **null-sha1** Default: **aes256-gcm**

Field	Description
Perfect Forward Secrecy	Specify the PFS settings to use on the IPsec tunnel by choosing one of the following values: • **group-2**: Use the 1024 bit Diffie-Hellman prime modulus group • **group-14**: Use the 2048 bit Diffie-Hellman prime modulus group • **group-15**: Use the 3072 bit Diffie-Hellman prime modulus group • **group-16**: Use the 4096 bit Diffie-Hellman prime modulus group • **none**: Disable PFS Default: **group-16**

d) Configure advanced IPsec fields.

Table 246: Advanced

Field	Description
Associated VPN	Select a VPN from the drop-down list to associate with the IPsec tunnel.
Tunnel Route Via	Specify the tunnel route details to steer the application traffic through. **Note** You cannot use the tunnel route via option to configure IPSec tunnels on a cellular interface because cellular interfaces do not include a next hop IP address for the default route.
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. Range: 10 through 3600 seconds (1 hour) Default: 10 seconds
DPD Retries	Specify how many unacknowledged packets to accept before declaring an IKE peer to be dead and then removing the tunnel to the peer. Range: 2 through 60 Default: 3
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: None
Clear-Dont-Fragment	Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface.

Field	Description
IP MTU	Based on your choice in the **Tunnel Mode** option, specify the maximum MTU size of the IPv4 or IPv4 packets on the interface. Range: 576 through 9216 Default: 1500 bytes
Shutdown	Click **Off** to enable the interface.

What to do next

Also see Deploy a configuration group.

Configure IPsec on the service VPN using a configuration group

Follow these steps to configure IPsec on the service VPN using a configuration group.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure the VPN interface IPsec feature.

a) Configure basic configuration fields.

Table 247: Basic Configuration

Field	Description
Interface Name	Enter the name of the IPsec interface.
Description	Enter a description of the IPsec interface.
Tunnel Mode	Choose from one of the following IPsec tunnel modes: • **ipv4**: IPsec tunnel with IPv4 overlay and IPv4 underlay. IPv4 underlay is the default value. • **ipv6**: IPsec tunnel with IPv6 overlay and IPv6 underlay. • **ipv4-v6overlay**: IPsec tunnel with IPv6 overlay and IPv4 underlay.
Interface Address	Enter the IPv4 or IPv6 address of the IPsec interface, based on your choice from the **Tunnel Mode** drop-down list.
Mask	Enter the subnet mask.

Field	Description
Tunnel Source	Enter the source of the IPsec interface: • **IP Address**: Enter the IPv4 or IPv6 address of the IPsec interface, based on your choice from the **Tunnel Mode** drop-down list.. This address is on the local router. • **Interface**: Enter the physical interface that is the source of the IPsec tunnel.
Tunnel Destination	Enter the destination of the IPsec interface: • **Address**: Enter the destination IPv4 or IPv6 address of the IPsec interface, based on your choice from the **Tunnel Mode** drop-down list. This address is on a remote device. • **Application**: Choose an application from the drop-down list. • None • Sig
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the vEdge router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: None
Clear-Dont-Fragment	Click On to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface.
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 through 1804 Default: 1500 bytes

b) Configure IKE fields.

Table 248: Internet Key Exchange

Field	Description
IKE Version	Enter 1 to choose IKEv1. Enter 2 to choose IKEv2. Default: IKEv1

Field	Description
IKE Integrity Protocol	Choose one of the following modes for the exchange of keying information and setting up IKE security associations: • **Main**: Establishes an IKE SA session before starting IPsec negotiations. • **Aggressive**: Negotiation is quicker, and the initiator and responder ID pass in the clear. Aggressive mode does not provide identity protection for communicating parties. Default: Main mode
IPsec Rekey Interval (Seconds)	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 14400 seconds (4 hours)
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Values: aes128-cbc-sha1, aes128-cbc-sha2, aes256-cbc-sha1, aes256-cbc-sha2 Default: aes256-cbc-sha1
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchanges. Values: 2, 14, 15, 16, 19, 20, 21, 24 Default: 16
IKE ID for Local End Point	If the remote IKE peer requires a local endpoint identifier, specify it. Range: 1 through 64 characters Default: Source IP address of the tunnel
IKE ID for Remote End Point	If the remote IKE peer requires a remote end point identifier, specify it. Range: 1 through 64 characters Default: Destination IP address of the tunnel There is no default option if you have chosen IKEv2.

c) Configure IPsec fields.

Table 249: IPSEC

Field	Description
IPsec Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 3600 seconds

Field	Description
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. Values: 64, 128, 256, 512, 1024, 2048, 4096, 8192 bytes Default: 512 bytes
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Values: **aes256-cbc-sha1**, **aes256-gcm**, **null-sha1** Default: **aes256-gcm**
Perfect Forward Secrecy	Specify the PFS settings to use on the IPsec tunnel by choosing one of the following values: • **group-2**: Use the 1024-bit Diffie-Hellman prime modulus group • **group-14**: Use the 2048-bit Diffie-Hellman prime modulus group • **group-15**: Use the 3072-bit Diffie-Hellman prime modulus group • **group-16**: Use the 4096-bit Diffie-Hellman prime modulus group • **none**: Disable PFS Default: **group-16**

d) Configure advanced fields.

Table 250: Advanced

Field	Description
Associated VPN	Select a VPN from the drop-down list to associate with the IPsec tunnel.
Tunnel Route Via	Specify the tunnel route details to steer the application traffic through. **Note** You cannot use the tunnel route via option to configure IPSec tunnels on a cellular interface because cellular interfaces do not include a next hop IP address for the default route.
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. Range: 10 through 3600 seconds (1 hour) Default: 10 seconds
DPD Retries	Specify how many unacknowledged packets to accept before declaring an IKE peer to be dead and then removing the tunnel to the peer. Range: 2 through 60 Default: 3

Field	Description
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the Cisco vEdge device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: None
Clear-Dont-Fragment	Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface.
IP MTU	Based on your choice in the **Tunnel Mode** option, specify the maximum MTU size of the IPv4 or IPv4 packets on the interface. Range: 576 through 9216 Default: 1500 bytes
Shutdown	Click **Off** to enable the interface.

What to do next

Also see Deploy a configuration group.

Configure VPN interface IPsec using templates

Follow these steps to configure VPN interface IPsec using a feature template.

Use the VPN Interface IPsec feature template to configure IPsec tunnels on Cisco IOS XE service VPNs that are being used for Internet Key Exchange (IKE) sessions. You can configure IPsec on tunnels for VPN 1 through 65527, except for 512.

Cisco IOS XE Catalyst SD-WAN devices use VRFs in place of VPNs. However, the following steps still apply to configure Cisco IOS XE Catalyst SD-WAN devices through Cisco SD-WAN Manager. In Cisco SD-WAN Manager, the system automatically maps the VPN configurations to VRF configurations.

In controller mode, only Route based IPSec tunnels are supported.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**.

In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

a) Click **Add Template**.
b) Choose a Cisco IOS XE Catalyst SD-WAN device from the list.
c) From the VPN section, click **VPN Interface IPsec**. The Cisco VPN Interface IPsec template displays.

d) In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
e) In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

Step 3 Configure the following VPN interface IPsec parameters:

a) Configure a basic IPsec tunnel interface.

Parameter Name	Options/Format	Description
Shutdown*	**Yes** / **No**	Click **No** to enable the interface; click **Yes** to disable.
Interface Name*	**ipsec** *number* (1…255)	Enter the name of the IPsec interface. *Number* can be from 1 through 255.
Description	Enter a description of the IPsec interface.	
IPv4 Address*	*ipv4-prefix/length*	Enter the IPv4 address of the IPsec interface. The address must have a **/30** subnet.
Source *	Set the source of the IPsec tunnel that is being used for IKE key exchange:	
	IP Address	Click and enter the IPv4 address that is the source tunnel interface. This address must be configured in **VPN 0**.
	Interface	Click and enter the name of the physical interface that is the source of the IPsec tunnel. This interface must be configured in **VPN 0**. • If you selected the Source as **Interface**, enter the name of the source interface. If you enter a loopback interface, an additional field **Tunnel Route-via Interface** displays where you enter the egress interface name. **Note** You cannot use the tunnel route via option to configure IPSec tunnels on a cellular interface because cellular interfaces do not include a next hop IP address for the default route.

Parameter Name	Options/Format	Description
Destination*	Set the destination of the IPsec tunnel that is being used for IKE key exchange.	
	IPsec Destination IP Address	Enter an IPv4 address that points to the destination.
	TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. *Range:* 552 to 1960 bytes *Default:* None
	IP MTU	Specify the maximum transmission unit (MTU) size of packets on the interface. *Range:* 576 through 2000 *Default:* 1500 bytes

b) Configure Internet key exchange (IKE) dead-peer detection (DPD) to determine whether the connection to an IKE peer is functional and reachable.

Parameter Name	Description
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. Range: 10 through 3600 seconds Default: Disabled
DPD Retries	Specify how many unacknowledged packets to accept before declaring an IKE peer to be dead and then tearing down the tunnel to the peer. Range: 2 through 60 Default: 3

c) Configure IKE.

When you create an IPsec tunnel on a Cisco IOS XE Catalyst SD-WAN device, IKE Version 1 is enabled by default on the tunnel interface.

Parameter Name	Options	Description
IKE Version	**1** IKEv1 **2** IKEv2	Enter **1** to choose IKEv1. Enter **2** to choose IKEv2. Default: IKEv1 **Note** In IKEv2 Preshared Keys (PSK), the '\' character is not supported and should not be used.

Parameter Name	Options	Description
IKE Mode	**Aggressive mode** **Main mode**	For IKEv1 only, specify one of the following modes: • Aggressive mode - Negotiation is quicker, and the initiator and responder ID pass in the clear. • Establishes an IKE SA session before starting IPsec negotiations. **Note** For IKEv2, there is no mode. **Note** IKE aggressive mode with pre-shared keys should be avoided where possible. Otherwise a strong pre-shared key should be chosen. Default: Main mode
IPsec Rekey Interval	3600 - 1209600 seconds	Specify the interval for refreshing IKE keys. Range: 1 hour through 14 days Default: 14400 seconds (4 hours)
IKE Cipher Suite	• AES 256 CBC SHA 256 • AES 256 CBC SHA 384 • AES 256 CBC SHA 512 • AES 256 CBC SHA 1 • AES 256 GCM • Nul SHA 256 • Nul SHA 384 • Nul SHA 512 • Nul SHA 1	Specify the type of authentication and encryption to use during IKE key exchange. Default: AES 256 CBC SHA 1

Parameter Name	Options	Description
IKE Diffie-Hellman Group	**2** **14** **15** **16**	Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2. • 1024-bit modulus • 2048-bit modulus • 3072-bit modulus • 4096-bit modulus Default: 4096-bit modulus
IKE Authentication	Configure IKE authentication.	
	Preshared Key	Enter the password to use with the preshared key.
	IKE ID for Local End Point	If the remote IKE peer requires a local end point identifier, specify it. Range: 1 through 64 characters Default: Tunnel's source IP address
	IKE ID for Remote End Point	If the remote IKE peer requires a remote end point identifier, specify it. Range: 1 through 64 characters Default: Tunnel's destination IP address

When you are pushing authentication from Cisco SD-WAN Manager, use the authentication string configured for the source and destination stations in double quotes as special characters are not supported. The string can be up to eight characters long.

d) Configure the IPsec tunnel that carries Internet Key Exchange (IKE) traffic.

Parameter Name	Options	Description
IPsec Rekey Interval	3600 - 1209600 seconds	Specify the interval for refreshing IKE keys. Range: 1 hour through 14 days Default: 3600 seconds
IKE Replay Window	64, 128, 256, 512, 1024, 2048, 4096, 8192	Specify the replay window size for the IPsec tunnel. Default: 512
IPsec Cipher Suite	aes256-cbc-sha1 aes256-gcm null-sha1	Specify the authentication and encryption to use on the IPsec tunnel Default: aes256-gcm

Parameter Name	Options	Description
Perfect Forward Secrecy	**2** 1024-bit modulus **14** 2048-bit modulus **15** 3072-bit modulus **16** 4096-bit modulus **none**	Specify the PFS settings to use on the IPsec tunnel. Choose one of the following Diffie-Hellman prime modulus groups: 1024-bit – group-2 2048-bit – group-14 3072-bit – group-15 4096-bit – group-16 none –disable PFS. *Default*: group-16

From Cisco IOS XE Catalyst SD-WAN Release 17.11.1a, as part of the security hardening, the weaker ciphers are deprecated. As part of this change, the option to configure Diffie-Hellman (DH) groups 1, 2, and 5 is no longer supported. DH groups are used in IKE to establish session keys and are also available in IPsec as support for perfect forward secrecy.

Change the IKE version from IKEv1 to IKEv2

Follow these steps to change the IKE version.

There is no single CLI for changing the IKE version. You need to follow the sequence of steps listed in the Change the IKE Version from IKEv1 to IKEv2 section.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**, and then click **Add Template**.

In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

Step 3 Choose the device for which you are creating the template.

Step 4 Click **Basic Configuration**.

Step 5 Use the **shutdown** parameter with the **yes** option (**yes shutdown**) to shut down the tunnel.

Step 6 Remove the ISAKMP profile from the IPsec profile.

Step 7 Attach the IKEv2 profile with the IPsec profile.

Perform this step if you already have an IKEv2 profile. Otherwise, create an IKEv2 profile first.

Step 8 Use the **shutdown** parameter with the **no** option (**no shutdown**) to start up the tunnel.

You must issue the **shutdown** operations in two separate operations.

CLI configuration examples for VPN interface IPsec

Basic configuration

The following is an example of the basic IPsec tunnel interface configuration.

```
crypto
   interface tunnel ifnum
      no shutdown
      vrf forwarding vrf_id
      ip address ip_address[mask]
      tunnel source wanif_ip
      tunnel mode {ipsec ipv4 | gre ip}
      tunnel destination gateway_ip
      tunnel protection ipsec profile ipsec_profile_name
```

Dead-Peer detection

The following is an example of Internet key exchange (IKE) dead-peer detection (DPD) configuration.

```
crypto
   ikev2
      profile ikev2_profile_name
         dpd 10-3600 2-60 {on-demand | periodic}
```

IKE

The following is an example of ISAKMP CLI configuration for IKEv1.

```
crypto
   isakmp
      keepalive 60-86400 2-60 {on-demand | periodic}
      policy policy_num
         encryption {AES128-CBC-SHA1 | AES256-CBC-SHA1}
         hash {sha384 | sha256 | sha}
         authentication pre-share
         group {2 | 14 | 16 | 19 | 20 | 21}
         lifetime 60-86400
      profile ikev1_profile_name
         match identity address ip_address [mask]
         keyring keyring_name
```

The following is an example of IPsec CLI configuration for IKEv1.

```
profile ipsec_profile_name
         set transform-set transform_set_name
         set isakmp-profile ikev1_profile_name
         set security-association
            lifetime {kilobytes disable | seconds 120-2592000}
            replay {disable | window-size [64 | 128 | 256 | 512 | 1024]}
         set pfs group {14 | 16 | 19 | 20 | 21}
   keyring keyring_name
      pre-shared-key address ip_address [mask] key key_string
   ipsec transform-set transform_set_name {esp-gcm 256 | esp-aes 256 [esp-sha384-hmac |
esp-sha256-hmac] mode tunnel
```

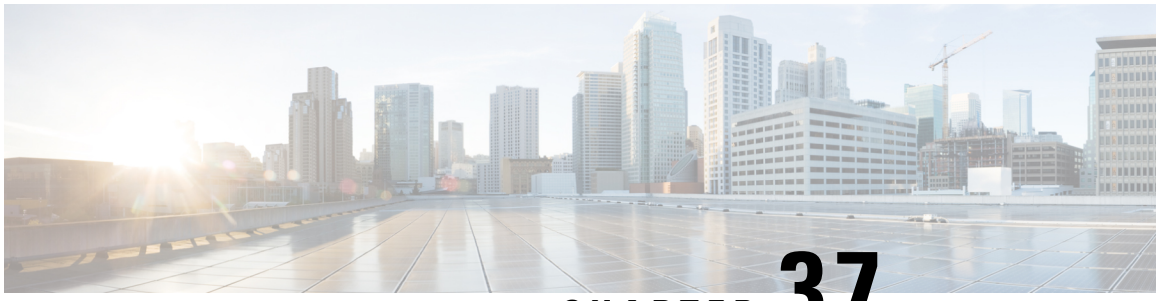
The following is an example configuration for IKE2.

```
crypto
   ikev2
      proposal proposal_name
         encryption {3des | aes-cbc-128 | aes-cbc-192 | aes-cbc-256 | des}
         integrity {sha256 | sha384 | sha512}
         group {2 | 14 | 15 | 16}
      keyring idev2_keyring_name
         peer peer_name
         address tunnel_dest_ip [mask]
         pre-shared-key key_string
      profile ikev2_profile_name
         match identity remote address ip_address
         authentication {remote | local} pre-share
         keyring local ikev2_keyring_name
         lifetime 120-86400
```

IPsec tunnel

The following is an example configuration of IPsec tunnels.

```
crypto
   ipsec
      profile ipsec_profile_name
         set ikev2-profile ikev2_profile_name
         set security-association
            lifetime {seconds 120-2592000 | kilobytes disable}
            replay {disable | window-size {64 | 128 | 256 | 512 | 1024 | 4096 | 8192}
         set pfs group {2 | 14 | 15 | 16 | none}
         set transform-set transform_set_name
```



CHAPTER 37

VPN Interface Multilink

- Configure VPN interface multilink, on page 655

Configure VPN interface multilink

Use one of these methods to configure VPN interface multilink:

- Configuration group
- Feature template

Configure VPN interface multilink using a configuration group

Follow these steps to configure VPN interface multilink using a configuration group.

Multilink Point-to-Point Protocol (MLP) is used to combine multiple physical links into a single logical connection, called an MLP bundle.

Use the VPN Interface Multilink feature to configure multilink interface properties for Cisco SD-WAN Manager devices.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure VPN Interface Multilink in a service profile.

a) Enter the basic configuration information.

Table 251: Basic Configuration

Parameter Name	Description
Interface Name	Enter the name of the multilink interface.

Parameter Name	Description
Multilink Group Number *	Enter the number of the multilink group. It must be the same as the number you enter in the multilink interface name parameter. Range: 1 through 65535
PPP Authentication Protocol	Select the authentication protocol used by the multilink interface: • **CHAP**: Enter the hostname and password provided by your Internet Service Provider (ISP). *hostname* can be up to 254 characters. • **PAP**: Enter the username and password provided by your ISP. *username* can be up to 254 characters. • **PAP** and **CHAP**: Configure both authentication protocols. Enter the login credentials for each protocol. To use the same username and password for both, click Same Credentials for PAP and CHAP.
Hostname *	Enter hostname for PPP CHAP Authentication.
CHAP Password *	Enter password for PPP CHAP Authentication.
IPv4 Address *	To configure a static address, click **Static** and enter an IPv4 address. To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click Dynamic. You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. Default: 1
Mask	Choose a value for the subnet mask.
IPv6 Address *	To configure a static address for an interface in VPN 0, click Static and enter an IPv6 address. To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click Dynamic. You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. The default DHCP distance is 1. You can optionally enable DHCP rapid commit, to speed up the assignment of IP addresses.

b) Enter multilink information

Table 252: Multilink

Parameter Name	Description
Add T1/E1 Interface	
T1	
Description	Enter a description for the T1controller.

Parameter Name	Description
Slot*	Enter the number of the slot in slot/subslot/port format, where the T1 NIM is installed. For example, 0/1/0.
Framing	Enter the T1 frame type: • **esf**: Send T1 frames as extended superframes. This is the default. • **sf**: Send T1 frames as superframes. Superframing is sometimes called D4 framing.
Clock Source	Select the clock source: • **line**: Use phase-locked loop (PLL) on the interface. This is the default. When both T1 ports use line clocking and neither port is configured as the primary, by default, port 0 is the primary clock source and port 1 is the secondary clock source. • **internal**: Use the controller framer as the primary clock.
Line Code	Select the line encoding to use to send T1 frames: • **ami**: Use alternate mark inversion (AMI) as the linecode. AMI signaling uses frames grouped into superframes. • **b8zs**: Use bipolar 8-zero substitution as the linecode. This is the default. B8ZS uses frames that are grouped into extended superframes.
Cable Length	Select the cable length to configure the attenuation • **short**: Set the transmission attenuation for cables that are 660 feet or shorter. • **long**: Attenuate the pulse from the transmitter using pulse equalization and line buildout. You can configure a long cable length for cables longer that 660 feet. There is no default length.
E1	
Description	Enter a description for the E1 controller.
Slot*	Enter the number of the slot in slot/subslot/port format, where the E1 NIM is installed. For example, 0/1/0.
Framing	Enter the E1 frame type: • **crc4**: Use cyclic redundancy check 4 (CRC4). This is the default. • **no-crc4**: Do no use CRC4.

Parameter Name	Description
Clock Source	Select the clock source: • **line**: Use phase-locked loop (PLL) on the interface. This is the default. When both E1 ports use line clocking and neither port is configured as the primary, by default, port 0 is the primary clock source and port 1 is the secondary clock source. • **internal**: Use the controller framer as the primary clock.
Line Code	Select the line encoding to use to send E1 frames: • **ami**: Use alternate mark inversion (AMI) as the linecode. • **hdb3**: Use high-density bipolar 3 as the linecode. This is the default.
Add Channel Group	
Channel Group	To configure the serial WAN on the interface, enter a channel group number. Range: 0 through 30
Time Slot	To configure the serial WAN on the interface, enter a value for the timeslot. Range: 0 through 31
Add New A/S Serial Interface	
Interface Name	Enter the name of the serial interface.
Description	Enter a description for the serial interface.
Bandwidth	For transmitted traffic, set the bandwidth above which to generate notifications.
Clock Rate	Specify a value for the clock rate. Range: 1200 through 800000

c) Enter tunnel information

Table 253: Tunnel

Parameter Name	Description
Color	Choose a color for the TLOC.
Color Description	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enter a description associated to the TLOC color.
Restrict	Enable this option to drop packets when a tunnel to the service is unreachable.
Groups	Enter the list of groups in the field.
Border	From the drop-down list, select **Global**. Click **On** to set TLOC as border TLOC.

Parameter Name	Description
Maximum Control Connections	Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8 Default: 2
Validator As Stun Server	Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT.
Exclude Controller Group List	Set the Cisco SD-WAN Controllers that the tunnel interface is not allowed to connect to. Range: 0 through 100
Cisco SD-WAN Manager Connection Preference	Set the preference for using a tunnel interface to exchange control traffic with Cisco SD-WAN Manager. Range: 0 through 8 Default: 5
Full Port Hop	Minimum release: Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled
Port Hop	From the drop-down list, select **Global**. Click **Off** to allow port hopping on tunnel interface. Default: **On**, which disallows port hopping on tunnel interface Starting from Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, this field is deprecated. Instead use the **Full Port Hop** option. See the **Full Port Hop** field.
Low-Bandwidth Link	Click **On** to set the tunnel interface as a low-bandwidth link. Default: **Off**
Network Broadcast	From the drop-down list, select **Global**. Click **On** to accept and respond to network-prefix-directed broadcasts. Enable this parameter only if the **Directed Broadcast** is enabled on the LAN interface feature template. Default: **Off**

Parameter Name	Description
Tunnel TCP MSS	TCP MSS affects any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS is examined against the MSS exchanged in the three-way handshake. The MSS in the header is lowered if the configured TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. To configure TCP MSS, provide a value that is 40 bytes lower than the minimum path MTU. Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes

d) Enter ACL information.

Table 254: ACL

Parameter Name	Description
Ingress ACL - IPv4	Enter the name of an IPv4 access list to packets being received on the interface.
Egress ACL - IPv4	Enter the name of an IPv4 access list to packets being transmitted on the interface.
Igress ACL - IPv6	Enter the name of an IPv6 access list to packets being received on the interface.
Egress ACL - IPv6	Enter the name of an IPv6 access list to packets being transmitted on the interface.

e) Enter advanced information.

Table 255: Advanced

Parameter Name	Description
Shutdown	Click **No** to enable the multilink interface.
Description	Enter a description for the multilink interface.
PPP Authentication Type	Select the type authentication from one of the following options.: • **Unidirectional**: The server initiates the authentication. • **Bidirectional**: Both the client and the server can initiate the authentication.

Parameter Name	Description
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the Cisco Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 500 through 1460 bytes Default: 536
Disable Fragmentation	Click **On** to disable fragmentation for PPP Multilink Protocol data units (PDUs).
Fragment Max Delay	Configure the delay between the transmission of fragments in a PPP Multilink Protocol link. Range: 0 through 1000 Default: No CLI Command
Interleaving Fragments	Enable interleave fragmentation for PPP Multilink Protocol data units (PDUs).
TLOC Extension	Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration binds the service-side interface to the WAN transport by enabling a device to access the opposite WAN transport connected to the neighbouring device using a TLOC-extension interface.
IP MTU	Specify the maximum MTU size of packets on the interface. MLP encapsulation adds 6 extra bytes (4 header, 2 checksum) to each outbound packet. These overhead bytes reduce the effective bandwidth on the connection; therefore, the throughput for an MLP bundle is slightly less than an equivalent bandwidth connection that is not using MLP. Range: 576 through 1804 Default: 1500 bytes
IP Directed-Broadcast	Enable the translation of a directed broadcast to physical broadcasts.
Shaping Rate (Kbps)	Configure the aggregate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).

What to do next

Also see Deploy a Configuration Group.

Configure VPN interface multilink using templates

Follow these steps to configure VPN interface multilink using a feature template.

Multilink Point-to-Point Protocol (MLP) is used to combine multiple physical links into a single logical connection, called an MLP bundle.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**.

In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

a) Click **Add Template**.
b) Choose a Cisco IOS XE Catalyst SD-WAN device from the list.
c) If you are configuring the multilink interface in the transport VPN (VPN 0), click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.

Under Additional VPN 0 Templates, located to the right of the screen, click **VPN Interface Multilink Controller**.

d) If you are configuring the multilink interface in a service VPN (VPNs other than VPN 0), click **Service VPN** or scroll to the **Service VPN** section.

In the Service **VPN** drop-down list, enter the number of the service VPN. Under Additional VPN Templates, located to the right of the screen, click **VPN Interface Multilink Controller**.

e) From the **VPN Interface Multilink Controller** drop-down list, click **Create Template**. The VPN Multilink template form is displayed. This form contains fields for naming the template, and fields for defining multilink Interface parameters.
f) In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
g) In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

Step 3 Configure the following parameters in the VPN interface multilink template.

a) Configure a multilink interface.

If you are creating a VPN Interface Multilink template, you do not need to create a T1/E1 Controller template or a VPN Interface T1/E1 template.

Table 256:

Parameter Name	Description
Shutdown*	Click **No** to enable the multilink interface.
Interface Name*	Enter the number of the MLP interface. It can be a number from 1 through 65,535.
Description	Enter a description for the multilink interface.
Multilink Group Number*	Enter the number of the multilink group. It can be a number from 1 through 65,535 but it must be the same as the number you enter in the Multilink Interface Name parameter.
IPv4 Address*	To configure a static address, click **Static** and enter an IPv4 address. To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click Dynamic. You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. The default DHCP distance is 1.

Parameter Name	Description
IPv6 Address*	To configure a static address for an interface in VPN 0, click Static and enter an IPv6 address. To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click Dynamic. You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. The default DHCP distance is 1. You can optionally enable DHCP rapid commit, to speed up the assignment of IP addresses.
Bandwidth Upstream	For transmitted traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32} / 2) – 1 kbps
Bandwidth Downstream	For received traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32} / 2) – 1 kbps
IP MTU	Specify the maximum MTU size of packets on the interface. MLP encapsulation adds 6 extra bytes (4 header, 2 checksum) to each outbound packet. These overhead bytes reduce the effective bandwidth on the connection; therefore, the throughput for an MLP bundle is slightly less than an equivalent bandwidth connection that is not using MLP. Range: 576 through 1804 Default: 1500 bytes

b) Configure the PPP authentication protocol.

Table 257:

Parameter Name	Description
Authentication Protocol	Select the authentication protocol used by the MLP: • **CHAP**—Enter the hostname and password provided by your Internet Service Provider (ISP). *hostname* can be up to 254 characters. • **PAP**—Enter the username and password provided by your ISP. *username* can be up to 254 characters. • **PAP** and **CHAP**—Configure both authentication protocols. Enter the login credentials for each protocol. To use the same username and password for both, click Same Credentials for PAP and CHAP.

c) Configure a tunnel interface for the multilink interface.

Table 258:

Parameter Name	Description
Tunnel Interface	Click **On** to create a tunnel interface.
Color	Select a color for the TLOC.

Parameter Name	Description
Color Description	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enter a description associated to the TLOC color.
Control Connection	By default, Control Conection is set to **On**, which establishes a control connection for the TLOC. If the router has multiple TLOCs, click **No** to have the tunnel not establish control connection for the TLOC. **Note** We recommend a minimum of 650-700 Kbps bandwidth with default 1 sec hello-interval and 12 sec hello-tolerance parameters configured to avoid any data/packet loss in connection traffic. For each BFD session, an additional average sized BFD packet of 175 Bytes consumes 1.4 Kbps of bandwidth. A sample calculation of the required bandwidth for bidirectional BFD packet flow is given below: • 650 – 700 Kbps per device for control connections. • 175 Bytes (or 1.4 Kbps) per BFD session on the device (request) • 175 Bytes (or 1.4 Kbps) per BFD session on the device (response) If the path MTU discovery (PMTUD) is enabled, bandwidth for send/receive BFD packets per tunnel for every 30 secs: A 1500 Bytes BFD request packet is sent per tunnel every 30 secs: 1500 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 400 bps (request) A 147 Bytes BFD packet is sent in response: 147 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 40 bps (response) Therefore, a device with 775 BFD sessions (for example) requires a bandwidth of: 700k + (1.4k*775) + (400 *775) + (1.4k*775) + (40 *775) = ~3,5 MBps
Maximum Control Connections	Specify the maximum number of Cisco SD-WAN Controller that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8 Default: 2
vBond As STUN Server	Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the device is located behind a NAT.
Exclude Controller Group List	Set the Cisco SD-WAN Controller that the tunnel interface is not allowed to connect to. Range: 0 through 100

Parameter Name	Description
vManage Connection Preference	Set the preference for using a tunnel interface to exchange control traffic with Cisco SD-WAN Manager. Range: 0 through 8 Default: 5
Full Port Hop	Minimum release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled
Port Hop	Click **On** to enable port hopping, or click **Off** to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. Default: Enabled Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, this field is deprecated. Instead use the **Full Port Hop** option. See the **Full Port Hop** field.
Low-Bandwidth Link	Select to characterize the tunnel interface as a low-bandwidth link.
Tunnel TCP MSS	TCP MSS affects any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS is examined against the MSS exchanged in the three-way handshake. The MSS in the header is lowered if the configured TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. If the TCP MSS is to be configured, it should be set at 40 bytes lower than the minimum path MTU. Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes Default: None
Clear-Dont-Fragment	Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent. Click **On** to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, packets larger than the MTU of the interface are fragmented before being sent. **Note** **Clear-Dont-Fragment** clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected.
Allow Service	Select **On** or **Off** for each service to allow or disallow the service on the interface.

To configure additional tunnel interface parameters, click **Advanced Options** and configure the following parameters:

Table 259:

Parameter Name	Description
GRE	Use GRE encapsulation on the tunnel interface. By default, GRE is disabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
IPsec	Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
IPsec Preference	Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295. Default: 0
IPsec Weight	Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255. Default: 1
Carrier	Select the carrier name or private network identifier to associate with the tunnel. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default. Default: default
Bind Loopback Tunnel	Enter the name of a physical interface to bind to a loopback interface.
Last-Resort Circuit	Select to use the tunnel interface as the circuit of last resort. **Note** An interface configured as a circuit of last resort is expected to be down and is skipped while calculating the number of control connections, the cellular modem becomes dormant, and no traffic is sent over the circuit. When the configurations are activated on the edge device with cellular interfaces, then all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down. Only when all the primary interfaces lose their connections to remote edges, then the circuit of last resort activates itself triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are used as backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode the radio interface is turned off, and no control or data connections exist over the cellular interface.

Parameter Name	Description
NAT Refresh Interval	Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds. Default: 5 seconds
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 10000 milliseconds. Default: 1000 milliseconds (1 second)
Hello Tolerance	Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down. Range: 12 through 60 seconds. Default: 12 seconds

d) Apply a rewrite rule, access lists, and policers to a router interface.

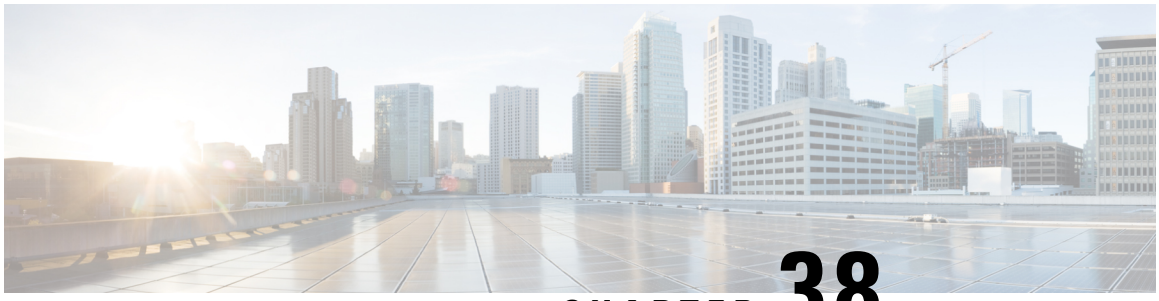
Table 260:

Parameter Name	Description
Shaping rate	Configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).
QoS map	Specify the name of the QoS map to apply to packets being transmitted out the interface.
Rewrite Rule	Click **On**, and specify the name of the rewrite rule to apply on the interface.
Ingress ACL – IPv4	Click **On**, and specify the name of the access list to apply to IPv4 packets being received on the interface.
Egress ACL – IPv4	Click **On**, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface.
Ingress ACL – IPv6	Click **On**, and specify the name of the access list to apply to IPv6 packets being received on the interface.
Egress ACL – IPv6	Click **On**, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface.
Ingress Policer	Click **On**, and specify the name of the policer to apply to packets being received on the interface.
Egress Policer	Click **On**, and specify the name of the policer to apply to packets being transmitted on the interface.

e) Configure other interface properties.

Table 261:

Parameter Name	Description
PMTU Discovery	Click **On** to enable path MTU discovery on the interface, to allow the router to determine the largest MTU size supported without requiring packet fragmentation.
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the Cisco Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes. Default: None
Clear Dont Fragment	Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent.
Static Ingress QoS	Select a queue number to use for incoming traffic. Range: 0 through 7
Auto negotiate	Click **Off** to turn off autonegotiation. By default, an interface runs in autonegotiation mode.
TLOC Extension	Enter the name of the physical interface on the same router that connects to the WAN transport circuit. This configuration then binds this service-side interface to the WAN transport. A second Cisco Catalyst SD-WAN device at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.



CHAPTER 38

VPN Interface SVI

- Feature history for VPN interface SVI, on page 669
- Configure VPN interface SVI, on page 669

Feature history for VPN interface SVI

Table 262: Feature History

Feature Name	Release Information	Description
Support for Configuring Secondary IP Address	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	You can configure up to four secondary IPv4 or IPv6 addresses, and up to four DHCP helpers. Secondary IP addresses can be useful for forcing unequal load sharing between different interfaces, for increasing the number of IP addresses in a LAN when no more IPs are available from the subnet, and for resolving issues with discontinuous subnets and classful routing protocol.

Configure VPN interface SVI

Use one of these methods to configure VPN interface SVI:

- Configuration group
- Feature template

Configure SVI interface using a configuration group

Follow these steps to configure SVI interface using a configuration group.

Configure a switch virtual interface (SVI) to create a VLAN interface.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure the SVI Interface feature.

a) Configure the SVI Interface feature.

Field	Description
Type	Choose a feature from the drop-down list.
Feature Name*	Enter a name for the feature.
Description	Enter a description of the feature. The description can contain any characters and spaces.
Associated VPN: VPN*	Choose a VPN.

b) Configure basic configuration fields.

Table 263: Basic Configuration

Field	Description
Shutdown	Enable or disable the VLAN interface.
VLAN Interface Name*	Enter a name for the VLAN interface. The name must contain a minimum of five characters. The name must be in the following format: `^Vlan(([1-9]\d|\d)/){0,2}(0|[1-9]\d*)([:|\.][1-9]\d*)?`
Interface Description	Enter a description for the interface.
Interface MTU	Enter the maximum transmission unit size for frames received and transmitted on the interface. Range: 1500 through 9216 Default: 1500 bytes
IP MTU	Enter the maximum transmission unit (MTU) size of IP packets sent on an interface. Range: 576 through 9216 Default: 1500 bytes
Configure IPV4 Address	

Field	Description
IPv4 Address Prefix*	Enter the IPv4 address for the interface.
List of DHCP helper addresses*	Enter up to eight IP addresses for DHCP servers in the network to have the interface be a DHCP helper. Separate each address with a comma. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers.
Configure IPV4 Secondary Address	
Secondary IP Address*	Enter up to four secondary IP addresses.
Configure IPV6 Address	
IPV6 address*	Enter the IPv6 address for the interface.
Configure IPV6 Secondary Address	
Address*	Enter up to four secondary IP addresses.
Configure IPV6 DHCP Helper	
Address*	Enter an IP address for DHCP servers in the network to have the interface be a DHCP helper. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers.
VPN	VPN ID for the DHCP helper address.

c) Configure ACL fields.

Table 264: ACL

Field	Description
Configure Access List V4	
Direction*	Choose a direction of the ACL: **in** or **out**.
Name of ACL*	Enter the name of the access list.
Configure Access List V6	
Direction*	Choose a direction of the ACL: **in** or **out**.
Name of ACL*	Enter the name of the access list.

d) Configure VRRP fields.

Table 265: VRRP

Field	Description
Configure VRRP	

Field	Description
Group ID*	Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups. Range: 1 through 255
Priority*	Enter the priority level of the router. The router with the highest priority is elected as the primary router. If two routers have the same priority, the one with the higher IP address is elected as the primary router. Range: 1 through 254 Default: 100
Timer*	Specify how often the primary VRRP router sends VRRP advertisement messages. If secondary routers miss three consecutive VRRP advertisements, they elect a new primary router . Range: 100 through 40950 seconds Default: 100 seconds
Track OMP	When you enable this option, VRRP tracks the Overlay Management Protocol (OMP) session running on the WAN connection. If the primary VRRP router loses all its OMP sessions, VRRP elects a new default gateway from those that have at least one active OMP session.
Prefix List*	Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the primary VRRP router loses all its OMP sessions, VRRP failover occurs as described for the **Track OMP** option. In addition, if the reachability to one of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic while the Cisco IOS XE Catalyst SD-WAN device determines the primary VRRP router.
IP Address	Enter the IP address of the virtual router. This address must be different from the configured interface IP addresses of both the local router and the peer running VRRP.
Add VRRP IP Address Secondary	
Address*	Enter an IP address for the secondary VRRP router.
TLOC Preference Change	Enable or disable this option to set whether the TLOC preference can be changed or not.
Add VRRP Tracking Object	
Tracker Id*	Enter the interface object ID or object group tracker ID.
Track Action*	Choose one of the options: • **decrement** • **shutdown**

Field	Description
Decrement Value	Enter a decrement value. Range: 1-255 From Cisco vManage Release 20.10.1, this option is enabled only when you choose **decrement** in **Track Action**.
Configure VRRP IPv6	
Group ID*	Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups. Range: 1 through 255
Priority*	Enter the priority level of the router. The router with the highest priority is elected as the primary router. If two routers have the same priority, the one with the higher IP address is elected as the primary router. Range: 1 through 254 Default: 100
Timer*	Specify how often the primary VRRP router sends VRRP advertisement messages. If secondary routers miss three consecutive VRRP advertisements, they elect a new primary router . Range: 100 through 40950 seconds Default: 100 seconds
Track OMP*	When you enable this option, VRRP tracks the Overlay Management Protocol (OMP) session running on the WAN connection. If the primary VRRP router loses all its OMP sessions, VRRP elects a new default gateway from those that have at least one active OMP session.
Track Prefix List	Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the primary VRRP router loses all its OMP sessions, VRRP failover occurs as described for the **Track OMP** option. In addition, if the reachability to one of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic while the Cisco IOS XE Catalyst SD-WAN device determines the primary VRRP router.
Add VRRP IPv6 Primary	
IPv6 Link Local*	Enter a virtual link local IPv6 address, which represents the link local address of the group. The address should be in standard link local address format. For example, FE80::AB8.
Prefix	Enter the IPv6 address of the primary VRRP router.

e) Configure ARP fields.

Table 266: ARP

Field	Description
Configure ARP	
IP Address*	Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name.
MAC Address*	Enter the MAC address in colon-separated hexadecimal notation.

f) Configure advanced fields.

Table 267: Advanced

Field	Description
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1960 bytes Default: None
ARP Timeout	Specify how long it takes for a dynamically learned ARP entry to time out. Range: 0 through 2678400 seconds (744 hours) Default: 1200 (20 minutes)
IP Directed-Broadcast	An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet. A device that is not directly connected to its destination subnet forwards an IP directed broadcast in the same way it would forward unicast IP packets destined to a host on that subnet. When a directed broadcast packet reaches a device that is directly connected to its destination subnet, that packet is broadcast on the destination subnet. The destination address in the IP header of the packet is rewritten to the configured IP broadcast address for the subnet, and the packet is sent as a link-layer broadcast. If directed broadcast is enabled for an interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which that interface is attached are broadcast on that subnet.
ICMP/ICMPv6 Redirect Disable	ICMP redirects are sent by a router to the sender of an IP packet when a packet is being routed sub-optimally. The ICMP redirect informs the sending host to forward subsequent packets to that same destination through a different gateway. By default, an interface allows ICMP redirect messages.

What to do next

Also see Deploy a configuration group.

Configure SVI interface using templates

Follow these steps to configure SVI interface using a feature template.

Use the VPN Interface SVI template to configure SVI for Cisco IOS XE Catalyst SD-WAN devices. Configure a switch virtual interface (SVI) to create a VLAN interface.

To configure DSL interfaces on Cisco routers using Cisco SD-WAN Manager templates, create a VPN Interface SVI feature template to configure VLAN interface parameters.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**.

In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

a) Click **Add Template**.
b) Choose a Cisco IOS XE Catalyst SD-WAN device from the list.
c) If you are configuring the multilink interface in the transport VPN (VPN 0), click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.

Under Additional VPN 0 Templates, located to the right of the screen, click **VPN Interface SVI**.

d) If you are configuring the multilink interface in a service VPN (VPNs other than VPN 0), click **Service VPN** or scroll to the **Service VPN** section.

In the Service **VPN** drop-down list, enter the number of the service VPN. Under Additional VPN Templates, located to the right of the screen, click **VPN Interface SVI**.

e) From the **VPN Interface SVI** drop-down list, click **Create Template**. The VPN Interface SVI template form is displayed. This form contains fields for naming the template, and fields for defining multilink Interface parameters.
f) In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
g) In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

Step 3 Configure the following parameters in the VPN Interface SVI feature template.

To get the SVI interface up and functional, ensure that the appropriate VLAN is explicitly configured on the Switch Port Access or Trunk interface.

a) Configure basic VLAN interface functionality in a VPN.

Table 268:

Parameter Name	Description
Shutdown*	Click **No** to enable the VLAN interface.

Parameter Name	Description
VLAN Interface Name*	Enter the VLAN identifier of the interface. Range: 1 through 1094.
Description	Enter a description for the interface.
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 through 1500. Default: 2000 bytes
IPv4* or IPv6	Click to configure one or more IPv4 of IPv6 addresses for the interface. (Beginning with Cisco IOS XE SD-WAN Release 17.2.)
IPv4 Address* IPv6 Address	Enter the IPv4 address for the interface.
Secondary IP Address	Click **Add** to enter up to four secondary IP addresses. (Beginning with Cisco IOS XE SD-WAN Release 17.2.)
DHCP Helper*	Enter up to eight IP addresses for DHCP servers in the network to have the interface be a DHCP helper. Separate each address with a comma. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers. Click **Add** to configure up to four DHCP helpers. (Beginning with Cisco IOS XE SD-WAN Release 17.2, for IPv6.)

b) Apply a rewrite rule, access lists, and policers to a router interface.

Table 269:

Parameter Name	Description
Ingress ACL – IPv4	Click **On** and specify the name of the access list to apply to IPv4 packets being received on the interface.
Egress ACL – IPv4	Click **On** and specify the name of the access list to apply to IPv4 packets being transmitted on the interface.
Ingress Policer	Click **On** and specify the name of the policer to apply to packets being received on the interface.
Egress Policer	Click **On** and specify the name of the policer to apply to packets being transmitted on the interface.

c) To have an interface run the Virtual Router Redundancy Protocol (VRRP), which allows multiple routers to share a common virtual IP address for default gateway redundancy, configure VRRP.

Table 270:

Parameter Name	Description
Group ID	Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups. Range: 1 through 255
Priority	Enter the priority level of the router. There router with the highest priority is elected as the primary router. If two Cisco IOS XE Catalyst SD-WAN devices have the same priority, the one with the higher IP address is elected as the primary one. Range: 1 through 254 Default: 100
Timer	Specify how often the primary VRRP router sends VRRP advertisement messages. If the subordinate routers miss three consecutive VRRP advertisements, they elect a new primary router. Range: 1 through 3600 seconds Default: 1 second
Track OMP Track Prefix List	By default, VRRP uses of the state of the service (LAN) interface on which it is running to determine which Cisco IOS XE Catalyst SD-WAN device is the primary virtual router. if a Cisco IOS XE Catalyst SD-WAN device loses all its WAN control connections, the LAN interface still indicates that it is up even though the router is functionally unable to participate in VRRP. To take WAN side connectivity into account for VRRP, configure one of the following: Track OMP—Click **On** for VRRP to track the Overlay Management Protocol (OMP) session running on the WAN connection. If the primary VRRP router loses all its OMP sessions, VRRP elects a new default gateway from those that have at least one active OMP session. Track Prefix List—Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the primary VRRP router loses all its OMP sessions, VRRP failover occurs as described for the Track OMP option. In addition, if reachability to all of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic is dropped while the Cisco IOS XE Catalyst SD-WAN device determines the primary VRRP router.
IP Address	Enter the IP address of the virtual router. This address must be different from the configured interface IP addresses of both the local Cisco IOS XE Catalyst SD-WAN device and the peer running VRRP.

d) Configure static Address Resolution Protocol (ARP) table entries on the interface.

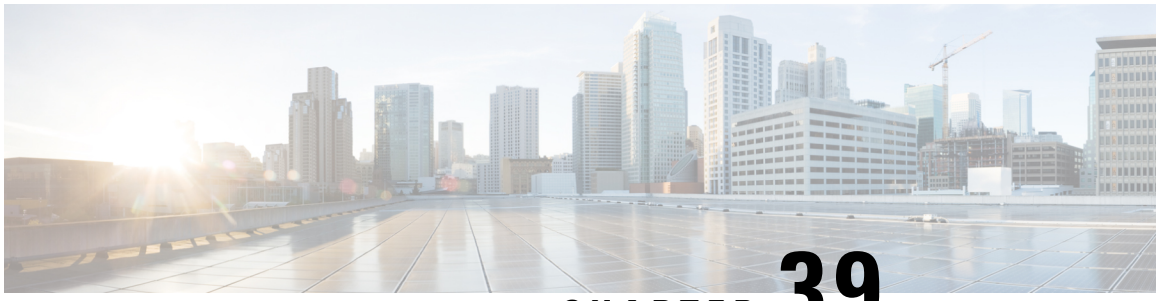
Table 271:

Parameter Name	Description
IP Address	Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name.
MAC Address	Enter the MAC address in colon-separated hexadecimal notation.

e) Configure other interface properties.

Table 272:

Parameter Name	Description
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes Default: None
ARP Timeout	Specify how long it takes for a dynamically learned ARP entry to time out. Range: 0 through 2678400 seconds (744 hours) Default: 1200 (20 minutes)



CHAPTER 39

VPN Interface T1/E1

- Configure VPN interface T1/E1, on page 679

Configure VPN interface T1/E1

Use one of these methods to configure VPN interface T1/E1:

- Configuration group
- Feature template

Configure VPN interface T1/E1 using a configuration group

Follow these steps to configure VPN interface T1/E1 using a configuration group.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure the Transport VPN feature in a Transport and Management Profile.

Step 3 Create and configure the T1 and E1 feature for the VPN interface.

a) Configure the basic VPN settings.

Table 273: Basic Configuration

Parameter Name	Description
Shutdown	Click **No** to enable the interface.

Parameter Name	Description
Interface name*	Enter a name for the interface. The name should be in the following format: **serial** *slot* / *subslot* / *port* **:** *channel-group* You must also configure a number for the channel group in the T1/E1 Controller feature configuration template.
Description	Enter a description for the interface.
More Settings	
IPv4 Address*	Enter an IPv4 address.
IPv6 Address*	Enter an IPv6 address.
Bandwidth	For transmitted traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32} / 2) – 1 kbps
Bandwidth Downstream	For received traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32} / 2) – 1 kbps
Clock Rate	Specify a value for the clock rate. Range: 1200 through 800000
Encapsulation	Choose an encapsulation method for traffic that crosses a WAN link. • **hdlc**: High-Level Data Link Control (HDLC) protocol for a serial interface. This encapsulation method provides the synchronous framing and error detection functions of HDLC without windowing or retransmission. This is the default for synchronous serial interfaces. • **ppp**: Described in RFC 1661, PPP encapsulates network layer protocol information over point-to-point links.

b) Configure the tunnel parameters.

Table 274: Tunnel

Parameter Name	Description
Tunnel Interface*	From the drop-down list, select **Global**. Click **On** to create a tunnel interface.
Per-tunnel QoS	From the drop-down list, select **Global**. Click **On** to create per-tunnel QoS. You can apply a Quality of Service (QoS) policy on individual tunnels, and is only supported for hub-to-spoke network topologies.
Color	From the drop-down list, select **Global**. Select a color for the TLOC. The color typically used for cellular interface tunnels is **lte**.
Color Description	Enter a description associated to the TLOC color.

Parameter Name	Description
Groups	From the drop-down list, select **Global**. Enter the list of groups in the field.
Border	From the drop-down list, select **Global**. Click **On** to set TLOC as border TLOC.
Maximum Control Connections	Set the maximum number of Cisco SD-WAN Controller that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8 Default: 2
Validator As Stun Server	Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT.
Exclude Control Group List	Set the identifiers of one or more Cisco SD-WAN Controller groups that this tunnel is not allows to establish control connections with. Range: 0 through 100
Manager Connection Preference	Set the preference for using the tunnel to exchange control traffic with Cisco SD-WAN Manager. Range: 0 through 9 Default: 5 If the edge device has two or more cellular interfaces, you can minimize the amount of traffic between Cisco SD-WAN Manager and the cellular interfaces by setting one of the interfaces to be the preferred one to use when sending updates to the Cisco SD-WAN Manager and receiving configurations from the Cisco SD-WAN Manager. To have a tunnel interface never connect to Cisco SD-WAN Manager, set the number to 0. At least one tunnel interface on the edge device must have a nonzero Cisco SD-WAN Manager connection preference.
Port Hop	From the drop-down list, select **Global**. Click **Off** to allow port hopping on tunnel interface. Default: **On**, which disallows port hopping on tunnel interface.
Low-Bandwidth Link	Click **On** to set the tunnel interface as a low-bandwidth link. Default: **Off**

Parameter Name	Description
Tunnel TCP MSS	TCP MSS affects any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS is examined against the MSS exchanged in the three-way handshake. The MSS in the header is lowered if the configured TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. If the TCP MSS is to be configured, it should be set at 40 bytes lower than the minimum path MTU. Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: None
Clear-Dont-Fragment	Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent. Click **On** to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, packets larger than the MTU of the interface are fragmented before being sent. **Note** **Clear-Dont-Fragment** clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected.
Network Broadcast	From the drop-down list, select **Global**. Click **On** to accept and respond to network-prefix-directed broadcasts. Enable this parameter only if the **Directed Broadcast** is enabled on the LAN interface feature template. Default: **Off**
Allow Service	Click **On** or **Off** for each service to allow or disallow the service on the cellular interface.
Encapsulation	

Parameter Name	Description
Add Encapsulation	From the drop-down list, select **Global** and choose from one of the two encapsulation methods: • **gre**: Enter a value to set GRE preference for TLOC. Range: 0 to 4294967295 • **ipsec**: Enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0
Preference	From the drop-down list, select **Global** and enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0
Weight	From the drop-down list, select **Global** and enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1
Advanced Options	
Carrier	From the drop-down list, select **Global**and select the carrier name or private network identifier to associate with the tunnel. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default. Default: default
Bind Loopback Tunnel	Enter the name of a physical interface to bind to a loopback interface. The interface name has the following format: **ge** *slot*/*port*.

Parameter Name	Description
Last-Resort Circuit	From the drop-down list, select **Global** and click **On** to use the tunnel interface as the circuit of last resort. By default, it is disabled. **Note** It is assumed that an interface configured as a circuit of last resort is unavailable and is skipped while calculating the number of control connections. As a result, the cellular modem becomes dormant, and no traffic is sent over the circuit. When the configurations are activated on the edge device with cellular interfaces, all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down. If the primary interfaces lose their connections to remote edges, the circuit of last resort activates itself, triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are a backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode, the radio interface is turned off, and no control or data connections exist over the cellular interface.
NAT Refresh Interval	Set the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds Default: 5 seconds
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 10000 milliseconds Default: 1000 milliseconds (1 second)

Parameter Name	Description
Hello Tolerance	Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down. Range: 12 through 60 seconds Default: 12 seconds The default hello interval is 1000 milliseconds, and it can be a time in the range 100 through 600000 milliseconds (10 minutes). The default hello tolerance is 12 seconds, and it can be a time in the range 12 through 600 seconds (10 minutes). To reduce outgoing control packets on a TLOC, it is recommended that on the tunnel interface you set the hello interval to 60000 milliseconds (10 minutes) and the hello tolerance to 600 seconds (10 minutes) and include the **no track-transport disable** regular checking of the DTLS connection between the edge device and the controller. For a tunnel connection between a edge device and any controller device, the tunnel uses the hello interval and tolerance times configured on the edge device. This choice is made to minimize the traffic sent over the tunnel, to allow for situations where the cost of a link is a function of the amount of traffic traversing the link. The hello interval and tolerance times are chosen separately for each tunnel between a edge device and a controller device. Another step taken to minimize the amount of control plane traffic is to not send or receive OMP control traffic over a cellular interface when other interfaces are available. This behavior is inherent in the software and is not configurable.

c) Configure ACL/QoS parameters.

Table 275: ACL/QoS

Parameter Name	Description
Shaping rate	Configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).
ACL	
Select ACL IPv4 Ingress	Enter the name of an IPv4 access list to packets being received on the interface.
Select ACL IPv4 Egress	Enter the name of an IPv4 access list to packets being transmitted on the interface.
Select ACL IPv6 Ingress	Enter the name of an IPv6 access list to packets being received on the interface.
Select ACL IPv6 Egress	Enter the name of an IPv6 access list to packets being transmitted on the interface.

d) Configure the advanced parameters.

Table 276: Advanced

Parameter Name	Description
TCP MSS	Enter the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 500 through 1460 bytes Default: 536
MTU	Enter the path MTU discovery on the interface, to allow the router to determine the largest MTU size supported without requiring packet fragmentation. Default: 1500
IP MTU	Enter the maximum MTU size of packets on the interface. Range: 576 through 9216 Default: 1500
TLOC Extension	Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration binds this service-side interface to the WAN transport, by enabling a device to access the opposite WAN transport connected to the neighbouring device using a TLOC-extension interface.

What to do next

Also see Deploy a configuration group.

Configure T1 or E1 controller using a configuration group

Follow these steps to configure T1 or E1 controller using a configuration group.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure the T1 or E1 network interface module (NIM) parameters in a Transport and Management Profile.

a) Configure a T1 Controller.

Table 277: Configure a T1 Controller

Parameter Name	Description
Slot*	Enter the number of the slot in slot/subslot/port format, where the T1 NIM is installed. For example, 0/1/0.
Description	Enter a description for the controller.
Framing	It is an optional field. Enter the T1 frame type: • **esf**: Send T1 frames as extended superframes. This is the default. • **sf**: Send T1 frames as superframes. Superframing is sometimes called D4 framing.
Line Code	It is an optional field. Select the line encoding to use to send T1 frames: • **ami**: Use alternate mark inversion (AMI) as the linecode. AMI signaling uses frames grouped into superframes. • **b8zs**: Use bipolar 8-zero substitution as the linecode. This is the default. B8ZS uses frames that are grouping into extended superframes
Cable Length	Select the cable length to configure the attenuation • **short**: Set the transmission attenuation for cables that are 660 feet or shorter. • **long**: Attenuate the pulse from the transmitter using pulse equalization and line buildout. You can configure a long cable length for cables longer that 660 feet. There is no default length.
Clock Source	Select the clock source: • **line**: Use phase-locked loop (PLL) on the interface. This is the default. When both T1 ports use line clocking and neither port is configured as the primary, by default, port 0 is the primary clock source and port 1 is the secondary clock source. • **internal**: Use the controller framer as the primary clock. • **loop-timed**: • **network**:

b) Configure an E1 Controller.

Table 278: Configure an E1 Controller

Parameter Name	Description
Slot*	Enter the number of the slot in slot/subslot/port format, where the E1 NIM is installed. For example, 0/1/0.
Description	Enter a description for the controller.

Parameter Name	Description
Framing	Enter the E1 frame type: • **crc4**: Use cyclic redundancy check 4 (CRC4). This is the default. • **no-crc4**: Do not use CRC4.
Line Code	Choose the line encoding to use to send E1 frames: • **ami**: Use alternate mark inversion (AMI) as the linecode. • **hdb3**: Use high-density bipolar 3 as the linecode. This is the default.
Clock Source	Choose the clock source: • **internal**: Use the controller framer as the primary clock. • **line**: Use phase-locked loop (PLL) on the interface. This is the default.

c) Configure channel group.

Table 279: Channel Group

Parameter Name	Description
Add Channel Group	To configure the serial WAN on the E1 interface, enter a channel group number and a value for the timeslot. • **Channel Group**: Enter a value for the channel group. Range: 0 through 30 • **Time Slot**: Type a value for the timeslot. Range: 0 through 31

What to do next

Also see Deploy a configuration group.

Configure VPN interface T1/E1 using templates

Follow these steps to configure VPN interface T1/E1 using a feature template.

Use the VPN Interface T1/E1 template for Cisco Catalyst SD-WANs running the Cisco Catalyst SD-WAN software.

To configure the T1/E1 interfaces in a VPN using Cisco SD-WAN Manager templates:

1. Create a VPN Interface T1/E1 feature template to configure T1/E1 interface parameters, as described in this article.

2. Create a T1/E1 Controller template to configure the T1 or E1 network interface module (NIM) parameters.
3. Create a VPN feature template to configure VPN parameters.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**.

In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

a) Click **Add Template**.
b) Choose a Cisco IOS XE Catalyst SD-WAN device from the list.
c) If you are configuring the multilink interface in the transport VPN (VPN 0), click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.

Under Additional VPN 0 Templates, located to the right of the screen, click **VPN Interface T1/E1 Serial**.

d) If you are configuring the multilink interface in a service VPN (VPNs other than VPN 0), click **Service VPN** or scroll to the **Service VPN** section.

In the Service **VPN** drop-down list, enter the number of the service VPN. Under Additional VPN Templates, located to the right of the screen, click **VPN Interface T1/E1 Serial**.

e) From the **VPN Interface T1/E1 Serial** drop-down list, click **Create Template**. The VPN Interface SVI template form is displayed. This form contains fields for naming the template, and fields for defining multilink Interface parameters.
f) In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
g) In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

Step 3 Configure the following parameters in the VPN Interface T1/E1 Serial template.

a) Configure basic interface functionality in a VPN.

Table 280:

Parameter Name	Description
Shutdown*	Click **No** to enable the interface.
Interface name*	Enter a name for the interface. The name should be in the format **serial** *slot* / *subslot* / *port* : *channel-group*. You must also configure a number for the channel group in the T1/E1 Controller feature configuration template.
Description	Enter a description for the interface.
IPv4 Address*	Enter an IPv4 address.
IPv6 Address*	Enter an IPv6 address.

Parameter Name	Description
Bandwidth Upstream	For transmitted traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32} / 2) – 1 kbps
Bandwidth Downstream	For received traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32} / 2) – 1 kbps
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 through 1804 Default: 1500 bytes

b) Configure a tunnel interface for the multilink interface.

Table 281:

Parameter Name	Description
Tunnel Interface	Click **On** to create a tunnel interface.
Color	Select a color for the TLOC.
Color Description	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enter a description associated to the TLOC color.

Parameter Name	Description
Control Connection	By default, Control Conection is set to **On**, which establishes a control connection for the TLOC. If the router has multiple TLOCs, click **No** to have the tunnel not establish control connection for the TLOC. **Note** We recommend a minimum of 650-700 Kbps bandwidth with default 1 sec hello-interval and 12 sec hello-tolerance parameters configured to avoid any data/packet loss in connection traffic. For each BFD session, an additional average sized BFD packet of 175 Bytes consumes 1.4 Kbps of bandwidth. A sample calculation of the required bandwidth for bidirectional BFD packet flow is given below: • 650 – 700 Kbps per device for control connections. • 175 Bytes (or 1.4 Kbps) per BFD session on the device (request) • 175 Bytes (or 1.4 Kbps) per BFD session on the device (response) If the path MTU discovery (PMTUD) is enabled, bandwidth for send/receive BFD packets per tunnel for every 30 secs: A 1500 Bytes BFD request packet is sent per tunnel every 30 secs: 1500 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 400 bps (request) A 147 Bytes BFD packet is sent in response: 147 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 40 bps (response) Therefore, a device with 775 BFD sessions (for example) requires a bandwidth of: 700k + (1.4k*775) + (400 *775) + (1.4k*775) + (40 *775) = ~3,5 MBps
Maximum Control Connections	Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8 Default: 2
Cisco SD-WAN Validator As STUN Server	Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT.
Exclude Controller Group List	Set the Cisco SD-WAN Controllers that the tunnel interface is not allowed to connect to. Range: 0 through 100
Cisco SD-WAN Manager Connection Preference	Set the preference for using a tunnel interface to exchange control traffic with the Cisco SD-WAN Manager NMS. Range: 0 through 8 Default: 5

Parameter Name	Description
Full Port Hop	Minimum release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled
Port Hop	Click **On** to enable port hopping, or click **Off** to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. Default: Enabled Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, this field is deprecated. Instead use the **Full Port Hop** option. See the **Full Port Hop** field.
Low-Bandwidth Link	Select to characterize the tunnel interface as a low-bandwidth link.
Tunnel TCP MSS	TCP MSS affects any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS is examined against the MSS exchanged in the three-way handshake. The MSS in the header is lowered if the configured TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. If the TCP MSS is to be configured, it should be set at 40 bytes lower than the minimum path MTU. Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes Default: None
Clear-Dont-Fragment	Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has **Dont Fragment** configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent. Click **On** to clear the **Dont Fragment** bit in the IPv4 packet header for packets being transmitted out of the interface. When the **Dont Fragment** bit is cleared, packets larger than the MTU of the interface are fragmented before being sent. **Note** **Clear-Dont-Fragment** clears the **Dont Fragment** bit and the **Dont Fragment** bit is set. For packets not requiring fragmentation, the **Dont Fragment** bit is not affected.
Allow Service	Select **On** or **Off** for each service to allow or disallow the service on the interface.

Configure T1 or E1 controller using templates

Follow these steps to configure T1 or E1 controller using a feature template.

Use the T1/E1 Controller template for Cisco IOS XE Catalyst SD-WAN devices running the Cisco Catalyst SD-WAN software.

To configure the T1/E1 interfaces in a VPN using Cisco SD-WAN Manager templates:

1. Create a T1/E1 Controller template to configure the T1 or E1 network interface module (NIM) parameters, as described in this article.
2. Create a VPN Interface T1/E1 feature template to configure T1/E1 interface parameters.
3. Create a VPN feature template to configure VPN parameters.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**.

In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

a) Click **Add Template**.
b) Choose a Cisco IOS XE Catalyst SD-WAN device from the list.
c) If you are configuring the multilink interface in the transport VPN (VPN 0), click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.

Under Additional VPN 0 Templates, located to the right of the screen, click **VPN Interface T1/E1**.

d) From the **VPN Interface T1/E1 Serial** drop-down list, click **Create Template**. The VPN Interface SVI template form is displayed. This form contains fields for naming the template, and fields for defining multilink Interface parameters.
e) In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
f) In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

Step 3 Configure the following T1 or E1 controller parameters.

a) Configure a T1 controller.

Table 282:

Parameter Name	Description
Slot*	Enter the number of the slot in slot/subslot/port format, where the T1 NIM is installed. For example, 0/1/0.
Framing*	Enter the T1 frame type: • **esf**—Send T1 frames as extended superframes. This is the default. • **sf**—Send T1 frames as superframes. Superframing is sometimes called D4 framing.

Parameter Name	Description
Line Code	Select the line encoding to use to send T1 frames: • ami—Use alternate mark inversion (AMI) as the linecode. AMI signaling uses frames grouped into superframes. • b8zs—Use bipolar 8-zero substitution as the linecode. This is the default. B8ZS uses frames that are grouping into extended superframes
Clock Source	Select the clock source: • internal—Use the controller framer as the primary clock. • line—Use phase-locked loop (PLL) on the interface. This is the default. When both T1 ports use line clocking and neither port is configured as the primary, by default, port 0 is the primary clock source and port 1 is the secondary clock source.
Line Mode	If you choose the Line clock source, select whether the line is a primary or a secondary line.
Description	Enter a description for the controller.
Channel Group	Enter the number of the channel group. If you do so, you must enter a time slot in the Time Slot field. Range: 0 through 30
Time Slot	Enter the time slot or time slots that are part of the channel group. Range: 1 through 24
Cable Length	Select the cable length to configure the attenuation • long—Attenuate the pulse from the transmitter using pulse equalization and line buildout. You can configure a long cable length for cables longer that 660 feet. • short—Set the transmission attenuation for cables that are 660 feet or shorter. There is no default length.

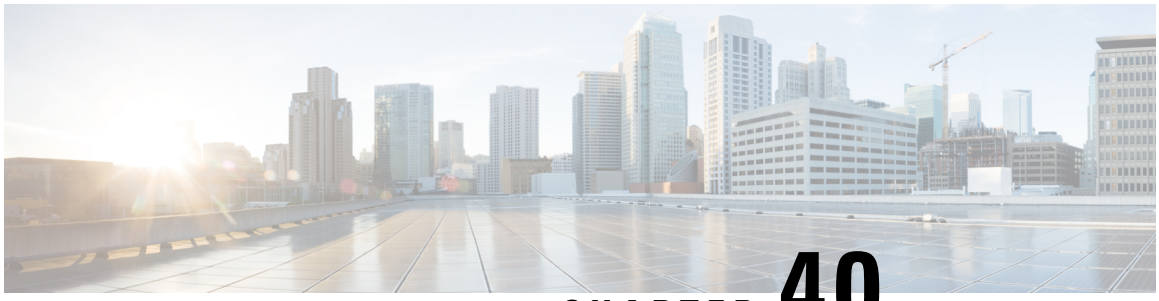
Parameter Name	Description
Length	If you specify a value in the **Cable Length Field**, enter the length of the cable. For short cables, the length values can be: • 110—Length from 0 through 110 feet • 220—Length from 111 through 220 feet • 330—Length from 221 through 330 feet • 440—Length from 331 through 440 feet • 550—Length from 441 through 550 feet • 660—Length from 551 through 660 feet For long cables, the length values can be: • 0 dB • –7.5 dB • –15 dB • –22.5 dB

b) Configure an E1 controller.

Table 283:

Parameter Name	Description
Slot*	Enter the number of the slot in slot/subslot/port format, where the E1 NIM is installed. For example, 0/1/0.
Framing*	Enter the E1 frame type: • **crc4**—Use cyclic redundancy check 4 (CRC4). This is the default. • **no-crc4**—Do no use CRC4.
Line Code*	Select the line encoding to use to send E1 frames: • ami—Use alternate mark inversion (AMI) as the linecode. • hdb3—Use high-density bipolar 3 as the linecode. This is the default.
Clock Source	Select the clock source: • internal—Use the controller framer as the primary clock. • line—Use phase-locked loop (PLL) on the interface. This is the default.

Parameter Name	Description
Line Mode	If you choose the Line clock source, select whether the line is a primary or secondary line. If you configure both a primary and a secondary line, if the primary line fails, the PLL automatically switches to the secondary line. When the PLL on the primary line becomes active again, the PLL automatically switches back to the primary line.
Description	Enter a description for the controller.
Channel Group	To configure the serial WAN on the E1 interface, enter a channel group number. Range: 0 through 30
Time Slot	For a channel group, configure the timeslot. Range: 1 through 31



CHAPTER 40

IP Directed Broadcast

- IP directed broadcast, on page 697
- Configure IP directed broadcast using CLI commands, on page 697

IP directed broadcast

An IP directed broadcast is a type of IP packet that

- has a destination address that is a valid broadcast address for a specific IP subnet but originates from a node outside that subnet, and
- is forwarded by devices not directly connected to the destination subnet in the same way as unicast IP packets.

The WAN edge device rewrites the destination address in the IP header of the packet to the configured IP broadcast address for the subnet, and then sends the packet as a link-layer broadcast.

Note The access control list (ACL) option for directed broadcast is not supported in Cisco SD-WAN Manager.

Configure IP directed broadcast using CLI commands

Procedure

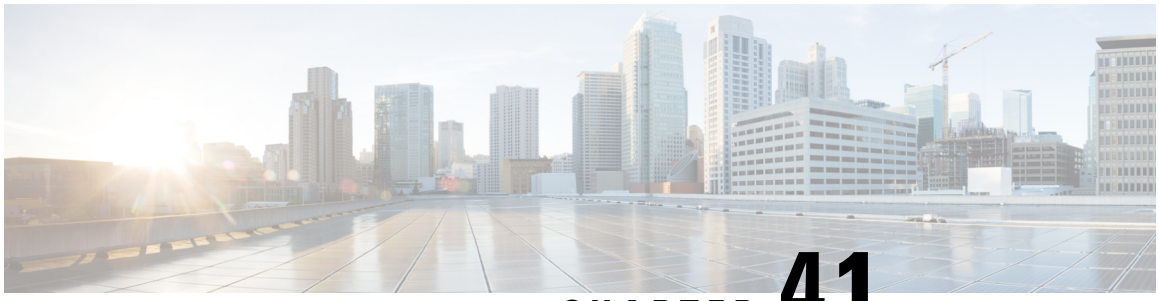
Enable the translation of a directed broadcast to physical broadcasts using the **ip directed-broadcast** command.

Note
If you enable directed broadcast on a network interface, any incoming packet that is a broadcast for that subnet is sent out to all devices on that subnet.

By default, **ip directed-broadcast** is disabled and all IP directed broadcasts are dropped.

Example:

```
device# configure-transaction
device(config)# interface ethernet 2/1
device(config-if)# ip address 10.114.114.1 255.255.255.0
device(config-if)# ip directed-broadcast
device(config-if)# end
```



CHAPTER 41

Layer 2 VPN

- Feature history for L2VPN, on page 699
- Layer 2 VPNs within the SD-WAN overlay network , on page 700
- Supported platforms for Layer 2 VPN, on page 703
- Restrictions for Layer 2 VPN, on page 703
- Methods to configure Layer 2 VPN using CLI template, on page 704
- Configure a Layer 2 VPN on a Cisco IOS XE Catalyst SD-WAN device using CLI template, on page 704
- Configure a point-to-point Layer 2 VPN using CLI template, on page 705
- Configure a point-to-multipoint Layer 2 VPN using CLI template, on page 708
- Configure a Layer 2 VPN Switchport using CLI template, on page 712
- Methods to verify Layer 2 VPN using CLI, on page 714
- Monitor configured layer 2 VPN using CLI, on page 718

Feature history for L2VPN

This table describes the developments of this feature, by release.

Table 284: Feature History

Feature Name	Release Information	Description
Layer 2 (L2) VPN	Cisco Catalyst SD-WAN Manager Release 20.14.1 Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	The feature adds Layer 2 VPN support on the Cisco Catalyst SD-WAN overlay network. It allows you to configure Layer 2 point-to-point and point-to-multipoint connections within the Cisco Catalyst SD-WAN fabric.
Layer 2 (L2) VPN Multihoming and Hub-and-Spoke Support	Cisco Catalyst SD-WAN Manager Release 20.15.1 Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	With this feature, you can configure Layer 2 VPN on multiple devices on the same site in an active-standby configuration. This feature also enables Layer 2 connections using an indirect path, such as a hub, for point-to-multipoint connections within the Cisco Catalyst SD-WAN fabric.

Layer 2 VPNs within the SD-WAN overlay network

Layer 2 VPN within the Cisco Catalyst SD-WAN overlay network is a network feature that

- enables Layer 2 connectivity across the SD-WAN fabric for legacy systems and non-IP applications,
- supports point-to-point (P2P) and point-to-multipoint (P2MP) L2VPN services with options for single homing, multihoming, and topologies including full mesh and hub-and-spoke, and
- provides MAC learning through OMP protocol (Control Plane), along with features such as ingress replication for broadcast, unknown-unicast, and multicast (BUM) traffic.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, the following L2VPN features are supported:

- Point-to-point L2VPN Service (P2P)
- Point-to-Multipoint L2VPN Service (P2MP)
- Single homing
- Flood and Learn in WAN and LAN
- Ingress replication for Broadcast, Unknown-unicast and Multicast (BUM)
- Full mesh topology only

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, the following L2VPN features are supported:

- Multihoming for P2P and P2MP
- Hub-and-spoke topology support for L2VPN services
- The MAC learning mode (previously the Flood and Learn in WAN and LAN) is changed to learning through OMP protocol (that is, Control Plane).



Note From Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, you can adjust the TCP Maximum Segment Size (MSS) even for a TCP packet encapsulated in an MPLS label. You can set the TCP MSS per the Path Maximum Transmission Unit (PMTU) with 30 bytes to account for Layer 2 headers, such as Ethernet, VLAN tags and MPLS headers.

For IPv4, the TCP MSS is set per PMTU with 80 bytes for IPv4 and TCP headers and an additional 30 bytes for Layer 2 headers. For example, if the PMTU is 1438, the TCP MSS is set as 1328 (1438 - 80 - 30).

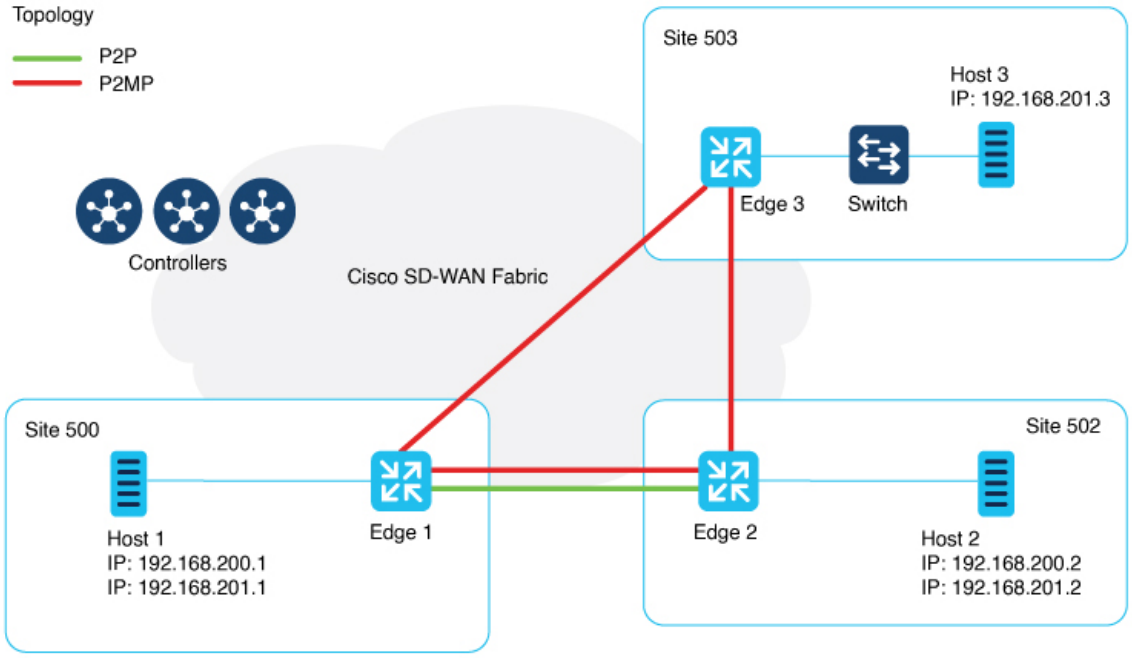
For IPv6, the TCP MSS is set per PMTU with 100 bytes for IPv6 and TCP headers and an additional 30 bytes for Layer 2 headers. For example, if the PMTU is 1438, the TCP MSS is set as 1308 (1438-100-30).

For more information about configuring TCP MSS, see Configure TCP MSS Using CLI

This change helps prevent drop in TCP sessions, improving overall network performance and reliability.

Network Topology for Layer 2 Connections

Figure 2: Topology

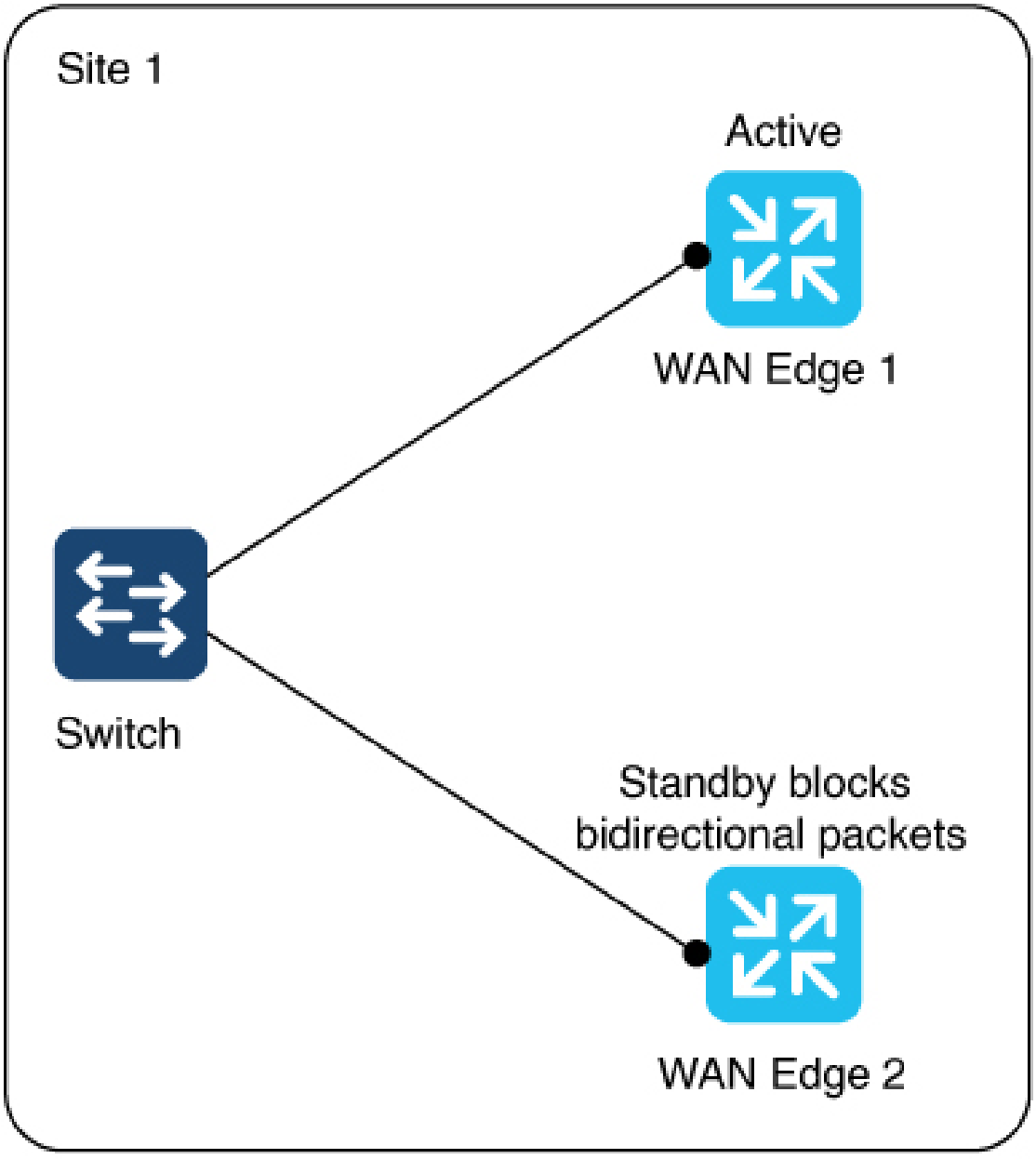


This illustration shows three sites and shows P2P (green line) and P2MP (red lines) connections between edge routers at the sites.

- Point-to-Point (P2P): Connects sites 500 and 502 with a dedicated Layer 2 VPN. The L2VPN connection between the two sites allows Host 1 and Host 2 to interact.
- Point-to-Multipoint (P2MP): Connects sites 500, 502, and 503 with Layer 2 VPN. Host 1 communicates with both Host 2 and Host 3 across a Layer 2 multipoint network.

The L2VPN connections use existing Cisco Catalyst SD-WAN tunnels.

Figure 3: Multihoming



The illustration shows two edge routers on the same site connected to a switch. For an (instance-id + vc), one router is active and the other is on standby. (instance-id +vc) maps to a bridge domain and a bridge-domain maps to a VLAN (or a VLAN range).

The router on standby blocks bidirectional traffic for that VLAN.

Multihoming supports L2VPN configuration on up to two edge devices on the same site, thereby providing redundancy for L2VPN service over SD-WAN.

Multihoming allows an active-standby scenario where one device is chosen as active and the other as standby. This provides automated failover. It determines which of the two edge devices should be active and which one should be on standby. When the OMP timer expires on the controller, it marks the L2VPN status route as stale, and notifies other edges.

Role determination for an Active and Standby device

The active and standby role between edge devices is automatically determined by with this algorithm: (SDWAN-Instance-ID + VC-ID) modular 2.

If the modular result is 0, the edge with lower system-ip is selected as the active device. The edge with the higher system-ip is selected as the standby device.

If the modular result is 1, the edge with higher system-ip is selected as the active device. The edge with the lower system-ip is selected as the standby device.

Example:

There are two WAN edge devices. WAN edge 1 has a system-ip of 172.16.255.10. WAN edge 2 has a system-ip of 172.16.255.11.

For sdwan-instance-id 100, vc-id 2, WAN edge 1 with the lower system-ip is selected as the active device. WAN edge 2 is the standby device.

For sdwan-instance-id 100, vc-id 1, WAN edge 2 with the higher system-ip is selected as the active device. WAN edge 1 is the standby device.

If a failure occurs on the service side of one of the edge devices, the controller is notified about a change to the L2VPN status route, and other edge routers can switchover traffic to the new active device.

Supported platforms for Layer 2 VPN

All Cisco IOS XE Catalyst SD-WAN devices.

Restrictions for Layer 2 VPN

Supported configuration CLI templates for Layer 2 VPN

Only CLI template or CLI add-on template configuration is supported for Layer 2 VPN.

LAN side interface limitation in single homing and multihoming

For both single homing and multihoming, only one LAN side interface is supported in a bridge-domain.

Point-to-Multipoint (P2MP) requirements for hub and spoke connectivity

P2P configuration between two spokes is not supported. In such cases, use P2MP instead of P2P.

Note P2P configuration between hub and spoke is supported.

Multihoming support only for dual homing

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, multihoming only supports dual homing.

Layer 2 VPN limitations for hub-and-spoke topology

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, hub-and-spoke topology is supported for Layer 2 VPN. It is limited by:

- No support for point-to-point Layer 2 VPN service between spokes.
- Support for up to 6000 spokes and 6000 sites within the same Layer 2 VPN in hub-and-spoke topology, and
- Support for only 256 sites within the same Layer 2 VPN in a non-hub-and-spoke design.

Methods to configure Layer 2 VPN using CLI template

Using these procedures, configure a Layer 2 VPN on a Cisco Catalyst SD-WAN overlay network.

- Configure a Layer 2 VPN on a Cisco IOS XE Catalyst SD-WAN device using CLI template, on page 704
- Configure a point-to-point Layer 2 VPN using CLI template, on page 705
- Configure a point-to-multipoint Layer 2 VPN using CLI template, on page 708
- Configure a Layer 2 VPN Switchport using CLI template, on page 712

Configure a Layer 2 VPN on a Cisco IOS XE Catalyst SD-WAN device using CLI template

Before you begin

For information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

Follow these steps to configure an L2VPN on a Cisco IOS XE Catalyst SD-WAN Device Using CLI Template

Procedure

Step 1 Configure an L2VPN instance for P2P and P2MP connections.

```
l2vpn sdwan instance instance-id point-to-point
l2vpn sdwan instance instance-id multipoint
```

The instance ID is a unique identifier for each L2VPN connection, and must not overlap or be shared with any Layer 3 VRFs in the SD-WAN fabric. For example, you cannot use L2VPN instance 10 and vrf definition 10.

Step 2 Configure a bridge-domain.

```
bridge-domain bridge-id
```

Step 3 Configure a Layer 2 interface on a Cisco IOS XE Catalyst SD-WAN device.

```
interface vlan-id
 service instance instance-id ethernet
  encapsulation dot1q vlan-id
  no shutdown
```

Note
A rewrite is used to modify the default VLAN tag. If you have not configured rewrite under service instance, dot1q must be the same at all sites participating in the Layer 2 network. The rewrite option in a Layer 2 configuration modifies the VLAN tags of packets as they ingress or egress an interface. To use the rewrite option, you need to configure Ethernet Virtual Connections (EVCs) on edge routers (Cisco ASR 1000 Series). For more information about configuring an EVC, see Configuring Ethernet Virtual Connections on a Cisco Router.

Configure a point-to-point Layer 2 VPN using CLI template

Before you begin

- You can use one L2VPN instance ID for one or more bridge domains. It must be the same at both ends of the circuit.

  To identify a particular bridge-domain, use Virtual Circuit (VC) ID. This ID is the identifier of the virtual circuit between the Cisco IOS XE Catalyst SD-WAN devices.

- To create a P2P pseudowire, L2VPN instance ID, and VC ID must be the same on different Cisco IOS XE Catalyst SD-WAN devices.
- Remote-site-id is only supported for P2P configuration.
- For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates for Cisco IOS XE Catalyst SD-WAN Devices

Note By default, CLI templates execute commands in Global Configuration mode.

Follow these steps to configure P2P L2VPN services between two sites (Site A and Site B) on the Cisco Catalyst SD-WAN overlay network.

Procedure

Step 1 Configure an edge router at Site A for point-to-point Layer 2 VPN using CLI template, on page 706

Step 2 Configure an edge router at Site B for point-to-point Layer 2 VPN using CLI temple, on page 707

Configure an edge router at Site A for point-to-point Layer 2 VPN using CLI template

Site A uses an edge router and connects the Ethernet interface to the L2 network that bridges to Site B.

Follow these steps to configure a an Edge Router at Site A for Point-to-Point Layer 2 VPN Using CLI Template

Procedure

Step 1 Define the L2VPN instance for point-to-point service:

```
l2vpn sdwan instance instance-id point-to-point
```

Step 2 Configure the Ethernet interface:

```
interface interface-name
 service instance instance-id ethernet
  encapsulation dot1q vlan-id
```

Step 3 Define the bridge domain and associate it with the interface and L2VPN instance:

```
bridge-domain bridge-id
 member vlan-name service-instance instance-id
 member sdwan instance  instance-id  remote-site remote-site-id vc-id  virtual-circuit-id single-homing
```

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, you can specify the homing type as dual homing to enable multihoming.

```
bridge-domain bridge-id
member vlan-name service-instance instance-id
member sdwan instance instance-id remote-site remote-site-id vc-id virtual-circuit-id
dual-homing
```

Example

The following configures Site A using Cisco Catalyst 8000V Edge Software to manage traffic through GigabitEthernet5, which is linked to the Layer 2 network that provides connectivity to Site B.

```
l2vpn sdwan instance 100 point-to-point

interface GigabitEthernet5
 service instance 100 ethernet
  encapsulation dot1q 2002
  !
bridge-domain 100
 member GigabitEthernet5 service-instance 100
 member sdwan-instance 100 remote-site 502 vc-id 100 single-homing
```

Configure an edge router at Site B for point-to-point Layer 2 VPN using CLI temple

Site B uses an edge router and Switchport Ethernet interface.

Follow these steps to configure an edge router at Site B for point-to-point Layer 2 VPN.

Procedure

Step 1 Define the L2VPN instance for point-to-point service.

```
l2vpn sdwan instance instance-id point-to-point
```

Step 2 Define the VLAN for the L2VPN.

```
vlan vlan-id
 name l2vpn
```

Step 3 Configure the VLAN interface.

```
interface interface-name
 service instance instance-id ethernet
  encapsulation dot1q vlan-id
  no shutdown
```

Step 4 Configure the Ethernet interface as an access port for VLAN.

```
interface interface-name
 switchport access vlan vlan-id
```

Step 5 Define the bridge-domain for site B and associate it with the VLAN and L2VPN instance.

```
bridge-domain bridge-id
 member vlan-name service-instance instance-id
 member sdwan instance  instance-id  remote-site remote-site-id vc-id  virtual-circuit-id single-homing
```

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, specify the homing type as dual homing to enable multihoming.

```
bridge-domain bridge-id
member vlan-name service-instance instance-id
member sdwan instance instance-id remote-site remote-site-id vc-id virtual-circuit-id
dual-homing
```

Example

The following configures Switchport GigabitEthernet 0/1/7 at Site B to connect to the interface with a Cisco ISR1100-8P device.

```
l2vpn sdwan instance 100 point-to-point
vlan 2002
 name L2vpn
interface Vlan2002
 service instance 100 ethernet
  encapsulation dot1q 2002
  no shutdown
  !
interface GigabitEthernet 0/1/7
 switchport access vlan 2002
bridge-domain 100
 member Vlan2002 service-instance 100
 member sdwan-instance 100 remote-site 500 vc-id 100 single-homing
```

After configuring the point-to-point L2VPN service on both sites, you can integrate these configuration blocks into your CLI Template or CLI Add-On Feature Template. This template can then be used to deploy the configuration across the relevant devices in the Cisco Catalyst SD-WAN fabric. Verify the connectivity and functionality of the L2VPN service following the deployment to confirm that the bridge between site A and site B is operational.

Configure a point-to-multipoint Layer 2 VPN using CLI template

Before you begin

- For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

  By default, CLI templates execute commands in global config mode.

- One L2VPN instance ID can be used by one or more bridge domains. VC ID is used to identify a particular bridge-domain.

- L2VPN instance ID and VC ID must be the same on different edge devices.

Follow these steps to configure P2MP Layer 2 VPN over Cisco Catalyst SD-WAN overlay, connecting a local Layer 2 network at site A to multiple remote sites (B and C). Site A uses Gigabit Ethernet interface to connect to the Layer 2 network for bridging.

Procedure

Step 1 Configure an edge router at sites A, B and C, on page 708

Step 2 Configure an edge router at Site B for point-to-point Layer 2 VPN using CLI temple, on page 707

Step 3 Configure an edge router at Site C for point-to-point Layer 2 VPN using CLI template, on page 711

Configure an edge router at sites A, B and C

Site A is using an edge router, where an Ethernet interface is connected to the Layer 2 network that bridges to Site B and Site C.

Follow these steps to configure an Edge Router at Sites A, B, and C.

Procedure

Step 1 Define the L2VPN instance for the multipoint service on the data center router:

```
l2vpn sdwan instance instance-id multipoint
```

Step 2 Configure the Ethernet interface on the data center router:

```
interface interface-name
service instance instance-id ethernet
encapsulation dot1q vlan-id
```

Step 3 Define the bridge-domain on the data center route and associate it with the interface and L2VPN instance:

```
bridge-domain bridge-id
member vlan-name service-instance instance-id
member sdwan instance instance-id remote-site remote-site-id vc-id virtual-circuit-id
single-homing
```

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, specify the homing type as dual homing to enable multihoming.

```
bridge-domain bridge-id
member vlan-name service-instance instance-id
member sdwan instance instance-id remote-site remote-site-id vc-id virtual-circuit-id
dual-homing
```

What to do next

See the topic, Configure an edge router at Site B for point-to-point Layer 2 VPN using CLI Temple.

Configure an edge router at Site B for point-to-point Layer 2 VPN using CLI temple

Site B uses an edge router and Switchport Ethernet interface.

Follow these steps to configure an edge router at Site B for point-to-point Layer 2 VPN.

Procedure

Step 1 Define the L2VPN instance for point-to-point service.

```
l2vpn sdwan instance instance-id point-to-point
```

Step 2 Define the VLAN for the L2VPN.

```
vlan vlan-id
 name l2vpn
```

Step 3 Configure the VLAN interface.

```
interface interface-name
 service instance instance-id ethernet
  encapsulation dot1q vlan-id
  no shutdown
```

Step 4 Configure the Ethernet interface as an access port for VLAN.

```
interface interface-name
 switchport access vlan vlan-id
```

Step 5 Define the bridge-domain for site B and associate it with the VLAN and L2VPN instance.

```
bridge-domain bridge-id
 member vlan-name service-instance instance-id
 member sdwan instance  instance-id  remote-site remote-site-id vc-id  virtual-circuit-id single-homing
```

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, specify the homing type as dual homing to enable multihoming.

```
bridge-domain bridge-id
member vlan-name service-instance instance-id
member sdwan instance instance-id remote-site remote-site-id vc-id virtual-circuit-id
dual-homing
```

Example

The following configures Switchport GigabitEthernet 0/1/7 at Site B to connect to the interface with a Cisco ISR1100-8P device.

```
l2vpn sdwan instance 100 point-to-point
vlan 2002
 name L2vpn
interface Vlan2002
 service instance 100 ethernet
  encapsulation dot1q 2002
  no shutdown
  !
interface GigabitEthernet 0/1/7
 switchport access vlan 2002
bridge-domain 100
 member Vlan2002 service-instance 100
 member sdwan-instance 100 remote-site 500 vc-id 100 single-homing
```

After configuring the point-to-point L2VPN service on both sites, you can integrate these configuration blocks into your CLI Template or CLI Add-On Feature Template. This template can then be used to deploy the configuration across the relevant devices in the Cisco Catalyst SD-WAN fabric. Verify the connectivity and functionality of the L2VPN service following the deployment to confirm that the bridge between site A and site B is operational.

Configure an edge router at Site C for point-to-point Layer 2 VPN using CLI template

Before you begin

Repeat the same steps as for branch router C, substituting the specific interface used on site B.

Follow these steps to configure an edge router at Site C for point-to-point Layer 2 VPN.

Procedure

Step 1 Define the L2VPN instance for multipoint service on the branch router:

```
l2vpn sdwan instance instance-id multipoint
```

Step 2 Define the VLAN for the L2VPN on the branch router:

```
vlan vlan-id
name L2vpn
```

Step 3 Configure the VLAN interface on the branch router:

```
interface interface-name
service instance instance-id ethernet
encapsulation dot1q vlan-id
no shutdown
```

Step 4 Configure the Ethernet interface on the branch router as an access port for VLAN:

```
interface interface-name
switchport access vlan vlan-id
```

Step 5 Define the bridge-domain on the branch router and associate it with the VLAN and L2VPN instance:

```
bridge-domain bridge-id
member vlan-name service-instance instance-id
member sdwan instance instance-id  vc-id virtual-circuit-id single-homing
```

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, specify the homing type as dual homing to enable multihoming.

```
bridge-domain bridge-id
member vlan-name service-instance instance-id
member sdwan instance instance-id remote-site remote-site-id vc-id virtual-circuit-id
dual-homing
```

Example

This section provides an example configuration for P2MP L2VPN service within the Cisco Catalyst SD-WAN overlay network, connecting a local Layer 2 network at site A to multiple remote sites (B and C). Site A uses GigabitEthernet6 interface to connect to the L2 network for bridging.

Verify the connectivity and functionality of the P2MP L2VPN service and ensure that all sites are correctly bridged.

Site A is using a Cisco Catalyst 8000V edge router, where GigabitEthernet6 is connected to the Layer 2 network that bridges to site B and site C.

```
l2vpn sdwan instance 200 multipoint

vlan 2001
 name L2MPvpn

interface Vlan2001
 service instance 200 ethernet
  encapsulation dot1q 2001
  no shutdown
  !
interface GigabitEthernet 0/1/6
 switchport access vlan 2001

bridge-domain 200
 member Vlan2001 service-instance 200
 member sdwan-instance 200 vc-id 200 single-homing
```

Configure branch router C:

Repeat the same steps as for branch router B, substituting the specific interface used on router 503. In this example, we have used the GigabitEthernet 0/1/6 interface.

```
l2vpn sdwan instance 200 multipoint

vlan 2001
 name L2MPvpn

interface Vlan2001
 service instance 200 ethernet
  encapsulation dot1q 2001
  no shutdown
  !
bridge-domain 200
 member Vlan2001 service-instance 200
 member sdwan-instance 200 vc-id 200 single-homing
```

Configure a Layer 2 VPN Switchport using CLI template

If your device such as Cisco ISR1121-8P or similar has embedded switchports and you want to use one of them for the L2VPN services, configure a VLAN interface first and then assign that VLAN to your switchport as described in this section.

To support a Layer 2 switchport, configure a service instance in the VLAN interface. In the VLAN interface, a packet always has the dot1q tag even when the Layer 2 switchport is configured with switchport mode access. Therefore, the dot1q tag is mandatory in the service instance of the VLAN interface.

This following section provides steps to configure a Layer 2 switchport for P2MP (applicable for devices with embedded switchports). You can also configure a Layer 2 switchport for P2P by updating the Layer 2 VPN instance command.

Site A is using an edge router, where the Ethernet interface is connected to the Layer 2 network that bridges to Site B and Site C.

Follow these steps to configure a Layer 2 VPN Switchport using CLI template.

Procedure

Step 1 Define the Layer 2 VPN instance for multipoint service on the branch routers:

```
l2vpn sdwan instance instance-id multipoint
```

Step 2 Define the VLAN for the Layer 2 VPN on the branch routers:

```
vlan vlan-id
name l2vpn
```

Step 3 Configure the Ethernet interface on the routers:

```
interface interface-name
```

Step 4 Set the switch port access VLAN and switchport mode to access to accept traffic only from the specified VLAN:

```
switchport access Vlan vlan-id
```

Step 5 Configure the VLAN interface on a router and disable the IP address assignment

```
interface interface-name
no ip address
service instance instance-id ethernet
encapsulation dot1q vlan-id
```

Step 6 Define the bridge-domain on the data center router and associate it with the interface and L2VPN instance:

```
bridge domain bridge-id
member vlan-name service-instance instance-id
member sdwan instance instance-id vc-id virtual-circuit-id single homing
```

The following configures a Layer 2 VPN Switchport to integrate a multipoint SD-WAN instance and bridge-domain. This configuration sets up GigabitEthernet0/1/2 as an access port for VLAN 201.

```
l2vpn sdwan instance 200 multipoint

interface GigabitEthernet0/1/2
 switchport access Vlan 201
 switchport mode access

interface Vlan201
 no ip address
 service instance 200 ethernet
  encapsulation dot1q 201
  !

bridge-domain 201
 member Vlan201 service-instance 200
 member sdwan-instance 200 vc-id 201 single-homing
```

Methods to verify Layer 2 VPN using CLI

To verify Layer 2 VPN using CLI, use these methods.

1. View a Layer 2 VPN status, on page 714
2. View L2VPN information learned through OMP route on a Cisco SD-WAN Controller, on page 714
3. View Bridge-domain information, on page 715
4. View Cisco Catalyst SD-WAN Flood List Information and Packet Counters in Data Plane, on page 716
5. View packet counters in data plane, on page 716

View a Layer 2 VPN status

To view the remote peer information, system IP, status, and related information, use the **show l2vpn sdwan [instance** *instance-id]***[vc-id** *vc-id]* command.

This is an example for a Cisco IOS XE Catalyst SD-WAN device.

```
Device# show l2vpn sdwan instance 13 vc-id 13
VC_ID: 13 Bridge-domain: 13
Local l2vpn status: UP
Local Pseudoports: GigabitEthernet7 service instance 13
```

View L2VPN information learned through OMP route on a Cisco SD-WAN Controller

To view the specific L2-route or path learned in the specific VPN and virtual circuit, use the **show sdwan omp l2-routes**[**vpn** *vpn-id*] [**vc-id** *vc-id*] command. If the **vpn** and **vc-id** are not included, the command shows Layer 2 routes learned through OMP from all VPNs across the Cisco Catalyst SD-WAN fabric.

This is a sample output from the **show omp l2-routes** command displaying Layer 2 routes learned through OMP for Cisco SD-WAN Controllers.

```
Device# show omp l2-routes | tab
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
IA  -> On-demand inactive
U   -> TLOC unresolved


                                        REMOTE
                                ROUTE                   IP                      SITE
```

```
                PATH                        SITE
VPN     VC ID         ORIGINATOR       TYPE   MAC ADDRESS      ADDRESS  VPN TYPE    ID
FROM PEER         ID     LABEL    STATUS    ID
-------------------------------------------------------------------------------------
12      12            172.16.255.15    vpn    0000.0000.0000   ::       p2p         500
172.16.255.15    66     1004     C,R       501

172.16.255.15    69     1004     C,R       501

172.16.255.20    1      1004     C,R       501

172.16.255.20    2      1004     C,R       501
12      12            172.16.255.27    vpn    0000.0000.0000   ::       p2p         501
172.16.255.20    1      1014     C,R       500

172.16.255.27    70     1014     C,R       500
13      13            172.16.255.15    vpn    0000.0000.0000   ::       multipoint  500
172.16.255.15    66     1006     C,R       -

172.16.255.15    69     1006     C,R       -

172.16.255.20    1      1006     C,R       -

172.16.255.20    2      1006     C,R       -
13      13            172.16.255.27    vpn    0000.0000.0000   ::       multipoint  501
172.16.255.20    1      1016     C,R       -

172.16.255.27    70     1016     C,R       -
13      13            172.16.255.32    vpn    0000.0000.0000   ::       multipoint  503
172.16.255.20    1      1007     C,R       -

172.16.255.32    71     1007     C,R       -
14      1             172.16.255.27    vpn    0000.0000.0000   ::       multipoint  501
172.16.255.20    1      1018     C,R       -

172.16.255.27    70     1018     C,R       -
15      1             172.16.255.15    vpn    0000.0000.0000   ::       p2p         500
172.16.255.15    66     1020     C,R       501

172.16.255.15    69     1020     C,R       501

172.16.255.20    1      1020     C,R       501

172.16.255.20    2      1020     C,R       501
15      1             172.16.255.27    vpn    0000.0000.0000   ::       p2p         501
172.16.255.20    1      1020     C,R       500

172.16.255.27    70     1020     C,R       500
```

View Bridge-domain information

To verify information related to bridge domains within the context of Forwarding Table Management Daemon (FTMD), use the **show platform software sdwan ftmd bridge-domain** command on a device.

This is a sample output from the **show platform software sdwan ftmd bridge-domain** command that displays information related to bridge domains within the context of Forwarding Table Management Daemon (FTMD).

```
Device# show platform software sdwan ftmd bridge-domain
L2vpn Bridge-domain 12 Table:
```

```
  sdwan efp dpidx: 4210708(0x404014)
  Label: 1004 lbl-nhop-id: 196611 (binosId=0xf830003f)
  Bum Label: 1005 bum-lbl-nhop-id: 196612 (binosId=0xf830004f)
  Remote Site Table(1 entries in total):
    remote-site-id: 501 sla-nhop-id: 29 (binosId=0xf80001df)

L2vpn Bridge-domain 13 Table:
  sdwan efp dpidx: 4210709(0x404015)
  Label: 1006 lbl-nhop-id: 196613 (binosId=0xf830005f)
  Bum Label: 1007 bum-lbl-nhop-id: 196614 (binosId=0xf830006f)
  Remote Site Table(2 entries in total):
    remote-site-id: 501 sla-nhop-id: 30 (binosId=0xf80001ef)
remote-site-id: 503 sla-nhop-id: 33 (binosId=0xf800021f)
```

View Cisco Catalyst SD-WAN Flood List Information and Packet Counters in Data Plane

To verify information related to Cisco Catalyst SD-WAN flood list information, use the **show platform hardware qfp active feature bridge-domain datapath** *bridge-domain-id* **sdwan-flood-list** command.

This is a sample output from the **show platform hardware qfp active feature bridge-domain datapath** *bridge-domain-id* **sdwan-flood-list** command that displays the Cisco Catalyst SD-WAN flood list information.

```
Device#show platform software sdwan ftmd bridge-domain
L2vpn Bridge-domain 12 Table:
  sdwan efp dpidx: 4210708(0x404014)
  Label: 1004 lbl-nhop-id: 196611 (binosId=0xf830003f)
  Bum Label: 1005 bum-lbl-nhop-id: 196612 (binosId=0xf830004f)
  Remote Site Table(1 entries in total):
    remote-site-id: 501 sla-nhop-id: 29 (binosId=0xf80001df)

L2vpn Bridge-domain 13 Table:
  sdwan efp dpidx: 4210709(0x404015)
  Label: 1006 lbl-nhop-id: 196613 (binosId=0xf830005f)
  Bum Label: 1007 bum-lbl-nhop-id: 196614 (binosId=0xf830006f)
  Remote Site Table(2 entries in total):
    remote-site-id: 501 sla-nhop-id: 30 (binosId=0xf80001ef)
remote-site-id: 503 sla-nhop-id: 33 (binosId=0xf800021f)
```

View packet counters in data plane

To verify information related to a QuantumFlow Processor (QFP) hardware module packet counters for a specific bridge domain within the data path, use the **show platform hardware qfp active feature bridge-domain datapath** *bridge-id* command.

This is a sample output from the **show platform hardware qfp active feature bridge-domain datapath** *bridge-id* command to display a QFP hardware module packet counters for a specific bridge domain within the data path.

```
Device# show platform hardware qfp active feature bridge-domain datapath 200
QFP L2BD Bridge Domain information
```

```
BD id                  : 200

State enabled          : Yes

Aging timeout (sec)    : 300

Aging active entry     : Yes

Max mac limit          : 65536

Unkwn mac limit flood  : Yes

mac_learn_enabled      : Yes

mac_learn_controled    : No

Unknown unicast olist  : Yes

otv_aed_enabled : No

otv_enabled : No

mcast_snooping_enabled : No

Feature : sdwan

SISF snoop protocols   : None

Sdwan instance id      : 200

Mac learned            : 0

BDI outer vtag         : 00000000

BDI inner vtag         : 00000000


Replication tree info:

  Global replication    : depth encode 0X1000001, (head 0XE4E90000)

  Split-horizon-group 0 : depth encode 00000000, (head 00000000)

  Split-horizon-group 1 : depth encode 00000000, (head 00000000)
Bridge Domain statistics


Total bridged                pkts : 0          bytes: 0

Total unknown unicast        pkts : 0          bytes: 0

Total broadcasted            pkts : 0          bytes: 0

Total to BDI                 pkts : 0          bytes: 0

Total injected               pkts : 0          bytes: 0

Total mac-sec violation drop pkts : 0          bytes: 0

Total mac-sec move drop      pkts : 0          bytes: 0
```

```
Total mac-sec unknown drop   pkts : 0          bytes: 0

Total source filter drop     pkts : 0          bytes: 0

Total bfib policy drop       pkts : 0          bytes: 0

Total replication start drop pkts : 0          bytes: 0

Total recycle tail drop      pkts : 0          bytes: 0

Total static MAC move drop   pkts : 0          bytes: 0

Total BD disabled drop       pkts : 0          bytes: 0

Total STP state drop         pkts : 0          bytes: 0

Total UUF suppression drop   pkts : 0          bytes: 0

Total sisf ctrl punt         pkts : 0          bytes: 0

Total sisf ctrl drop         pkts : 0          bytes: 0

Total p2p lan to wan         pkts : 0          bytes: 0

Total p2p wan to lan         pkts : 0          bytes: 0
```

Monitor configured layer 2 VPN using CLI

This is a sample output from the **show l2vpn sdwan all** command. The following examples show the configuration and status information for Layer 2 VPN instances within a Cisco Catalyst SD-WAN overlay network. The output includes details for both point-to-point (P2P) and point-to-multipoint (P2MP) topologies.

Example 1: The example shows the L2VPN SD-WAN instance for instance 100 for point-to-point connectivity.

```
Device# show l2vpn sdwan all
L2VPN sdwan Instance : 100
VPN Type : point-to-point
  VC_ID: 100 Bridge-domain: 100 UP
    Local l2vpn status: UP
    Local Pseudoports: GigabitEthernet5 service instance 100
    Remote Site: 53
      System IP          status       up/down    color           encap    label  DF
      10.100.31.53       DOWN         00:15:04   public-internet ipsec    1023   N/A
```

Example 2: The example shows all the Layer 2 VPN SD-WAN instance for instance 200 for point-to-point connectivity.

```
Device# show l2vpn sdwan all
L2VPN sdwan Instance : 200
VPN Type : multipoint
IP Local-learning    : Disabled
Flooding Suppression : Disabled
  VC_ID: 200 Bridge-domain: 200 UP
    Local l2vpn status: UP
    Local Pseudoports: GigabitEthernet5 service instance 200
    Remote Site: 50
      System IP          status       up/down    color           encap    label  DF
      10.100.31.50       UP           00:04:14   public-internet ipsec    1008   N/A
```

```
    Remote Site: 53
      System IP          status       up/down    color           encap    label  DF
      10.100.31.53       UP           00:15:00   public-internet ipsec    1025   N/A
```

This is a sample output from the **show l2vpn sdwan instance** *instance-id* **vc-id** *vc-id***peers** command. The following examples show information about a specific Cisco Catalyst SD-WAN Layer 2 VPN instance (instance 200) and its associated virtual circuit (vc-id 200), including details about its peer connections.

`show l2vpn sdwan` **`instance`** *`instance-id`* **`vc-id`** *`vc-id`* **`peers`**

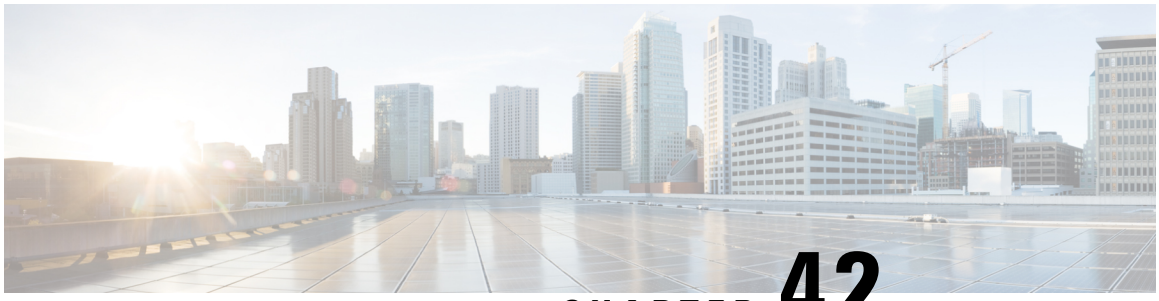
Example 1

```
Device1# show l2vpn sdwan instance 200 vc-id 200 peers
    Remote Site: 50   MACs Learn: 0
      System IP          status       up/down    color           encap    label  DF
      10.100.31.50       UP           00:19:54   public-internet ipsec    1008   N/A

    Remote Site: 53   MACs Learn: 0
      System IP          status       up/down    color           encap    label  DF
      10.100.31.53       UP           00:30:40   public-internet ipsec    1025   N/A
```

Example 2

```
Device# show l2vpn sdwan instance 200 vc-id 200 peers
     Remote Site: 1   MACs Learn: 0
      System IP          status       up/down    color           encap    label  DF
      10.100.31.1        UP           00:30:13   public-internet ipsec    1014   N/A
```



CHAPTER 42

VFR and Underlay Fragmentation

- Feature history for VFR and underlay fragmentation, on page 722
- Virtual Fragmentation Reassembly, on page 722
- Configure VFR and underlay fragmentation, on page 725
- Verify VFR and underlay fragments, on page 728

Feature history for VFR and underlay fragmentation

Table 285: Feature History

Feature Name	Release Information	Description
VFR and Underlay Fragmentation	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	In Cisco Catalyst SD-WAN networks, the VFR (Virtual Fragmentation Reassembly) actively fragments and reassembles packets. The packets undergo fragmentation to improve transportation efficiency while passing through a VFR-enabled Cisco IOS XE Catalyst SD-WAN device. The VFR reassembles the fragmented packets to match the original incoming packet. The reassembled packet contains critical Layer 4 or Layer 7 information necessary for proper reception by the destination device. Underlay fragmentation refers to the process of breaking down a large data packet into smaller fragments at the network layer. Underlay fragmentation allows the successful transmission of packets that exceed the MTU limitations by breaking them down into manageable fragments and ensuring their reliable delivery.

Virtual Fragmentation Reassembly

A Virtual Fragmentation Reassembly (VFR) is a Cisco feature that

- allows a router to collect IP fragments even if they lack necessary Layer 4 information,
- performs dynamic access control list (ACL) analysis for security, and
- enables security features such as Cisco IOS Firewall and NAT to inspect traffic.

While transmitting data across a network, due to various network constraints, the original data packets fragment into smaller fragments to facilitate seamless transmission. While the packets travel through the Cisco IOS XE Catalyst SD-WAN device, they are fragmented. VFR allows fragmented packets to be reassembled efficiently before reaching their destination.

Packet reassembly modes

In Cisco Catalyst SD-WAN network, data packets undergo reassembly in two modes:

- Default mode: Packets are virtually reassembled by default. Upon the delivery of the first fragment, each feature in the network receives the entire payload of the virtually reassembled packet. When the last fragment is received, the remaining features reassemble the packet. The original packet is fragmented, and the internal fragment information structure is shared. The fragments are then queued for refragmentation based on the fragment-offset sequence. The VFR mechanism reconstructs the packets using information from the fragment headers, such as fragment identifiers, sequence numbers, and offsets.
- Reassembly mode: Packets undergo physical reassembly, and fragment header information isn't saved. Upon receiving the last fragment, the fragments reassemble via a metapacket, and the internal fragment information structure is released.

If the packets were originally fragmented using the default mode, they undergo reassembly as if they were the original incoming packets. On the other hand, when the reassembly mode is utilized to virtually fragment the packets, they experience fragmentation based on the MTU of the egress interface before reassembly.

Some features (such as NAT, Cisco IOS XE Firewall, IPSec) automatically enable VFR to obtain Layer 4 or Layer 7 information.

When a particular interface enables VFR, it overrides the existing firewall or NAT's VFR mode configuration by default, ensuring interoperability with the firewall or NAT.

Underlay fragmentation

An underlay fragmentation is a network layer process that

- breaks down large data packets that exceed the Maximum Transmission Unit (MTU) size supported by the Cisco Catalyst SD-WAN network infrastructure,
- enables the transmission of packets that exceed MTU limitations by fragmenting them into smaller parts, and
- ensures the successful delivery of these fragments across the network.

Benefits of VFR and underlay fragmentation

- VFR enables the Cisco IOS XE Firewall to create appropriate dynamic access control lists (ACLs) to protect the network from various fragmentation attacks.
- VFR is responsible for detecting and preventing various types of fragment attacks.
- VFR drops all fragments within a fragment chain if an overlap of a fragment is detected.

Prerequisites for configuring VFR and underlay fragmentation

Properly configure the Maximum Transmission Unit (MTU) size on all network devices. The MTU defines the maximum packet size that can be transmitted without fragmentation. Ensure the MTU is set appropriately on every device along the network path to avoid unintended underlay fragmentation.

Restrictions for configuring VFR and underlay fragmentation

Fragment handling requirements

- The VFR process requires all fragments within an IP datagram to be present. If load balancing causes fragments to be sent to different devices, VFR may fail and drop fragments.
- If any fragments in a series of fragmented packets are lost or arrive out of order, the reassembly process may fail, resulting in incomplete or corrupted packets.

Feature integration

- VFR is designed to operate with features that require fragment reassembly, such as Cisco Catalyst SD-WAN NAT and IPsec. By default, NAT, Crypto-based IPSec, and NAT64 internally enable or disable VFR on an interface when these features are activated. If multiple features enable VFR on the same interface, VFR uses a reference count to track the number of enabling features. VFR is automatically disabled when the reference count reaches zero.
- The VFR CLIs are unavailable under port-channel sub-interfaces.

Underlay fragmentation

- The underlay fragmentation mechanism operates only at the network layer and is limited to the underlying network infrastructure. It does not manage fragmentation and reassembly across multiple network segments or provide end-to-end fragmentation handling.

Use cases for VFR and underlay fragmentation

Networks such as long-distance connections such as a connection between an airplane and aiport signal towers, can experience interruptions, due to the time it takes for large packets to traverse these links. When VFR is enabled, the fragments reassemble into a complete datagram, and then are fragmented within the Cisco Catalyst SD-WAN tunnel interface. With this, the first fragment is sent out first and there is no interruption in receiving the packets.

Underlay fragmentation helps in fragmenting large packets into smaller sizes, and reconstruct the packet back into the original one. This improves the overall application performance.

Boost mode

The boost mode helps in resolving one of the identified bottlenecks related to the memory management of fragments within the data plane of the network.

The boost mode is disabled by default on Cisco IOS XE Catalyst SD-WAN devices.

Before Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and later
The memory allocation to reassembly of fragments occured from a global chunk, necessitating a lock in period for the memory until the reassembly is complete. This leads to potential competition among multiple threads for the same global chunk and results in waiting for the same memory.	The boost mode enhances performance by utilizing CVLA, an alternative data plane memory infrastructure. Unlike the chunk mechanism, CVLA is lock-free and is an efficient memory management mechanism within Cisco IOS XE devices.

Configure VFR and underlay fragmentation

Use one of these methods to configure VFR and underlay fragmentation:

- Configuration groups
- CLI commands

Configure underlay fragmentation using a configuration group

Before you begin

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.15.1a

Procedure

Step 1 From the Cisco SD-WAN Manager, choose **Configuration** > **Configuration Groups**.
Step 2 Click **Transport & Management Profile**.
Step 3 Select the desired transport profile and click **Edit**.
Step 4 Click **Edit Ethernet Interface** > **Tunnel**.
Step 5 Enable **Allow Fragmentation** and **MTU To Max**.
Step 6 Click **Save**.

Configure VFR using CLI commands

Enable virtual fragment reassembly (VFR) on interfaces to prevent fragmentation attacks and ensure correct packet delivery.

You can configure VFR using a CLI template. For more information about using CLI templates, see *CLI Add-On Feature Templates* and *CLI Templates*.

Note By default, CLI templates execute commands in global config mode.

Procedure

Enable VFR.

- Enable VFR for IPv4 packets
- Enable VFR for IPv6 packets

To enable VFR for IPv4 packets on Inbound Interface Traffic perform the following steps:

a) Configure an interface type and enter interface configuration mode.

interface *interface-type interface-number*

b) Enable VFR on the interface and specify the maximum threshold values.

ip virtual-reassembly [**max-reassemblies** *number*] [**max-fragments** *number*] [**timeout** *seconds*] [**mode** *modes*][**drop-fragments**]

Example:

Here is the complete configuration example to enable VFR for IPv4 packets:

```
interface GigabitEthernet5
ip virtual-reassembly max-reassemblies 64 max-fragments 16 mode default timeout 5
```

To enable VFR for IPv4 packets on outbound interface traffic perform the following steps:

a) Configure an interface type and enter interface configuration mode.

interface *interface-type interface-number*

b) Enable VFR for outbound interface traffic on the interface and specify the maximum threshold values.

ip virtual-reassembly-out [**max-reassemblies** *number*] [**max-fragments** *number*] [**timeout** *seconds*] [**mode** *modes*][**drop-fragments**]

Example:

Here is the complete configuration example to enable VFR for IPv4 packets:

```
interface GigabitEthernet 5
ip virtual-reassembly-out mode default max-fragments 64
```

To enable VFR for IPv6 packets on inbound interface traffic perform the following steps:

a) Configure an interface type and enter interface configuration mode.

interface *interface-type interface-number*

b) Enable VFR for IPv6 packets on inbound interface traffic.

ipv6 virtual-reassembly [**in**|**out**] [**max-reassemblies** *number*] [**max-fragments** *number*] [**timeout** *seconds*] [**mode** *modes*][**drop-fragments**]

Example:

Here is the complete configuration example to enable VFR for IPv6 packets:

```
interface GigabitEthernet 5
```

```
ipv6 virtual-reassembly in mode default max-fragments 25
max-reassemblies 1024
```

To enable VFR for IPv6 packets on outbound interface traffic perform the following steps:

a) Configure an interface type and enter interface configuration mode.

interface *interface-type interface-number*

b) Enable VFR for IPv6 packets on outbound interface traffic.

ipv6 virtual-reassembly [**in**|**out**] [**max-reassemblies** *number*] [**max-fragments** *number*] [**timeout** *seconds*] [**mode** *modes*][**drop-fragments**]

Example:

Here is the complete configuration example to enable VFR for IPv6 packets:

```
interface GigabitEthernet 5
ipv6 virtual-reassembly out mode default max-fragments 25
```

Configure underlay fragmentation using CLI commands

You can configure underlay fragmentation using CLI templates. For more information about using CLI templates, see *CLI Add-On Feature Templates* and *CLI Templates*.

Note By default, CLI templates execute commands in global config mode.

This section provides example CLI configurations to configure underlay fragmentation.

Procedure

Step 1 Enter the config-sdwan mode

Example:

```
sdwan
```

Step 2 Configure an interface type and enter interface configuration mode.

Example:

```
interface interface-name interface-number
```

Step 3 Configure the tunnel interface.

Example:

```
tunnel-interface
```

Step 4 Skip Layer 3 fragmentation and clear overlay DF bit.

Example:

```
inner-fragmentation-disable
```

Step 5 Perform the encapsulation for the GRE interface of the TLOC.

Example:

```
encapsulation gre
```

Only GRE encapsulation is supported for underlay fragmentation in Cisco IOS XE Catalyst SD-WAN Release 17.12.1a.

Here is the complete configuration example to enable underlay fragmentation:

```
sdwan
interface GigabitEthernet1
tunnel-interface
inner-fragmentation-disable
encapsulation gre
```

Enable boost mode using CLI commands

You can enable boost mode using a CLI template. For more information about using CLI templates, see *CLI Add-On Feature Templates* and *CLI Templates*.

Note By default, CLI templates execute commands in global config mode.

Procedure

Enable the boost mode.

Example:

```
platform ipreass boost-mode
```

Here is the complete configuration example to enable the boost mode:

```
platform ipreass boost-mode
```

Verify VFR and underlay fragments

Boost mode

The following is a sample output of the **show platform hardware qfp active infrastructure cvla client handles** command:

```
Device# show platform hardware qfp active infrastructure cvla client handles
Handles for cpp 0:

---------------------

Entity name: IPREASS_CVLA_0

Handle: 0xeea45000

Number of allocations: 0

Memory allocated: 0


Entity name: FNF_AOR

Handle: 0xeea0d000

Number of allocations: 0

Memory allocated: 0


Entity name: NBAR_CVLA_ENTITY

Handle: 0xee946000

Number of allocations: 0

Memory allocated: 0


Entity name: FNF Chunk 2

Handle: 0xef929000

Number of allocations: 0

Memory allocated: 0


Entity name: FNF Chunk 1

Handle: 0xef928000

Number of allocations: 0

Memory allocated: 0




---------------------
```

The boost mode is disabled if entity for **IPREASS_CVLA_*** is not displayed. Once the boost mode is disabled, the **IPREASS_CVLA_*** disappears after 64 seconds.

VFR for IPv4 packets

The following is a sample output from the **show ip virtual-reassembly** command:

```
Device# show ip virtual-reassembly GigabitEthernet 5
GigabitEthernet5:

   Virtual Fragment Reassembly (VFR) is ENABLED [out]

   Concurrent reassemblies (max-reassemblies): 16

   Fragments per reassembly (max-fragments): 32

   Reassembly timeout (timeout): 3 seconds

   Drop fragments: OFF


   Current reassembly count:0

   Current fragment count:0

   Total reassembly count:12

   Total reassembly timeout
```

The example shows if VFR for IPv4 is enabled or not. **Virtual Fragment Reassembly (VFR) is ENABLED [out]** signifies that VFR is enabled. The total packets that underwent reassembly are also displayed.

VFR for IPv6 packets

The following is a sample output from the **show ipv6 virtual-reassembly** command:

```
Device# show ipv6 virtual-reassembly GigabitEthernet 5
GigabitEthernet5:

   IPv6 Virtual Fragment Reassembly (IPV6VFR) is ENABLED [out]

   IPv6 configured concurrent reassemblies (max-reassemblies): 64

   IPv6 configured fragments per reassembly (max-fragments): 16

   IPv6 configured reassembly timeout (timeout): 3 seconds

   IPv6 configured drop fragments: OFF


   IPv6 current reassembly count:0

   IPv6 current fragment count:0

   IPv6 total reassembly count:12

   IPv6 total reassembly timeout count:0
```

The example shows if VFR for IPv6 is enabled or not. **Virtual Fragment Reassembly (VFR) is ENABLED [out]** signifies that VFR is enabled. The total packets that underwent reassembly are also displayed.

Underlay fragmentation

The following is a sample output from the **show ip traffic interface GigabitEthernet 1** command:

```
Device# show ip traffic interface GigabitEthernet 1
GigabitEthernet 1 statistics :

  Rcvd:  11048818 total, 749458331 total_bytes

         0 format errors, 0 hop count exceeded

         0 bad header, 0 no route

         0 bad destination, 0 not a router

         0 no protocol, 0 truncated

         0 forwarded

         0 fragments, 0 total reassembled

         0 reassembly timeouts, 0 reassembly failures

         0 discards, 0 delivers

  Sent:  0 total, 0 total_bytes 0 discards

         0 generated, 0 forwarded

         0 fragmented into, 0 fragments, 0 failed

  Mcast: 0 received, 0 received bytes

         0 sent, 0 sent bytes

  Bcast: 0 received, 1256 sent
```

The example shows the number of packets that were sent and received, including the total number of packets. A change from the previous number of packet tranfer indicates that underlay fragmentation is enabled.

The following is a sample output from **show sdwan ftm tloc-list** command:

```
Device# show sdwan ftm tloc-list

--- LOCAL  TLOC LIST ---




Id: 32775 (binosId=0xf808007f), Tenant Id: 0      LocalTLOC, num-nhops: 0   ,hash: 0, ref:
 1    SLA 0x0:0x0 Inner-fragmentation
-disable: No


[TOTAL-LOCAL-TLOC:1]



--- REMOTE TLOC LIST ---
```

```
Id: 32768 (binosId=0xf808000f), Tenant Id: 0       SLAClass, num-nhops: 0   ,hash: 0, ref:
 1    SLA 0x0:0x0
 num-active-nhops: 0


Id: 32774 (binosId=0xf808006f), Tenant Id: 0       SLAClass, num-nhops: 1   ,hash: 0, ref:
 1    SLA 0x1:0x0
 [nhop1] nhop-Id: 19   , Type: IPsec     , Encap: IPSEC SLA 0x1:0x0hw_record_index:   5
198.100.1.5/12366->198.100.1.6/12346 pr
oto 0x800 hash 0x13 wan-if 3 tloc 32774 R-color mpls local-tloc 32775 L-color mpls BFD UP
tloc-capability 0 SLA 0x1:0x0 weight
1   pref 0

 num-active-nhops: 1


[TOTAL-REMOTE-TLOC:2]


--- PENDING TLOC LIST (is_pending_updates:FALSE)---



[TOTAL-PENDING-TLOC:0]



--- UNMATCHED TLOC LIST (is_pending_updates:FALSE)---



[TOTAL-UNMATCHED-TLOC:0]



--- TENANT LOCAL  TLOC LIST ---
```

The example displays all the local TLOCs in the network.

The following is a sample output from **show platform software sdwanR0 next-hop overlay all** command:

```
Device# show platform software sdwan R0 next-hop overlay all

Show sdwan next-hop oce all :


OCE ID: 0xf800013f, OCE Type: SDWAN_NH_OVERLAY
```

```
Overlay: client_handle (nil), ppe addr (nil)

  overlay encap: ipsec

  src-ip: 198.100.1.5, src-port: 12366

  dst-ip: 198.100.1.6, dst-port: 12346

  flags: 0x0, linktype: MCP_LINK_IP, ifhandle: 15, encap type: MCP_ET_NULL

  encap rewrite: 00

  mtu: 1446, fixup: 0x0, fixup_flags_2: 0x0, color: mpls, phy_oce_handle: 31, nh_overlay_h:
 0xf800013f
    Overlay_CFG:

    encap type: ipsec

    src-ip: 198.100.1.5, src-port: 12366

    dst-ip: 198.100.1.6, dst-port: 12346

    local_system_ip: 1.1.1.1

    remote_system_ip: 2.2.2.2

    local_color: 2 [mpls], remote_color: 2 [mpls]

    wan_ifindex: 8 [GigabitEthernet2], tun_ifindex: 15 [Tunnel0]

    tun_adj_id: 0, l2_adj_id: 0x1f, tunnel_qos_dpidx: 0x0

    bfd-ld: 20005, ipsec_flow_id: 603979786, session_id: 5

    Inner-fragmentation-disable: yes
```

The example demonstrates whether the inner fragmentation is disabled or enabled in a particular next-hop overlay.

The following is a sample output from **show platform software sdwan F0 next-hop overlay all** command:

```
Device# show platform software sdwan F0 next-hop overlay all

OCE ID: 0xf800013f, OCE Type: SDWAN_NH_OVERLAY

Overlay: client_handle 0x63d321350ba0, ppe addr db910710

  overlay encap: ipsec

  src-ip: 198.100.1.5, src-port: 12366

  dst-ip: 198.100.1.6, dst-port: 12346

  flags: 0x0, linktype: MCP_LINK_SDWAN, ifhandle: 15, encap type: MCP_ET_ARPA

  encap rewrite: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

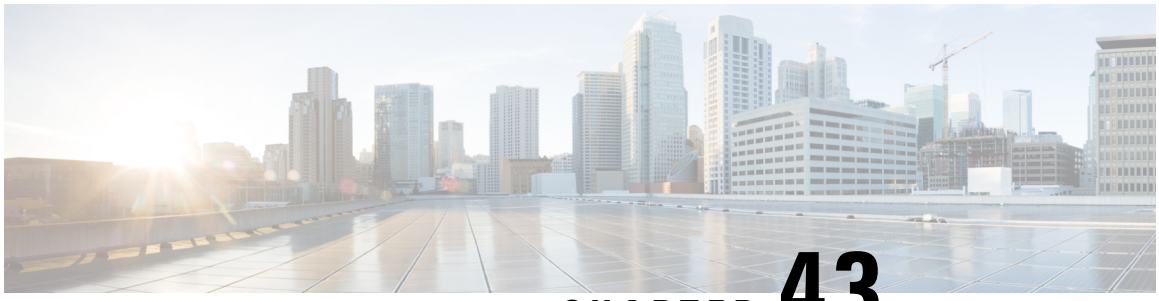
  mtu: 1446, fixup: 0x0, fixup_flags_2: 0x800000, color: mpls, phy_oce_handle: 31,
nh_overlay_h: 0xf800013f
    Overlay_CFG:

    encap type: ipsec

    src-ip: 198.100.1.5, src-port: 12366
```

```
dst-ip: 198.100.1.6, dst-port: 12346
local_system_ip: 1.1.1.1
remote_system_ip: 2.2.2.2
local_color: 2 [mpls], remote_color: 2 [mpls]
wan_ifindex: 8 [GigabitEthernet2], tun_ifindex: 15 [Tunnel0]
tun_adj_id: 0, l2_adj_id: 0x1f, tunnel_qos_dpidx: 0x0
bfd-ld: 20005, ipsec_flow_id: 603979786, session_id: 5
Inner-fragmentation-disable: yes
```

The example demonstrates whether the inner fragmentation is disabled or enabled in all the available overlays.



CHAPTER 43

PPPoE

- Feature history for PPPoE, on page 735
- PPPoE, on page 735
- PPPoE over ATM, on page 736
- Supported platforms for PPPoE over ATM, on page 736
- Configure PPPoE using templates, on page 736
- Configure PPPoE over ATM using templates, on page 739
- Configuration examples for PPPoE, on page 741

Feature history for PPPoE

Table 286: Feature History

Feature Name	Release Information	Description
Configure PPPoE over ATM	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	This feature provides support for configuring PPPoEoA on Cisco IOS XE Catalyst SD-WAN devices. PPPoEoA uses AAL5MUX encapsulation which delivers better efficiency compared to other encapsulation methods.

PPPoE

A Point-to-Point Protocol over Ethernet (PPPoE) is a network protocol that

- connects multiple users over an Ethernet local area network to a remote site through common customer premises equipment,
- is commonly used in broadband aggregation such as by digital subscriber line (DSL), and
- provides authentication with the CHAP or PAP protocol.

In the Cisco Catalyst SD-WAN overlay network, CCisco IOS XE Catalyst SD-WAN devices can run the PPPoE client. The PPPoE server component is not supported. It is recommended that you configure quality

of service (QoS) and shaping rate on a PPPoE Dialer interface. Queuing based QoS policies on both Dialer interface and PPPoE-enabled physical interface at the same time, is not supported.

PPPoE-enabled physical interfaces are supported on ATM PVCs and Ethernet interfaces. A dialer interface must be used for cloning virtual access. Multiple PPPoE client sessions can be configured on an Ethernet interface, but each session must use a separate dialer interface and a separate dialer pool.

The Cisco Catalyst SD-WAN implementation of PPPoE does not support the Compression Control Protocol (CCP) options, as defined in RFC 1962.

PPPoE over ATM

A PPPoEoA is a protocol encapsulation method that

- uses ATM Adaptation Layer 5 Multiplexed Encapsulation (AAL5MUX) to carry PPPoE over ATM permanent virtual circuits (PVCs),
- provides efficiency gain over AAL5 LLC/SNAP encapsulation, and
- reduces Subnetwork Access Protocol (SNAP) encapsulation bandwidth usage by using multiplexed (MUX) encapsulation to reduce the number of cells needed to carry voice packets.

You can configure PPPoE over ATM interfaces (PPPoEoA) on Cisco IOS XE Catalyst SD-WAN devices that support ADSL. Deploying the PPPoEoA over ATM AAL5MUX feature in a VoIP environment results in improved throughput and bandwidth usage.

Supported platforms for PPPoE over ATM

The following platforms support PPPoE over ATM:

- Cisco 1100 4G/6G Series Integrated Services routers.
- Cisco1100 Series Integrated Service routers.
- Cisco1109 Series Integrated Service routers.
- Cisco111x Series Integrated Service routers.
- Cisco1111x Series Integrated Service routers.
- Cisco1120 Series Integrated Service routers.
- Cisco1160 Series Integrated Service routers.

Configure PPPoE using templates

To use Cisco SD-WAN Manager templates to configure PPPoE on Cisco IOS XE Catalyst SD-WAN device, you create three feature templates and one device template:

- Create a VPN-Interface-PPP feature template to configure PPP parameters for the PPP virtual interface.
- Create a VPN-Interface-PPP-Ethernet feature template to configure a PPPoE-enabled interface.

- Optionally, create a VPN feature template to modify the default configuration of VPN 0.
- Create a device template that incorporates the VPN-Interface-PPP, VPN-Interface-PPP-Ethernet, and VPN feature templates.

Follow these steps to configure PPPoE using feature templates.

Procedure

Step 1 Create a VPN-Interface-PPP feature template to configure PPP parameters for the PPP virtual interface.

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
b) Click **Feature Templates**, and click **Add Template**.

In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is titled **Feature**.

c) Choose Cisco IOS XE Catalyst SD-WAN device Cloud or a router model.
d) Choose the **VPN-Interface-PPP** template.
e) In the template, configure the following parameters:

Table 287:

Parameter Field	Procedure
Template Name	Enter a name for the template. It can be up to 128 alphanumeric characters.
Description	Enter a description for the template. It can be up to 2048 alphanumeric characters.
Shutdown	Click **No** to enable the PPP virtual interface.
Interface Name	Enter the number of the PPP interface. It can be from 1 through 31.
Description (optional)	Enter a description for the PPP virtual interface.
Authentication Protocol	Select either CHAP or PAP to configure one authentication protocol, or select PAP and CHAP to configure both. For CHAP, enter the hostname and password provided by your ISP. For PAP, enter the username and password provided by your ISP. If you are configuring both PAP and CHAP, to use the same username and password for both, click Same Credentials for PAP and CHAP.
AC Name (optional)	Select the PPP tab, and in the AC Name field, enter the name of the the name of the access concentrator used by PPPoE to route connections to the Internet.
IP MTU	Click **Advanced**, and in the IP MTU field, ensure that the IP MTU is at least 8 bytes less than the MTU on the physical interface. The maximum MTU for a PPP interface is 1492 bytes. If the PPPoE server does not specify a maximum receive unit (MRU), the MTU value for the PPP interface is used as the MRU. Starting from Cisco vManage Release 20.9.1, there is 8 bytes overheads deduced based on the specified IP MTU value when configuration is pushed to the device.
Save	To save the feature template, click **Save**.

Step 2 Create a VPN-Interface-PPP-Ethernet feature template to enable the PPPoE client on the physical interfaces.

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

b) Click **Feature Templates**, and click **Add Template**.

In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is titled **Feature**.

c) Choose Cisco IOS XE Catalyst SD-WAN device Cloud or a router model.

d) Choose the **VPN-Interface-PPP-Ethernet** template.

e) In the template, configure the following parameters:

Parameter Field	Procedure
Template Name	Enter a name for the template. It can be up to 128 alphanumeric characters.
Description	Enter a description for the template. It can be up to 2048 alphanumeric characters.
Shutdown	Click **No** to enable the PPPoE-enabled interface.
Interface Name	Enter the name of the physical interface in VPN 0 to associate with the PPP interface.
Description (optional)	Enter a description for the PPPoE-enabled interface.
IP Confguration	Assign an IP address to the physical interface: • To use DHCP, select Dynamic. The default administrative distance of routes learned from DHCP is 1. • To configure the IP address directly, enter of the IPv4 address of the interface.
DHCP Helper (optional)	Enter up to four IP addresses for DHCP servers in the network.
Save	To save the feature template, click **Save**.

Step 3 Create a VPN feature template to configure the PPPoE-enabled interface in VPN 0, the transport VPN.

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

b) Click **Feature Templates**, and click **Add Template**.

In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is titled **Feature**.

c) Choose Cisco IOS XE Catalyst SD-WAN device Cloud or a router model.

d) Choose the **VPN** template.

e) In the template, configure the following parameters:

Parameter Field	Procedure
Template Name	Enter a name for the template. It can be up to 128 alphanumeric characters.
Description	Enter a description for the template. It can be up to 2048 alphanumeric characters.
VPN Identifier	Enter VPN identifier 0.
Name	Enter aname for the VPN.

Parameter Field	Procedure
Other interface parameters	Configure the desired interface properties.
Save	To save the feature template, click **Save**.

Step 4 Create a device template that incorporates the VPN-Interface-PPP, VPN-Interface-PPP-Ethernet, and VPN feature templates.

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
b) Click **Device Templates**, and then click **Create Template**.

In Cisco vManage Release 20.7.1 and earlier releases, **Device Templates** is titled **Device**.

c) From the **Create Template** drop-down list, choose From Feature Template.

From the **Device Model** drop-down list, choose the type of device for which you are creating the device template.

Cisco SD-WAN Manager displays the feature templates for the device type you selected. Required templates are indicated with an asterisk (*).

Enter a name and description for the device template. These fields are mandatory. The template name cannot contain special characters.

d) In **Transport & Management VPN**, under **VPN 0**, from the drop-down list of available templates, select the desired feature template. The list of available templates are the ones that you have previously created.
e) In **Additional VPN 0 Templates**, click the plus sign (+) next to **VPN Interface PPP**.
f) From **VPN-Interface-PPP** and **VPN-Interface-PPP-Ethernet** fields, select the feature templates to use.
g) To configure multiple PPPoE-enabled interfaces in VPN 0, click the plus sign (+) next to Sub-Templates.
h) To include additional feature templates in the device template, in the remaining sections, select the feature templates in turn, and from the drop-down list of available templates, select the desired template. The list of available templates are the ones that you have previously created. Ensure that you select templates for all mandatory feature templates and for any desired optional feature templates.
i) To create the device template, click **Create**.

Step 5 Attach a device template to a device.

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
b) Click **Device Templates**, and then click **Create Template**.

In Cisco vManage Release 20.7.1 and earlier releases, **Device Templates** is titled **Device**.

c) Choose a template.
d) Click …, and click **Attach Device**.
e) Search for a device or select a device from the Available Device(s) column to the left.
f) Click the arrow pointing right to move the device to the Selected Device(s) column on the right.
g) Click **Attach**.

Configure PPPoE over ATM using templates

Follow these steps to configure PPPoE using the device CLI template in Cisco SD-WAN Manager.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 From **Device Templates**, click **Create Template**.

In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

Step 3 From the **Create Template** drop-down list, select **CLI Template**.

Step 4 From the **Device Model** drop-down list, select the type of device for which you are creating the template.

a) In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

b) In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

Step 5 Choose **Device configuration**.

Using this option, you can provide IOS-XE configuration commands that appear in the output of the **show sdwan running-config** command.

Step 6 (Optional) To load the running config of a connected device, select it from the Load Running config from reachable device list and click **Search**.

Step 7 In CLI Configuration, enter the configuration either by typing it, cutting and pasting it, or uploading a file.

```
Device(config)# interface atm number
Device(config)# no ip address
Device(config)# interface atm number point-to-point
Device(config)# no atm enable-ilmi-trap
Device(config)# encapsulation aal5mux  pppoe-client
Device(config)# pppoe-client dial-pool-number number
Device(config)# interface Dialer dialer-rotary-group-number
Device(config)# mtu bytes
Device(config)# ip address negotiated
Device(config-if)# encapsulation encapsulation-type
Device(config)# load-interval seconds
Device(config)# dialer pool number
Device(config)# dialer-group group-number
Device(config)# ppp mtu adaptive
Device(config)# ppp chap hostname hostname
Device(config)# ppp chap password secret
Device(config)# ppp ipcp address required
Device(config)# ppp link reorders
```

Step 8 To convert an actual configuration value to a variable, select the value and click Create Variable. Enter the variable name, and click Create Variable. You can also type the variable name directly, in the format {{*variable-name*}}; for example, {{hostname}}.

Step 9 Click **Add**. The new device template is displayed in the Device Template table. The **Type** column shows **CLI** to indicate that the device template was created from CLI text.

Configuration examples for PPPoE

PPPoE server on IPv4 interfaces

This example shows configuring PPPoE server on IPv4 interfaces:

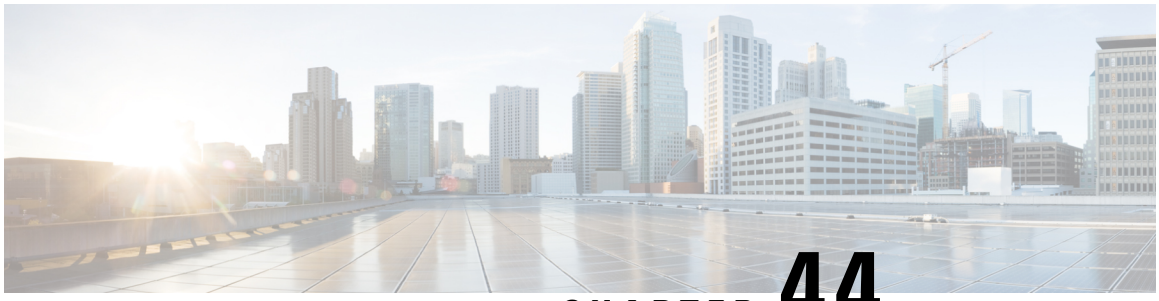
```
!
interface Dialer100
 mtu 1492
 ip address negotiated
 encapsulation ppp
 ip tcp adjust-mss 1460
 dialer pool 100
 dialer down-with-vInterface
 ppp authentication chap callin
 ppp chap hostname cisco
 ppp chap password 7 1511021F07257A767B
 ppp ipcp route default
```

To replace a template configured with PPPoE as WAN interface with a regular interface in Dialer100, remove the IP address assigned to the dialer interface using the **no ip address** command, and then add a new IP address for the dialer interface.

PPPoE over ATM interfaces

This example shows configuring PPPoE over ATM interfaces.

```
Device(config)# interface ATM0/1/0
Device(config)# no ip address
Device(config)# no atm enable-ilmi-trap
!
Device(config)# interface ATM0/1/0.10 point-to-point
Device(config)# no atm enable-ilmi-trap
Device(config)# cdp enable
Device(config)# pvc 22/62
Device(config)# ubr 1045
Device(config-if)# encapsulation aal5mux pppoe-client
Device(config)# pppoe-client dial-pool-number 120
!
!
Device(config)# interface Dialer 120
Device(config)# mtu 1492
Device(config)# ip address negotiated
Device(config)# ip nat outside
Device(config-if)# encapsulation ppp
Device(config)# load-interval 30
Device(config)# dialer pool 120
Device(config)# dialer-group 1
Device(config)# ppp mtu adaptive
Device(config)# ppp chap hostname test@cisco.com
Device(config)# ppp chap password 0 cisco
Device(config)# ppp ipcp address required
Device(config)# ppp link reorders
!
```



CHAPTER 44

GRE-in-UDP

- Feature history for GRE-in-UDP, on page 743
- GRE-in-UDP, on page 743
- Configure GRE-in-UDP using CLI commands, on page 743

Feature history for GRE-in-UDP

Table 288: Feature History

Feature Name	Release Information	Description
GRE-in-UDP	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	You can configure GRE encapsulation for UDP transport.

GRE-in-UDP

A GRE-in-UDP protocol is a network protocol that

- encapsulates Generic Routing Encapsulation (GRE) tunnels within a User Datagram Protocol (UDP) packet to facilitate load balancing and improve performance over networks, and
- enables a router to encapsulate GRE packets—including source and destination port information—within a UDP header, send the UDP packet through the tunnel, and allow the destination device to de-encapsulate the UDP packet.

Cisco Catalyst SD-WAN supports generic routing encapsulation (GRE) with UDP for IPv4 and IPv6 traffic.

Configure GRE-in-UDP using CLI commands

Follow these steps to configure GRE-in-UDP using a CLI template.

For more information about using CLI templates, see *CLI Add-On Feature Templates* and *CLI Templates*. By default, CLI templates execute commands in global config mode.

GRE-in-UDP is a protocol that encapsulates Generic Routing Encapsulation (GRE) tunnels within a User Datagram Protocol (UDP) packet to facilitate load balancing and improve performance over networks.

Procedure

Step 1 For the desired interface, enter interface configuration mode.

```
sdwan
interface interface
```

Step 2 Enter tunnel interface mode.

```
tunnel-interface
```

Step 3 Configure GRE encapsulation.

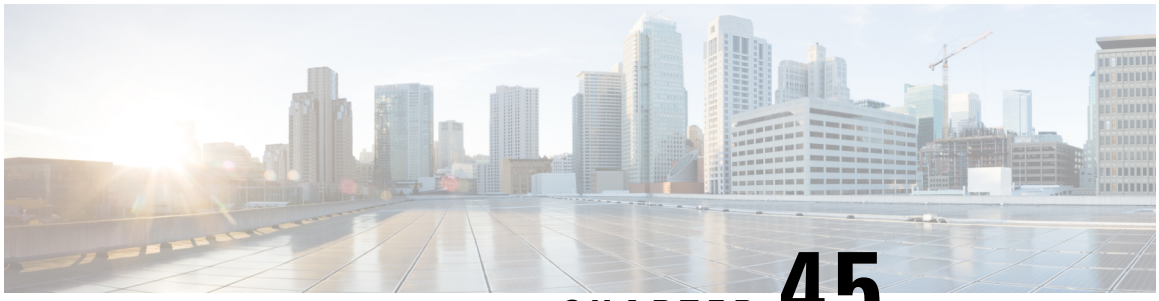
```
encapsulation gre
```

Step 4 Configure GRE-in-UDP as the encapsulation mode.

```
gre-in-udp
```

Here is a complete example of configuring GRE-in-UDP.

```
interface GigabitEthernet1
  tunnel-interface
   encapsulation gre
   color lte
   gre-in-udp
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   no allow-service snmp
   no allow-service bfd
  exit
```



CHAPTER 45

Track Static Routes for Service VPNs

- Feature history of track static routes for service VPNs, on page 745
- Track static routes for service VPNs, on page 746
- Supported platforms, on page 746
- Restrictions for IPv4 static route tracking, on page 747
- Configure tracker group using a configuration group, on page 747
- Create a static route tracker, on page 748
- Configure a next hop static route with tracker, on page 750
- Monitor static route tracker configuration, on page 751
- Configure static routes using CLI, on page 751
- Configuration examples static route tracking, on page 753
- Verify static route tracking configuration, on page 754

Feature history of track static routes for service VPNs

This table describes the developments of this feature, by release.

Table 289: Feature history

Feature Name	Release Information	Description
Static Route Tracker for Service VPNs	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature enables you to configure IPv4 static route endpoint tracking for service VPNs. For static routes, endpoint tracking determines whether the configured endpoint is reachable before adding that route to the route table of the device.
TCP/UDP Endpoint Tracker and Dual Endpoint Static Route Tracker for Cisco IOS XE Catalyst SD-WAN devices	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	This feature enables you to configure the TCP/UDP static route endpoint trackers. Using this feature you can also configure IPv4, TCP/UDP dual endpoint static-route tracker groups for service VPNs to enhance the reliability of probes.

Track static routes for service VPNs

Tracking static routes for service VPNs allows you to monitor the reachability of the configured next-hop endpoint IP address. You can verify the endpoint before the device adds the static route to its routing table. This is particularly important in service VPNs where static routes are advertised over the Overlay Management Protocol (OMP). The static route tracker periodically sends Internet Control Message Protocol (ICMP) ping probes to the configured endpoint IP address. If the endpoint is unreachable (no response to probes), the static route is excluded from the routing table and is not advertised to OMP, preventing traffic blackholing. You can configure backup routes with higher administrative distance to provide alternate paths.. This mechanism enhances route reliability and network stability in SD-WAN environments. The tracker sends periodic probes (ICMP echo requests, TCP, or UDP probes) to the static route's next-hop IP address.

- If the endpoint is unreachable, the static route is removed from the routing table and not advertised to OMP.
- Configure backup static routes with higher administrative distance for failover.
- Only one endpoint tracker is supported per static route per next-hop.
- IPv6 static routes are not supported for tracking.
- You can configure dual endpoint tracker groups to enhance probe reliability.
- This feature is supported on Cisco IOS XE Catalyst SD-WAN platforms such as ASR 1000, ISR 1000 and 4000, and CSR 1000 series routers.
- This feature ensures that static routes in service VPNs are advertised only when their next-hop endpoints are reachable. As a result, it prevents traffic blackholing and improves network resilience.

From Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, you can configure TCP or UDP individual endpoint trackers and configure a tracker group with dual endpoints (using two trackers), and associate the trackers and tracker group to a static route. Dual endpoints help avoid false negatives that route unavailability might introduce.

Starting with Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, Cisco SD-WAN Manager reports only UP/DOWN status changes. It does not report RTT value changes. This optimization improves efficiency in extensive networks.

Supported platforms

These devices support static route tracking for service VPNs:

- Cisco ASR 1000 Series Aggregated Services Routers
- Cisco ISR 1000 Series-Integrated Services Routers
- Cisco ISR 4000 Series Integrated Services Routers
- Cisco CSR 1000 Series Cloud Service Routers

Restrictions for IPv4 static route tracking

- Only one endpoint tracker is supported per static route per next-hop address.
- IPv6 static routes are not supported.
- To configure a static route with tracker:
  1. Delete any existing static route, if it is already configured without a tracker. Plan for any connectivity downtime that might occur during this step for static route advertisement.
  2. Configure a new static route with tracker using the same prefix and next-hop as the deleted static route.
- To add a new tracker after you reach maximum tracker limit per router:
  1. Delete an old tracker and attach the template to the device.
  2. Add a new tracker and attach the device to the template again.
- UDP tracker endpoint enabled with IP SLA UDP packet responder is supported only on Cisco IOS XE Catalyst SD-WAN devices.
- You cannot link the same endpoint-tracker to static routes in different VPNs. Endpoint-tracker is identified by a name and can be used for multiple static routes in a single VPN.

Configure tracker group using a configuration group

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure a tracker group in a Service Profile.

Table 290: Tracker Group

Field	Description
Tracker Elements*	This field is displayed only if you chose **Tracker Type** as the **Tracker Group**. Add the existing interface tracker names, separated with a space. When you add this tracker to the template, the tracker group is associated with these individual trackers, and you can then associate the tracker group to an interface.

Field	Description
Tracker Boolean	This field is displayed only if you chose **Tracker Type** as the **Tracker Group**. Select **AND** or **OR**. **OR** is the default boolean operation. An **OR** ensures that the transport interface status is reported as active if either one of the associated trackers of the tracker group reports that the interface is active. If you select the **AND** operation, the transport-interface status is reported as active if both the associated trackers of the tracker group report that the interface is active.

What to do next

Also see Deploy a configuration group.

Create a static route tracker

Before you begin

Use the **System Template** to create a tracker for static routes.

Delete existing static routes, if any, before you create a static route tracker. Configure a new static route tracker using the same prefix and next hop as the deleted static route.

Procedure

Step 1 From Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**.

Step 3 Navigate to the **Cisco System** template for the device.

For information about creating a System template, see Create System Template.

Step 4 Click **Tracker**. Click **New Endpoint Tracker** to configure the tracker parameters.

Table 291: Tracker Parameters

Field	Description
Name	Name of the tracker. The name can be up to 128 alphanumeric characters.
Threshold	Wait time for the probe to return a response before declaring that the configured endpoint is down. The range is from 100 to 1000 milliseconds. The default is 300 milliseconds.

Field	Description
Interval	Time interval between probes to determine the status of the configured endpoint. The default is 60 seconds (1 minute). The range is from 20 to 600 seconds.
Multiplier	Number of times probes are sent before declaring that the endpoint is down. The range is from 1 to 10. The default is 3.
Tracker Type	From the drop-down, choose Global. From the Tracker Type field drop-down, choose Static Route. From Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, you can configure a tracker group with dual endpoints on Cisco IOS XE Catalyst SD-WAN devices. You can associate this tracker group to a static route.
Endpoint Type	Choose endpoint type IP address. **Note** Configuring the tracker type Static Route using endpoint URL or endpoint DNS name is not supported.
End-Point Type: IP Address	IP address of the static route end point. This is the destination on the internet to which the router sends probes to determine the status of the route.

Step 5 Click **Add**.

Step 6 Click **Save**.

Complete all mandatory actions before saving the template.

Step 7 To create a tracker group, click **Tracker Groups** > **New Endpoint Tracker Groups** and configure the tracker parameters.

Ensure that you have created two trackers to form a tracker group.

Table 292: Tracker Group Parameters

Fields	Description
Name	Name of the tracker group.
Tracker Type	From the drop-down, choose **Global**. From the Tracker Type field drop-down, choose **Static Route**. From Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, you can configure a tracker group with dual endpoints on Cisco IOS XE Catalyst SD-WAN devices and associate this tracker group to a static route.
Tracker Elements	This field is displayed only if you chose **Tracker-group** as the tracker type. Add the existing interface tracker names (separated by a space). When you add this tracker to the template, the tracker group is associated with these individual trackers, and you can then associate the tracker group to a static route.

Fields	Description
Tracker Boolean	From the drop-down list, choose **Global**. This field is displayed only if you chose **tracker-group** as the **Tracker Type**. By default, the **OR** option is selected. Choose **AND** or **OR**. **OR** ensures that the static route status is reported as active if either one of the associated trackers of the tracker group report that the route is active. If you select **AND**, the static route status is reported as active if both the associated trackers of the tracker group report that the route is active.

Step 8 Click **Add**.

Step 9 Click **Save**.

Complete all mandatory actions before saving the template.

Configure a next hop static route with tracker

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates** and navigate to **Cisco VPN Template** for the device.

For information about creating a VPN template, see Create VPN Template.

Step 3 Enter **Template Name** and **Description** as required.

Step 4 In Basic Configuration, by default, VPN is set to 0. Set a VPN value within (1–511, 513–65530) range for service VPNs, for service-side data traffic on Cisco IOS XE Catalyst SD-WAN devices.

You can configure static route tracker only on service VPNs.

Step 5 Click **IPv4 Route** and **New IPv4 Route**.

Step 6 In the **IPv4 Prefix** field, enter a value.

Step 7 Click **Next Hop**. Click **Add Next Hop** with **Tracker** and enter values for the fields listed in the table.

Parameter Name	Description
Address	Specify the next-hop IPv4 address.
Distance	Specify the administrative distance for the route.
Tracker	Enter the name of the gateway tracker to determine whether the next hop is reachable before adding that route to the route table of the device.

Parameter Name	Description
Add Next Hop with Tracker.	Enter the name of the gateway tracker with the next hop address to determine whether the next hop is reachable before adding that route to the route table of the device.

Step 8 Click **Add** and **Save** to create the static route with the next-hop tracker.

You need to fill all the mandatory fields in the form to save the VPN template.

Monitor static route tracker configuration

To view information about a static tracker on a transport interface:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

Step 2 Choose a device from the list of devices.

Step 3 Click **Real Time**.

Step 4 From the **Device Options** drop-down list, choose **Endpoint Tracker Info**.

Configure static routes using CLI

These sections provide information about how to configure static routes using the CLI.

You can configure static route tracking using the Cisco SD-WAN Manager CLI Add-on feature templates and CLI device templates. For more information on configuring using CLI templates, see CLI Templates.

Configure a static route tracker

```
Device# config-transaction
Device(config)# endpoint-tracker <tracker-name>
Device(config-endpoint-tracker)# tracker-type <tracker-type>
Device(config-endpoint-tracker)# endpoint-ip <ip-address>
Device(config-endpoint-tracker)# threshold <value>
Device(config-endpoint-tracker)# multiplier <value>
Device(config-endpoint-tracker)# interval <value>
Device(config-endpoint-tracker)# exit
Device(config)# track <tracker-name> endpoint-tracker
```

Configure a static route tracker with TCP port as the endpoint

```
Device# config-transaction
Device(config)# endpoint-tracker <tracker-name>
Device(config-endpoint-tracker)# tracker-type <tracker-type>
Device(config-endpoint-tracker)# endpoint-ip <ip-address> tcp <port-number>
```

```
Device(config-endpoint-tracker)# threshold <value>
Device(config-endpoint-tracker)# multiplier <value>
Device(config-endpoint-tracker)# interval <value>
Device(config-endpoint-tracker)# exit
Device(config)# track <tracker-name> endpoint-tracker
```

Configure a static route tracker with UDP port as the endpoint

```
Device# config-transaction
Device(config)# endpoint-tracker <tracker-name>
Device(config-endpoint-tracker)# tracker-type <tracker-type>
Device(config-endpoint-tracker)# endpoint-ip <ip-address> udp <port-number>
Device(config-endpoint-tracker)# threshold <value>
Device(config-endpoint-tracker)# multiplier <value>
Device(config-endpoint-tracker)# interval <value>
Device(config-endpoint-tracker)# exit
Device(config)# track <tracker-name> endpoint-tracker
```

Configure tracker groups

You can create tracker groups to probe static routes from Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1.

```
Device# config-transaction
Device(config)# endpoint-tracker <tracker-name1>
Device(config-endpoint-tracker)# tracker-type <tracker-type>
Device(config-endpoint-tracker)# endpoint-ip <ip-address> tcp <port-number>
Device(config-endpoint-tracker)# threshold <value>
Device(config-endpoint-tracker)# multiplier <value>
Device(config-endpoint-tracker)# interval <value>
Device(config-endpoint-tracker)# exit
Device(config)# track <tracker-name1> endpoint-tracker


Device# config-transaction
Device(config)# endpoint-tracker <tracker-name2>
Device(config-endpoint-tracker)# tracker-type <tracker-type>
Device(config-endpoint-tracker)# endpoint-ip <ip-address> udp <port-number>
Device(config-endpoint-tracker)# threshold <value>
Device(config-endpoint-tracker)# multiplier <value>
Device(config-endpoint-tracker)# interval <value>
Device(config-endpoint-tracker)# exit
Device(config)# track <tracker-name2> endpoint-tracker


Device(config)# endpoint-tracker <static-tracker-group>
Device(config-endpoint-tracker)# tracker-type tracker-group
Device(config-endpoint-tracker)# tracker-elements <tracker-name1> <tracker-name2>
Device(config-endpoint-tracker)# boolean {and | or}
Device(config-endpoint-tracker)# exit
Device(config)# track <static-tracker-group> endpoint-tracker

Device(config)# ip route vrf <vrf-name> <prefix> <mask> <nexthop-ipaddress>
<administrative-distance> track name <static-tracker-group>
```

Note

- Use the **ip route** command to bind a tracker or tracker group with a static route and to configure a backup route for administrative distance that is higher than the default value of 1.
- You can apply only one tracker to an endpoint.
- A tracker group can have a mix of endpoint trackers. For example, you can create a tracker group with an IP address tracker and UDP tracker.

Configuration examples static route tracking

Configure Tracker

This example shows how to configure a single static route tracker:

```
config-transaction
!
 endpoint-tracker tracker1
!
  tracker-type static-route
  endpoint-ip 10.1.1.1
  threshold 100
  multiplier 5
  interval 20
  exit
!
track tracker1 endpoint-tracker
!
ip route vrf 1 192.168.0.0 255.255.0.0 10.1.19.16 100 track name tracker1
```

This example shows how to configure a tracker with TCP port as endpoint:

```
config-transaction
!
 endpoint-tracker tcp-10001
!
  tracker-type static-route
  endpoint-ip 10.0.0.1 tcp 10001
  threshold    100
  interval     10
  multiplier   1
  exit
!
track tcp-10001 endpoint-tracker
!
ip route vrf 1 192.168.0.0 255.255.0.0 10.1.19.16 100 track name tcp-10001
```

This example shows how to configure a tracker with UDP port as endpoint:

```
config-transaction
!
  endpoint-tracker udp-10001
!
    tracker-type static-route
    endpoint-ip 10.0.0.1 udp 10001
```

```
    threshold    100
    interval     10
    multiplier   1
    exit
!
track udp-10001 endpoint-tracker
!
ip route vrf 1 192.168.0.0 255.255.0.0 10.1.19.16 100 track name udp-10001
```

Configure Tracker Groups

This example shows how to configure a tracker group with two trackers (two endpoints). You can create tracker groups to probe static routes.

```
config-transaction
!
 endpoint-tracker tcp-10001
!
    tracker-type static-route
    endpoint-ip 10.1.1.1 tcp 10001
    threshold 100
    multiplier 5
    interval 20
    track tcp-10001 endpoint-tracker
!
 endpoint-tracker udp-10002
!
   tracker-type static-route
   endpoint-ip 10.2.2.2 udp 10002
   threshold 100
   multiplier 5
   interval 20
   track udp-10002 endpoint-tracker
!
endpoint-tracker static-tracker-group
!
  tracker-type tracker-group
  tracker-elements tcp-10001 udp-10002
  boolean and
  track static-tracker-group endpoint-tracker
!
ip route vrf 1 192.168.0.0 255.255.0.0 10.1.19.16 100 track name static-tracker-group
```

Note

- You must configure an administrative distance when you are configuring through CLI templates.
- Use the **ip route** command to bind the tracker or tracker group with a static route and to configure a backup route for administrative distance when it is higher than the default value of 1.
- You can apply only one tracker to an endpoint.

Verify static route tracking configuration

Use these commands to verify if the configuration is committed. The sample configuration shows tracker definition for a static route tracker and it's application to an IPv4 static route:

```
Device# show running-config | sec endpoint-tracker
endpoint-tracker tracker1
endpoint-ip 10.1.1.1
interval 60
multiplier 5
tracker-type static-route
endpoint-tracker tracker2
endpoint-ip 10.1.1.12
interval 40
multiplier 2
tracker-type static-route
track tracker2 endpoint-tracker
track tracker1 endpoint-tracker
```

Use this command to verify the IPv4 route:

```
Device# show running-config | inc ip route
ip route vrf 1 10.1.1.11 255.255.0.0 10.20.2.17 track name tracker2
ip route vrf 1 10.1.1.12 255.255.0.0 10.20.24.17 track name tracker1
```

The sample output from the **show endpoint-tracker static-route** command displaying individual static route tracker status:

```
Device#  show endpoint-tracker static-route
Tracker Name   Status     RTT (in msec) Probe ID
tcp-10001         UP         3             1
udp-10002         UP         1             6
```

The sample output from the **show endpoint-tracker tracker-group** command displaying tracker group status:

```
Device# show endpoint-tracker group
Tracker Name               Element trackers name    Status         RTT in msec  Probe ID

group-tcp-10001-udp-10002  tcp-10001, udp-10002     UP(UP AND UP)  5, 1          9, 10
```

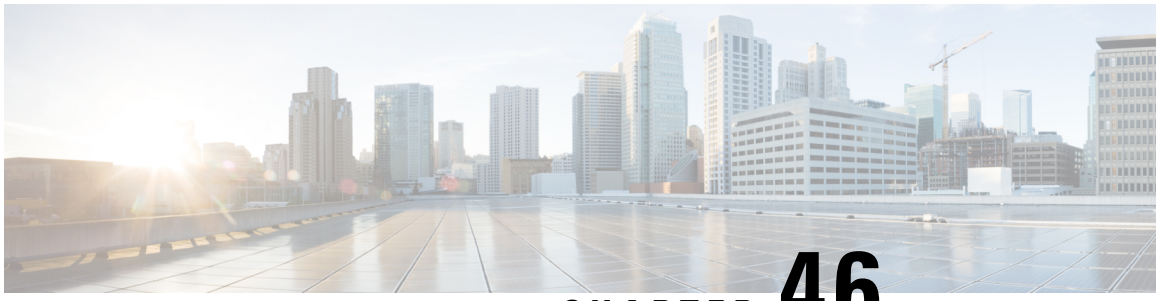
The sample output from the **show endpoint-tracker records** command displaying tracker/tracker group configuration:

```
Device# show endpoint-tracker records
Record Name                Endpoint                 EndPoint Type Threshold(ms) Multiplier
 Interval(s) Tracker-Type
group-tcp-10001-udp-10002  tcp-10001 AND udp-10002  N/A           N/A           N/A
 N/A         static-tracker-group
tcp-10001                  10.1.1.1                 TCP           100           1
 20          static-route
udp-10002                  10.2.2.2                 UDP           100           1
 20          static-route
```

The sample output from the **show ip static route vrf** command:

```
Device# show ip static route vrf 1
Codes: M - Manual static, A - AAA download, N - IP NAT, D - DHCP,
       G - GPRS, V - Crypto VPN, C - CASA, P - Channel interface processor,
       B - BootP, S - Service selection gateway
       DN - Default Network, T - Tracking object
       L - TL1, E - OER, I - iEdge
       D1 - Dot1x Vlan Network, K - MWAM Route
       PP - PPP default route, MR - MRIPv6, SS - SSLVPN
       H - IPe Host, ID - IPe Domain Broadcast
       U - User GPRS, TE - MPLS Traffic-eng, LI - LIIN
       IR - ICMP Redirect, Vx - VXLAN static route
       LT - Cellular LTE, Ev - L2EVPN static route
Codes in []: A - active, N - non-active, B - BFD-tracked, D - Not Tracked, P - permanent,
-T Default Track
Codes in (): UP - up, DN - Down, AD-DN - Admin-Down, DL - Deleted
```

```
Static local RIB for 1
T  192.168.0.0 [1/0] via 10.1.19.16 [A]
```



CHAPTER 46

VDSL and GSHDSL

- VDSL and GSHDSL, on page 757
- GSHDSL EFM-ATM NIM, on page 761
- Cisco VDSL examples, on page 761
- Cisco GSHDSL examples, on page 763

VDSL and GSHDSL

Very High-Speed Digital Subscriber Line (VDSL) is a digital subscriber line (DSL) technology that provides high-speed data transmission over existing copper telephone wires. It is an advanced version of earlier DSL standards like ADSL, offering significantly faster speeds by utilizing higher frequency ranges

Symmetric High-Speed Digital Subscriber Line (G.SHDSL) is a data communications technology designed for symmetric high-speed data transmission over copper twisted pairs. While the query mentioned G.HDSL, G.SHDSL (standardized as ITU-T G.991.2) is the more modern and widely adopted international standard for symmetric DSL. G.HDSL (G.991.1) is an older standard.

Key characteristics of VDSL

- Speed: VDSL can offer speeds up to 52 Mbit/s downstream and 16 Mbit/s upstream. Its successor, VDSL2 (ITU-T G.993.2), can provide data rates exceeding 100 Mbit/s simultaneously in both upstream and downstream directions, and VDSL2+ can reach 300+ Mbit/s.
- Technology: It uses frequencies up to 12 MHz (VDSL) or up to 30 MHz (VDSL2) to achieve these higher speeds.
- Applications: VDSL is capable of supporting applications such as high-definition television (HDTV), voice over IP (VoIP), and general high-speed internet access over a single connection.
- Distance Sensitivity: The performance of VDSL degrades as the distance from the service provider's equipment increases.

For related information, see VDSL Commands.

Key characteristics of G.SHDSL

G.SHDSL is an international standard that allows devices to send and receive high-speed symmetrical data streams over a single pair of copper wires. This section provides information about the Cisco G.SHDSL EFM/ATM NIM and provides guidelines for configuring G.SHDSL in SD-WAN mode.

- Symmetry: Unlike asymmetric DSL (ADSL), G.SHDSL provides symmetrical transmit and receive data rates, meaning the upload and download speeds are equal.
- Speed: It offers symmetric rates typically ranging from 192 kbit/s to 15296 kbit/s on a single twisted pair.
- Applications: G.SHDSL is often used for high-speed commercial broadband services, enabling applications that require significant data transfer in both directions, such as LAN remote access, web hosting, and combining multiple voice and data channels.
- Compatibility: It is compatible with other DSL technologies and can extend transmission distances while maintaining high data rates.

For related information, see Configuring Cisco G.SHDSL HWICs in Cisco Access Routers and VDSL Commands.

VDSL configuration guidelines

This table provides usage information and guidelines for configuring asymmetric DSL (ADSL2/2+) and VDSL for supported Integrated Services Router Network Interface Modules (ISR NIMs) in SD-WAN mode. VDSL2 and ADSL2/2+ provide highly reliable WAN connections for remote sites.

Function	Command	Guidelines
Configure operating mode	Device# **configure terminal** Device(config)# **controller VDSL** *slot/subslot/port* Device(config)# **operating mode auto**	To switch from operating mode auto adsl1 (adsl2+/ or vdsl2) to operating mode auto ads2+ (adsl1 or vdsl2), switch to operating mode auto first. Before you change the operating mode, ensure that line-mode is changed to line-mode single-wire line 0.
Enable DSL on a line	Device(config)# **line-mode single-wire line** *line-number*	This command is supported only on DSL NIM-VAB-A.
Enable bonding	Device(config)# **line-mode bonding**	This command is supported only on DSL NIM-VAB-A.
Load firmware on a device	Device# **configure terminal** Device(config)# **controller VDSL** *slot / subslot / port* Device(config-controller)# **firmware phy filename** *filename*	The Cisco Catalyst SD-WAN CLI template does not support specifying the file location. Prepend the file name with flash: or with bootflash:, depending on its location.

Function	Command	Guidelines
Enable or disable SRA	Device(config-controller)# **sra**	The Cisco Catalyst SD-WAN CLI template does not support the sra *line number* command. In line-mode bonding, sra enables sra on both lines and no sra disables sra on both lines.
Enable or disable bitswap	Device(config-controller)# **bitswap**	The Cisco Catalyst SD-WAN CLI template does not support the bitswap *line number* command. In line-mode bonding, bitswap enables bitswap on both lines and no bitswap disables bitswap on both lines.
Enable modem features	Device(config-controller)# **modem** *keyword*	–
Display a description of a controller	Device(config-controller)# **description** *string*	–
Enable dual ended line testing	Device(config-controller)# **diagnostics DELT**	–
Modify the file in which the training log is stored	Device(config-controller)# **training log filename flash:** *filename*	The Cisco Catalyst SD-WAN CLI template does not support specifying the file location. Prepend the file name with flash: or with bootflash:, depending where the file should be stored.
Enable sync mode	Device(config-controller)# **sync mode** *mode*	To switch from one sync mode to another, delete the existing sync mode, then configure the new one.
Enable sync interval	Device(config-controller)# **sync interval** *seconds*	–

GSHDSL configuration guidelines

This table provides usage information and guidelines that apply when you configure the Cisco G.SHDSL EFM/ATM in CPE or CO mode.

Function	Command	Guidelines
Configure a device with the dsl-group auto command	Device(config-controller)# **dsl-group auto**	Use customer premises equipment (CPE) mode when configuring a device with the dsl-group auto command. If you use this command in Central Office (CO) mode, the configuration does not take effect.
Add or delete a link	—	The efm-grp command is not supported. To add or delete a link to a dsl-group, delete the dsl-group, then create a new dsl-group.
Load firmware on a device	Device(config-controller)# **firmware phy filename** *location*	File name location options are not supported when using the firmware phy command. Prepend the file name with flash: or with bootflash:, depending on the location.
Create or delete an annex	Device(config-controller-dsl-group)# **no shdsl annex** Device(config-controller-dsl-group)# **no shdsl rate** *rate*	To avoid Cisco IOS and Cisco Catalyst SD-WAN configuration from going out of sync when you create or delete an annex, create or delete the rate in the same transaction.
Enable SHDSL to use enhanced mode	(config-controller-dsl-group)# **shdsl 4-wire mode enhanced**	To enable SHDSL to use the enhanced mode in a 2-pair digital subscriber line (DSL) group, use the shdsl 4-wire mode enhanced command in configuration controller DSL group mode.
Ignore CRC errors	(config-controller-dsl-group)# **ignore** *seconds*	To configure a device to ignore CRC errors, use the ignore command. Replace *timeout* with a value from 0 through 60, which indicates the number of seconds that the device ignores CRC errors that do not resolve before the device terminates an action.
Shutdown a DSL group	(config-controller-dsl-group)# **shutdown**	To shut down a DSL group, use the shutdown command.

GSHDSL EFM-ATM NIM

G.SHDSL EFM/ATM NIM

The Cisco G.SHDSL EFM/ATM NIM connects Cisco 4000 Series Integrated Services Routers with central office Digital Subscriber Line Access Multiplexers (DSLAMs) and supports up to four DSL pairs. The DSL pairs are bundled in groups and configured in the Cisco IOS CLI by using the dsl-group command. Use the mode command to choose the mode (ATM or EFM).

The NIM supports the following configuration:

- You can configure up to four DSL groups.
- You can configure auto mode on only one DSL group. For example, DSL group 0.
- In ATM Mode, you can configure the lines to use 2-wire, 4-wire (standard or enhanced), or m-pair.
- In EFM mode, you can configure a DSL group with any one of the lines in 2-wire non-bonding mode or with multiple lines in bonding mode.
- Depending on the mode (ATM or EFM), the corresponding interface (ATM or EFM) is automatically created.

Cisco VDSL examples

Configuration example for VDSL:

```
Device# config-transaction
Device(config)# controller VDSL 0/0/0
Device(config)# operating mode auto


Device# config-transaction
Device(config)# line-mode single-wire line 1


Device# config-transaction
Device(config)# line-mode bonding


Device# config-transaction
Device(config)# controller VDSL 0/0/0
Device(config-controller)# firmware phy filename flash:IDC_1.7.2.6_DFE_FW_BETA_120111A.pkg


Device# config-transaction
Device(config-controller)# sra


Device# config-transaction
Device(config-controller)# bitswap


Device# config-transaction
Device(config)# controller VDSL 0/0/0
Device(config-controller)# modem customUKAnnexM
```

```
Device# config-transaction
Device(config)# controller VDSL 0/0/0
Device(config-controller)# description to ISP 1


Device# config-transaction
Device(config)# controller VDSL 0/0/0
Device(config-controller)# diagnostics DELT


Device# config-transaction
Device(config)# controller VDSL 0/0/0
Device(config-controller)# training log filename bootflash:VDSLLOG.log



Device# config-transaction
Device(config)# controller VDSL 0/0/0
Device(config-controller)# sync mode ansi previous



Device# configure terminal
Device(config)# ptp clock ordinary domain 0
Device(config-ptp-clk)# clock-port slave slaveport
Device(config-ptp-port)# sync interval -4
Device(config-ptp-port)# end
```

The following example show the VDSL configuration:

```
Device(config)# show controllers vdSL 0/2/0
Controller VDSL 0/2/0 is UP

Daemon Status:          UP

                        XTU-R (DS)              XTU-C (US)
Chip Vendor ID:         'BDCM'                   'BDCM'
Chip Vendor Specific:   0x0000                   0xA39A
Chip Vendor Country:    0xB500                   0xB500
Modem Vendor ID:        'CSCO'                   'BDCM'
Modem Vendor Specific:  0x4602                   0x0000
Modem Vendor Country:   0xB500                   0xB500
Serial Number Near:     FGL2149956Y C1117-4P 16.7.20180
Serial Number Far:
Modem Version Near:     16.7.20180709:09395
Modem Version Far:      0xa39a

Modem Status:           TC Sync (Showtime!)
DSL Config Mode:        AUTO
Trained Mode:           G.993.2 (VDSL2) Profile 17a

TC Mode:                PTM
Selftest Result:        0x00
DELT configuration:     disabled
DELT state:             not running

Failed full inits:      0
Short inits:            0
Failed short inits:     0

Modem FW  Version:      4.14L.04
Modem PHY Version:      A2pv6F039t.d26d

Line 0:
```

```
                      XTU-R (DS)              XTU-C (US)
Trellis:               ON                      ON
SRA:                   enabled                 enabled
SRA count:             0                       0
Bit swap:              enabled                 enabled
Bit swap count:        1                       3
Line Attenuation:      18.4 dB                  0.0 dB
Signal Attenuation:     0.0 dB                  0.0 dB
Noise Margin:           5.2 dB                 6.0 dB
Attainable Rate:       46022 kbits/s           18866 kbits/s
Actual Power:          14.5 dBm                10.4 dBm
Per Band Status:       D1      D2      D3      U0      U1      U2      U3
Line Attenuation(dB):  13.9    32.7    50.1    N/A     25.6    37.7    42.3
Signal Attenuation(dB): 13.5   32.4    N/A     N/A     25.0    36.9    41.9
Noise Margin(dB):      5.3     5.1     N/A     N/A     6.0     6.0     5.9
Total FECC:            446                     0
Total ES:              3                       0
Total SES:             0                       0
Total LOSS:            0                       0
Total UAS:             50                      50
Total LPRS:            0                       0
Total LOFS:            0                       0
Total LOLS:            0                       0


                 DS Channel1     DS Channel0   US Channel1       US Channel0
Speed (kbps):             NA           47610            NA             18859
SRA Previous Speed:       NA               0            NA                 0
Previous Speed:           NA               0            NA                 0
Reed-Solomon EC:          NA             446            NA                 0
CRC Errors:               NA              51            NA                 0
Header Errors:            NA            3935            NA                 0
Interleave (ms):          NA            1.00            NA              1.00
Actual INP:               NA            0.00            NA              0.00

Training Log :  Stopped
Training Log Filename : flash:vdsllog.bin
```

Cisco GSHDSL examples

Configuration example for GSHDSL:

```
Device# config-transaction
Device(config)# controller SHDSL 0/0/0
Device(config-controller)# dsl-group auto


Device# config-transaction
Device(config)# controller VDSL 0/0/0
Device(config-controller)# firmware phy filename bootflash:IDC_1.1.1.0_DFE_1.1-1.8.1__001.pkg



Device# config-transaction
Device(config)# controller SHDSL 0/0/0
Device(config-controller)# dsl-group 0 pairs 0
Device(config-controller-dsl-group)# no shdsl annex
Device(config-controller-dsl-group)# no shdsl rate 5696


Device# config-transaction
Device(config)# controller SHDSL 0/0/0
```

```
Device(config-controller)# termination cpe
Device(config-controller)# dsl-group 0 pairs 0
(config-controller-dsl-group)# shdsl 4-wire mode enhanced


Device# config-transaction
Device(config)# controller SHDSL 0/0/0
Device(config-controller)# termination cpe
Device(config-controller)# dsl-group 0 pairs 0
config-controller-dsl-group)# ignore 30

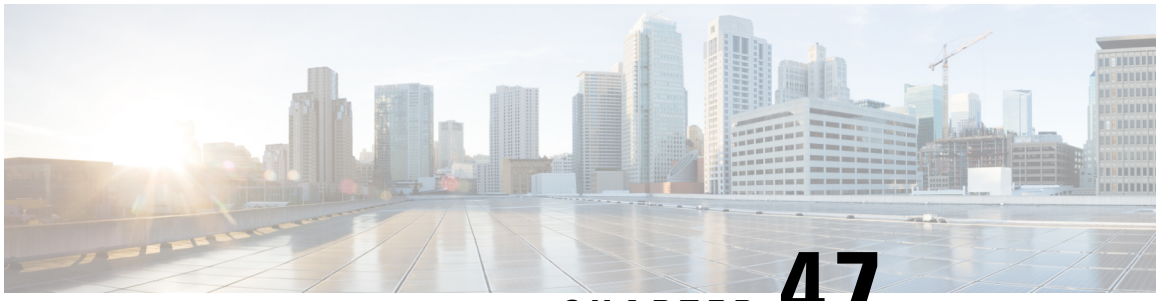

Device# config-transaction
Device(config)# controller SHDSL 0/0/0
Device(config-controller)# termination cpe
Device(config-controller)# dsl-group 0 pairs 0
config-controller-dsl-group)# shutdown
```

The following example show the GSHDSL configuration:

```
Device# show controllers shDSL 0/1/0
Controller SHDSL 0/1/0 is UP
  Hardware is NIM-SHDSL-EA, on slot 0,bay 0
  Capabilities: EFM: 2-wire, EFM-Bond, Annex A, B, F & G
                ATM: 2-wire, Mpair, Annex A, B, F & G
  CPE termination
  cdb=0x7F7EB723D8A8
  Vendor: Intel, Chipset: SOCRATES-4e
  PHY Source: System
  IDC Firmware version: 0.0.0.0
  DFE Firmware version:
  Group 0 info:
        Type: EFM Auto status: Down
         Ethernet Interface: Ethernet0/1/0, hwidb: 0x7F7EB723B648
         ATM Interface: ATM0/1/0, hwidb: 0x7F7EB724CE08
        Configured/active num links: 4/0, bit map: 0xF/0x0
        Line termination: CPE, Annex: auto
        PMMS disabled,Line coding: AUTO-TCPAM
        Configured/actual rate: AUTO/0 kbps
        Dying Gasp: Present
        SHDSL wire-pair (0) is in DSL DOWN state
                LOSWS Defect alarm: none
                SNR Margin alarm: none
                Loop Attenuation alarm: none
                Termination: CPE, Line mode: EFM Auto, Annex: auto
                Line coding: AUTO-TCPAM
                Configured/actual rate: AUTO/0 kbps
                Modem status: DOWN_NOT_READY,Condition: NO_COND_
        DSL Stats:
                Power Back Off: 0dB
                LoopAttn: 0dB, SnrMargin: 0dB
                Current 15 minute statistics (Time elapased 1 seconds)
                        ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
                Previous 15 minute statistics
                        ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
                Current 24 hr statistics
                        ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
                Previous 24 hr statistics
                        ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
        EFM Stats:
                EFM-TC Tx: data frames: 0
                EFM-TC Rx: data frames: 0
        SHDSL wire-pair (1) is in DSL DOWN state
                LOSWS Defect alarm: none
                SNR Margin alarm: none
```

```
        Loop Attenuation alarm: none
        Termination: CPE, Line mode: EFM Auto, Annex: auto
        Line coding: AUTO-TCPAM
        Configured/actual rate: AUTO/0 kbps
        Modem status: DOWN_NOT_READY,Condition: NO_COND_
    DSL Stats:
        Power Back Off: 0dB
        LoopAttn: 0dB, SnrMargin: 0dB
        Current 15 minute statistics (Time elapased 1 seconds)
            ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
        Previous 15 minute statistics
            ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
        Current 24 hr statistics
            ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
        Previous 24 hr statistics
            ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
    EFM Stats:
        EFM-TC Tx: data frames: 0
        EFM-TC Rx: data frames: 0
    SHDSL wire-pair (2) is in DSL DOWN state
        LOSWS Defect alarm: none
        SNR Margin alarm: none
        Loop Attenuation alarm: none
        Termination: CPE, Line mode: EFM Auto, Annex: auto
        Line coding: AUTO-TCPAM
        Configured/actual rate: AUTO/0 kbps
        Modem status: DOWN_NOT_READY,Condition: NO_COND_
    DSL Stats:
        Power Back Off: 0dB
        LoopAttn: 0dB, SnrMargin: 0dB
        Current 15 minute statistics (Time elapased 1 seconds)
            ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
        Previous 15 minute statistics
            ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
        Current 24 hr statistics
            ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
        Previous 24 hr statistics
            ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
    EFM Stats:
        EFM-TC Tx: data frames: 0
        EFM-TC Rx: data frames: 0
    SHDSL wire-pair (3) is in DSL DOWN state
        LOSWS Defect alarm: none
        SNR Margin alarm: none
        Loop Attenuation alarm: none
        Termination: CPE, Line mode: EFM Auto, Annex: auto
        Line coding: AUTO-TCPAM
        Configured/actual rate: AUTO/0 kbps
        Modem status: DOWN_NOT_READY,Condition: NO_COND_
    DSL Stats:
        Power Back Off: 0dB
        LoopAttn: 0dB, SnrMargin: 0dB
        Current 15 minute statistics (Time elapased 1 seconds)
            ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
        Previous 15 minute statistics
            ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
        Current 24 hr statistics
            ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
        Previous 24 hr statistics
            ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
    EFM Stats:
        EFM-TC Tx: data frames: 0
        EFM-TC Rx: data frames: 0
Group 1 is not configured
```

```
Group 2 is not configured
Group 3 is not configured
```



CHAPTER 47

Network Slicing

- Feature history of network slicing, on page 767
- Network slicing, on page 767
- Configure network slicing, on page 768
- Verify network slicing using CLI, on page 771

Feature history of network slicing

Table 293: Feature History

Feature Name	Release Information	Description
Cellular Network Slicing	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	This feature allows multiple networks to exist on the same physical network to optimize the network for different traffic types.

Network slicing

Network slicing is a network architecture solution that:

- partitions a single physical network into multiple virtual slices
- allows each slice to operate with customized network functions and resources
- allocates dedicated resources for diverse service types or customer requirements.

5G network slicing is supported only on 5G standalone networks. It is not available on 5G non-standalone (NSA) networks. The network provider defines a specific set of network functions and resources for each slice or service type. Service type defines the expected behavior of a network slice, specifying its features and services.

The following service types are supported in network slicing:

- Enhanced Mobile Broadband (eMBB): used for high-bandwidth and low-latency applications.

- Ultra-reliable low latency communications (URLLC): used for highly reliable and low-latency transmission requirements.
- Massive Internet of Things (MIoT): used for sending small quantities of data.

Configure network slicing

Before you begin

Create a configuration group for Cisco Catalyst Cellular Gateways using **Workflows** > **Create Cellular Gateway Group**. On the **Configuration Groups** page, the resulting configuration group is labelled cellular gateway in the **Device Solution** column.

For information about creating configuration groups and applying them to devices, see the Using Configuration Groups section of *Cisco Catalyst SD-WAN Configuration Groups, Cisco IOS XE Catalyst SD-WAN Release 17.x*.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create a Configuration Group. A new configuration group is created.

Step 3 In the configuration group, click **Add Profile**.

Step 4 Choose **Transport & Management Profile** from the drop-down list.

Step 5 Click **Edit** to add features to the Transport and Management profile and click **Add New Feature**.

Step 6 Choose **Cellular Controller** from the **Add Feature** drop-down list.

Step 7 Choose **Cellular Profile** from the **Add Fetaure** drop-down list.

Table 294: Cellular Settings

Field	Description
Primary Slot	Choose a SIM slot to designate it as primary. Range: 0, 1 Default: 0
SIM SLOT 0 Cellular Profile	
Profile Id	Profile ID. You can click **Add** to add multiple profiles.
Access Point Name	Access point name, from your service provider.
Authentication Method	Authentication method (**none**, **pap**, **chap**, **pap_or_chap**) indicated by your service provider.
Username	Username for authentication, as indicated by your service provider.

Field	Description
Password	Password for authentication, as indicated by your service provider.
Packet Data Network Type	Packet data network type (**IPv4**, **IPv6**, **IPv4v6**), as indicated by your service provider.
Attach Profile	Choose a attach profile from the defined profiles.
Data Profile	Choose a data profile from the defined profiles. You can use the same profile for the attach profile and data profile.
SIM SLOT 1 Cellular Profile	
See the fields described for SIM slot 0.	

Step 8 For the configured **Cellular Controller**, choose the **Cellular Profile** or click **Add New** to add a new cellular profile.

Step 9 Configure **Cellular Profile** using the following table.

Table 295: Cellular Profile Settings

Field	Description
Type	Choose a feature from the drop-down list.
Feature Name	Enter a name for the feature. The name can be up to 128 characters and can contain only alphanumeric characters.
Description	Enter a description of the feature. The description can be up to 2048 characters and can contain only alphanumeric characters.
Profile ID	Enter the identification number of the profile to use on the router. Range: 1 through 15
Access Point Name	Enter the name of the gateway between the service provider network and the public internet. It can be up to 32 characters long.
Authentication	Choose the authentication method used for the connection to the cellular network. It can be **none**, **pap**, **chap**, or **pap_chap**.
Profile Username	Enter the user name to use when making cellular connections for web services. It can be 1 to 32 characters. It can contain any alphanumeric characters, including spaces.
Profile Password	Enter the user password to use when making cellular connections for web services. The password is case-sensitive and can be clear text, or an AES-encrypted key. From Cisco Catalyst SD-WAN Manager Release 20.15.1, when you enter the password as clear text, Cisco SD-WAN Manager encrypts the password. When you view the configuration preview, the password appears in its encrypted form.
Packet Data Network Type	Choose the packet data network (PDN) type of the cellular network. It can be IPv4, IPv6, or IPv4v6.

Field	Description
No Overwrite	Enable this option to overwrite the profile on the cellular modem. By default, this option is disabled.
Slice Type	Choose the network slice type (SST) for the profile. The options are: • eMBB: Enhanced Mobile Broadband, used for high data throughput. • URLLC: Ultra-Reliable Low Latency Communication, used for high reliability and low latency transmission. • MIoT: Massive IoT, used for many devices transmitting small quantities of data.
Slice Differentiator	Enter the slice differentiator (SD) for the profile. This is an optional value that enables the user equipment (UE) to use multiple slice instances of the same SST. Range: 0 through 16777214
Slot	Enter the associated SIM slot for the profile.

Configure network slicing using CLI

The following example shows how to configure a cellular network slicing using a CLI:

```
Device(config-controller)# profile id 3 apn apn-ns authentication none pdn-type ipv4
   no-overwrite
   slot            Associated sim slot
   slice-type Associated network slice type(SST)

Device(config-controller)# profile id 3 apn apn-ns authentication none pdn-type ipv4 slice-
 type
<1-3>  Slice type number: 1(eMBB), 2(URLLC), 3(MioT)
Device(config-controller)# profile id 3 apn apn-ns authentication none pdn-type ipv4 slice-
 type embb
   slice-differentiator Associated Slice Differentiator(SD)  <--- if SD is bypassed here,"FF
 FF FF" wll be used internally as the SD to indicate that there is no SD associated with
this SST.
   slot                            Associated sim slot

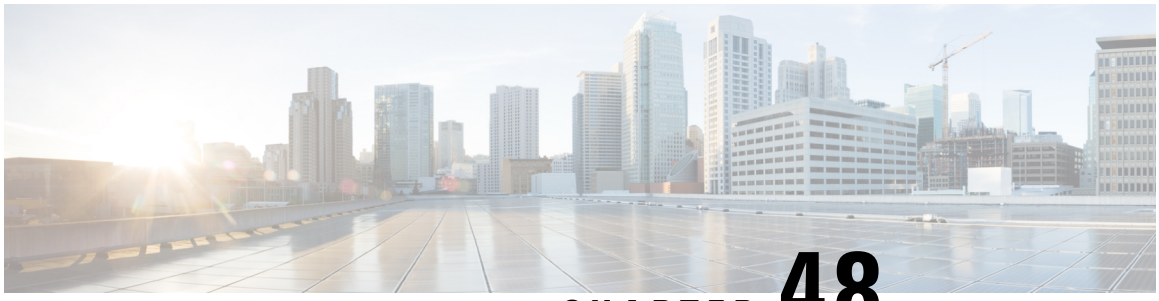
Device(config-controller)# profile id 3 apn apn-ns authentication none pdn-type ipv4 slice
 type
embb slice-differentiator
  <0-16777214>  Slice Differentiator
Device(config-controller)#
Device(config-controller)#$ pdn ipv6  slice-type miot slice-differentiator 6
  slot  Associated sim slot
```

Verify network slicing using CLI

The following is a sample output from the **show cellular** command that displays network slicing configuration and slice type details:

```
Device# show cellular profile 6

Profile 6 = INACTIVE
--------
PDP Type = IPv6
Access Point Name (APN) = TestNSSAI6_URLLC1
Authentication = None
S-NSSAI Slice Type is URLLC
S-NSSAI Slice Differentiator = 1
```



CHAPTER 48

Carrier Supporting Carrier

- Feature history for carrier supporting carrier, on page 773
- Carrier supporting carrier, on page 774
- Traffic flow configuration between CSC-CE and CSC-PE devices, on page 774
- Edge device functioning as a CSC-CE device, on page 775
- Use cases for carrier supporting carrier, on page 776
- Configure carrier supporting carrier, on page 776
- Verify device configuration for carrier supporting carrier, on page 779

Feature history for carrier supporting carrier

Table 296: Feature history

Feature name	Release information	Description
Cisco Catalyst SD-WAN Support for Carrier Supporting Carrier Connectivity	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	The feature adds support for carrier supporting carrier (CSC) connectivity on Cisco IOS XE Catalyst SD-WAN devices. CSC enables you to interconnect IP or multiprotocol label switching (MPLS) networks operating at different sites over an MPLS backbone network. Using CSC requires an edge router that supports CSC functionality, called a carrier edge (CE) device, at each site. This feature enables a Cisco IOS XE Catalyst SD-WAN device to serve as a CE device, making it unnecessary to have a separate dedicated CE device at each site managed by Cisco Catalyst SD-WAN.

Carrier supporting carrier

A carrier supporting carrier (CSC) is a hierarchical VPN model that

- allows organizations to interconnect their IP or MPLS networks located at different sites,
- operates over an MPLS backbone network, and
- eliminates the need for organizations to build and maintain their own MPLS backbone.

Components of carrier supporting carrier

- Backbone carrier: The service provider operates the backbone network. Typically, the backbone carrier network employs multiple segments to segregate the traffic of different customer carriers that share it. The same organization as the customer carriers or a different organization manages the backbone carrier.
- Customer carrier: An organization that uses the backbone network to route traffic from one site to another. The customer carrier may be part of the organization that operates the backbone network, or may be independent.
- CSC-CE: The customer edge (CE) device operates within a local site network and connects the site to the backbone carrier using an MPLS connection. It uses the backbone carrier to connect to other sites.
- CSC-PE: The provider edge (PE) device operates within the backbone carrier network and connects to CSC-CE devices at customer sites using an MPLS connection.

Benefits of carrier supporting carrier

A Cisco IOS XE Catalyst SD-WAN device functions as an customer edge device at a site requiring CSC, eliminating the need for a separate CE router.

Traffic flow configuration between CSC-CE and CSC-PE devices

The traffic flow configuration between CSC-CE and CSC-PE devices determines how service VPN, control, and BFD probe traffic is routed based on available MPLS and internet connections. This configuration optimizes network resources, ensures efficient traffic handling, and supports high availability in service provider networks.

Traffic flow

When a CSC-CE device has only an MPLS connection to its neighboring CSC-PE device, it sends all traffic, including service VPN traffic, control traffic, and Cisco Catalyst SD-WAN bidirectional forwarding detection (BFD) probe traffic, over the MPLS connection.

When a CSC-CE device has both an MPLS connection to the neighboring CSC-PE device and a separate internet connection, it routes traffic as follows:

- Based on the configured traffic policy, it can send control traffic and BFD probe traffic over either the internet or the MPLS connection.
- It sends service VPN traffic exclusively over the MPLS connection.

Label switching

When traffic uses an MPLS connection between a CSC device and the backbone carrier, the backbone carrier manages the traffic through label-switched paths and does not store any information about the customer carrier routes.

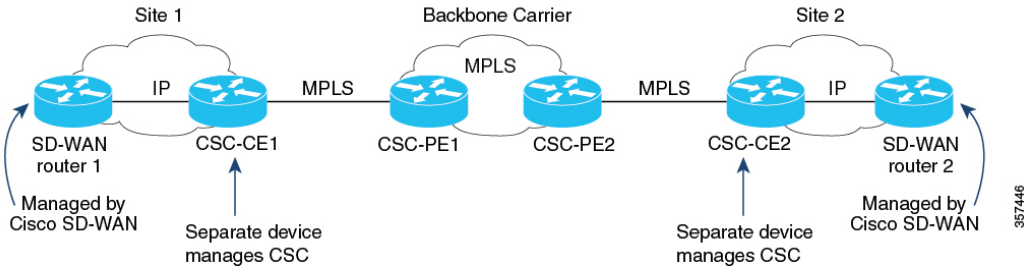
Edge device functioning as a CSC-CE device

The Cisco IOS XE Catalyst SD-WAN software simplifies carrier supporting carrier network topologies by enabling a single device to perform both SD-WAN edge and CSC-CE functions.

Before Cisco IOS XE Catalyst SD-WAN Release 17.6.1a

In releases earlier than 17.6.1a, each site in a CSC network topology used two separate devices: an edge device managed by Cisco Catalyst SD-WAN and a dedicated CSC-CE device. This is because the Cisco IOS XE Catalyst SD-WAN device could not function as a CSC-CE. See the illustration for the CSC topology before Cisco IOS XE Catalyst SD-WAN Release 17.6.1a.

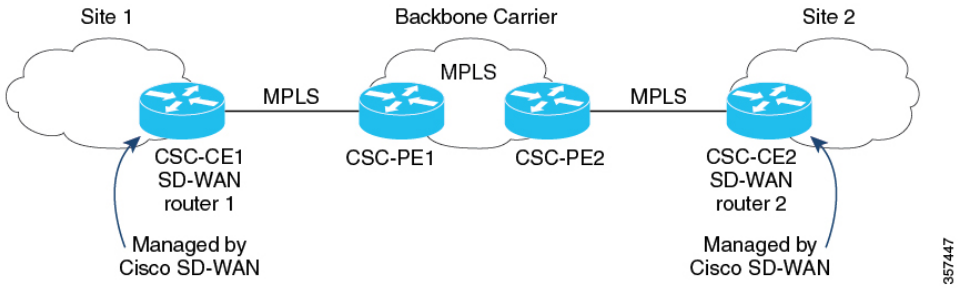
Figure 4: Carrier supporting carrier with Cisco Catalyst SD-WAN, before Cisco IOS XE Catalyst SD-WAN Release 17.6.1a



From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a

From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, a Cisco IOS XE Catalyst SD-WAN device can function as a CSC-CE, removing the need for a separate dedicated CSC-CE device. See the illustration for the simplified CSC topology with Cisco IOS XE Catalyst SD-WAN devices providing CSC-CE functionality.

Figure 5: Carrier supporting carrier with Cisco Catalyst SD-WAN, Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and later



Use cases for carrier supporting carrier

Carrier Supporting Carrier (CSC) enables secure, private transport of multiple customer networks over a shared backbone.

Global organizations

Global organizations can use Cisco Catalyst SD-WAN to support CSC with a backbone carrier, enabling multiple, separate divisions of an organization to maintain private traffic while sharing a common backbone carrier.

Service providers

Service providers that implement a CSC topology can benefit from Cisco Catalyst SD-WAN, as it allows carrier edge devices to handle CSC functionality without requiring a separate device.

Configure carrier supporting carrier

Use one of these methods to configure carrier supporting carrier.

- Feature template
- CLI commands

Configure carrier supporting carrier using a feature template

Follow these steps to configure a CE device for CSC using a new feature template in Cisco SD-WAN Manager.

Procedure

Step 1 Create a new device template.

a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

b. Choose **Device Templates**, and click **Create Template**.

c. From the drop-down list, select **From Feature Template**.

Note
In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled as **Device**.

Step 2 Enter device details.

- In the **Device Model** field, choose the correct device model.
- In the **Device Role** field, select **SDWAN Edge**.
- In the **Template Name** field, enter a name for the template.

Step 3 Configure VPN settings.

a. In the **Transport & Management VPN** section, under **Cisco VPN 0,** choose a template to configure VPN 0.

For more, see Configure Interfaces in the WAN Transport VPN (VPN 0).

b. In the **Cisco VPN Interface Ethernet** field, choose a template to configure the interface.

For more information, see Configure VPN Ethernet Interface.

Step 4 In the **Transport & Management VPN** section, click **Cisco BGP** to add the Cisco BGP field.

For more information, see see Configure BGP Using SD-WAN Manager Templates.

Step 5 In the **MPLS Interface** section, under **Interface Name 1**, enter the interface used to connect the device to the backbone carrier.

Step 6 In the **Neighbor** section, click **Advanced Options** to configure CSC options.

Table 297: Configure CSC options

Field	Description
Send label	Choose **On** to enable CSC support.
Explicit null	Choose **On** if the device uses a loopback WAN interface.
As override	Choose **On** if CE1 and CE2 use the same autonomous system (AS) number.
Allowas in	Choose **On** if the two CE sites use the same AS number.

Step 7 Click **Save** to save the BGP configuration.

Step 8 Click **Create** to create the feature template.

The **Configuration** > **Templates** page displays the available templates.

Step 9 Attach the template to a device.

a. On the **Configuration** > **Templates** page, click **Device Templates**.

b. For the new template, click **…** and choose **Attach Devices**.

c. Move a device to the **Selected Devices** column and click **Attach**.

Configure carrier supporting carrier using CLI

You can use the BGP feature template to configure CSC instead of CLI commands.

Before you begin

Apply a BGP configuration to a Cisco IOS XE Catalyst SD-WAN device before you configure it for CSC-CE functionality.

Follow these steps to configure a CE device for CSC using the CLI.

Procedure

Step 1 Configure CSC-CE1

a) Map MPLS labels to VRFs.

The device checks the MPLS label of incoming traffic and uses the IP lookup table of the VRF mapped to that label.For example, if the MPLS label 10 maps to VRF 1, the router uses the IP lookup table of VRF 1 for traffic with label 10.

```
device# config-transaction
device(config)# mpls label mode all-vrfs protocol bgp-vpnv4 per-vrf
device(config)# mpls label mode all-vrfs protocol bgp-vpnv6 per-vrf
device(config)# mpls label range min-label max-label static min-static-label max-static-label
```

b) Enable MPLS on the interface.

```
device(config)# interfaceinterface
device(config-if)# mpls bgp forwarding
```

c) Configure BGP.

```
device(config)# router bgp bgp-number
device(config-router)# neighbor neighbor-ip> allowas-in
```

d) Advertise MPLS labels when using a loopback WAN interface.

```
device(config-router)# neighbor <neighbor-ip> send-label explicit-null
```

Note
Using `send-label explicit-null` on non-loopback interfaces does not affect performance.

Step 2 Configure CSC-CE2

a. Map MPLS labels to VRFs.

```
device# config-transaction
device(config)# mpls label mode all-vrfs protocol bgp-vpnv4 per-vrf
device(config)# mpls label mode all-vrfs protocol bgp-vpnv6 per-vrf
device(config)# mpls label range min-label max-label static min-static-label max-static-label
```

b. Enable MPLS on the interface.

```
device(config)# interface interface
device(config-if)# mpls bgp forwarding
```

c. Configure BGP.

```
evice(config)# router bgp bgp-number
Device(config-router)# neighbor neighbor-ip as-override
Device(config-router)# neighbor neighbor-ip send-label explicit-null
```

The following example shows CSC-CE1 and CSC-CE2 configurations with BGP and MPLS:

- CSC-CE1: 10.1.1.10
- CSC-CE2: 10.1.1.20

- CSC-PE1 (neighbor of CSC-CE1): 10.2.2.10
- CSC-PE2 (neighbor of CSC-CE2): 10.2.2.20

CSC-CE1 Configuration

```
mpls label mode all-vrfs protocol bgp-vpnv4 per-vrf
mpls label mode all-vrfs protocol bgp-vpnv6 per-vrf
mpls label range 100000 1048575 static 16 99

interface GigabitEthernet2
 no shutdown
 mpls bgp forwarding
 ip address 10.1.1.15 255.255.255.0

router bgp 10
 bgp log-neighbor-changes
 bgp router-id 172.16.255.15
 neighbor 10.1.1.20 remote-as 100
 neighbor 10.1.1.20 fall-over bfd
 address-family ipv4 unicast
  maximum-paths 4
  neighbor 10.1.1.20 activate
  neighbor 10.1.1.20 advertisement-interval 30
  neighbor 10.2.2.10 allowas-in
  neighbor 10.2.2.10 send-label explicit-null
  neighbor 10.1.1.20 send-community both
 exit-address-family
 timers bgp 60 180
```

CSC-CE2 Configuration

```
mpls label mode all-vrfs protocol bgp-vpnv4 per-vrf
mpls label mode all-vrfs protocol bgp-vpnv6 per-vrf
mpls label range 100000 1048575 static 16 99

interface GigabitEthernet5
 ip address 10.0.6.11 255.255.255.0
 negotiation auto
 mpls bgp forwarding

router bgp 10
 bgp log-neighbor-changes
 bgp router-id 172.16.255.11
 neighbor 10.1.1.10 remote-as 200
 address-family ipv4 unicast
  neighbor 10.1.1.10 activate
  neighbor 10.1.1.10 advertisement-interval 30
  neighbor 10.2.2.20 as-override
  neighbor 10.2.2.20 send-label explicit-null
  network 10.0.7.0 mask 255.255.255.0
  redistribute connected
  redistribute static
 exit-address-family
```

Verify device configuration for carrier supporting carrier

To verify if a device is correctly configured to reach the remote CSC-CE device using MPLS-labeled routing.

Procedure

Step 1 Run the following command on the device:

Example:

```
show ip route remote-csc-ce-device-address
```

Step 2 Confirm if the output displays a routing entry for the remote site IP address.

Step 3 Check if the output includes one or more routing descriptor blocks that describe the next-hop addresses for the path to the remote CSC-CE device.

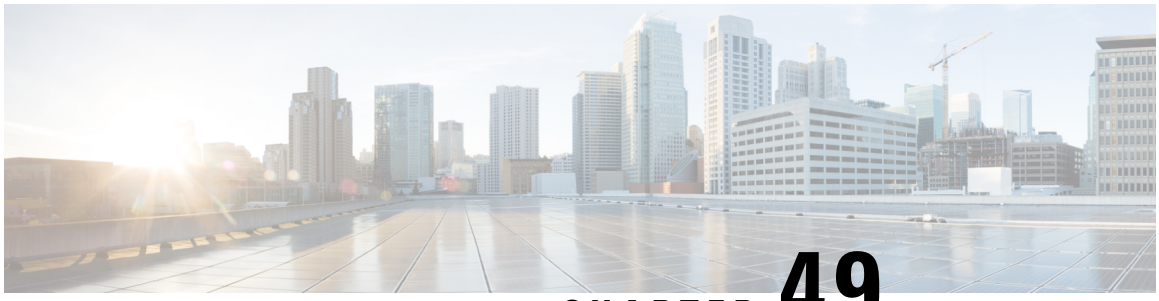
Step 4 Ensure that each descriptor block contains an MPLS label.

- If the device is configured correctly, the output shows:

```
Device# show ip route 10.0.1.100
Routing entry for 10.0.1.0/24
...
Routing Descriptor Blocks:
* 10.1.1.100, from 10.1.1.100, 00:00:50 ago
...
MPLS label: 26
```

- If the device is not configured correctly, the output shows:

```
% Subnet not in table
```



CHAPTER 49

TCP MSS and Clear Dont Fragment

- Feature history for TCP MSS and clear dont fragment, on page 781
- TCP MSS, on page 781
- Restrictions for TCP MSS and clear dont fragment, on page 782
- Configure TCP MSS and clear dont fragment, on page 782
- Verify TCP MSS and dont clear fragment configurations, on page 784

Feature history for TCP MSS and clear dont fragment

Table 298: Feature History

Feature Name	Release Information	Description
Configure TCP MSS	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature adds support for TCP MSS adjustment on Cisco IOS XE Catalyst SD-WAN devices on both directions of the Cisco Catalyst SD-WAN tunnel interface.
Configure Clear Don’t Fragment Option	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature provides the option to clear the Don't Fragment bit in the IPv4 packet header for packets being sent out on a Cisco Catalyst SD-WAN tunnel . When you clear the Don't Fragment configuration, packets larger than the interface MTU are fragmented before being sent.

TCP MSS

A TCP maximum segment size (MSS) is a parameter that

- specifies the largest amount of data, in bytes, that a communications device can receive in a single TCP segment without counting the TCP header or the IP header, and

- is specified as TCP MSS, initially in the TCP SYN packet during the TCP handshake.

TCP MSS for SYN packets

Small MSS values reduce or eliminate IP fragmentation, which results in higher overhead. You can configure the MSS of TCP SYN packets passing through a device. By default, the device dynamically adjusts the MSS based on the interface or tunnel maximum transmission unit (MTU) to ensure that TCP SYN packets are never fragmented. For data sent over an interface, the device calculates the MSS by adding the interface MTU, the IP header length, and the maximum TCP header length.

Restrictions for TCP MSS and clear dont fragment

TCP MSS

- TCP MSS values can be adjusted for Cisco Catalyst SD-WAN tunnel interfaces only.

  From Cisco IOS XE Catalyst SD-WAN Release 17.9.1aand Cisco vManage Release 20.9.1, you can adjust the TCP MSS value for a service VPN or for Network Address Translation (NAT) Direct Internet Access (DIA) use cases. Adjusting the TCP MSS value helps prevent TCP sessions from being dropped.

  For more information on NAT DIA, see the *Cisco Catalyst SD-WAN NAT Configuration Guide*.

- From Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, for an IPv4 SD-WAN tunnel carrying IPv6 traffic, the system uses the IPv6 TCP MSS value. Also, for an IPv6 tunnel carrying IPv4 traffic, the system uses the IPv4 TCP MSS value. This upgrade aligns MSS adjustment with the traffic protocol and tunnel configurations, ensuring accurate and efficient handling of traffic.

Clear dont fragment

- The option **Clear Dont Fragment** is available for Cisco Catalyst SD-WAN tunnel interfaces only.

Configure TCP MSS and clear dont fragment

Use one of these methods to configure TCP MSS and clear dont fragment:

- CLI commands
- Templates

Configure TCP MSS and clear dont fragment using CLI commands

Follow these steps to configure TCP MSS and clear dont fragment using CLI commands:

Procedure

Step 1 Configure an interface type and enter the interface configuration mode.

Example:

```
interface Tunnel 1
```

Step 2 Enable IP processing on an interface without assigning an explicit IP address to the interface.

Example:

```
ip unnumbered GigabitEthernet1
```

Step 3 Configure TCP MSS and clear dont fragment.

- Enable a maximum segment size (MSS) for TCP connections.

Example:

```
ip tcp adjust-mss 1460
```

- Clear the Don't Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface.

Example:

```
ip clear-dont-fragment
```

The following is an example configuration of TCP MSS:

```
Device(config)#interface Tunnel 1
Device(config-if)#ip unnumbered GigabitEthernet1
Device(config-if)#ip tcp adjust-mss 1460
```

The following is an example to configure Clear Dont Fragment option:

```
Device(config)#interface Tunnel 1
Device(config-if)#ip unnumbered GigabitEthernet1
Device(config-if)#ip clear-dont-fragment
```

Configure TCP MSS and clear dont fragment using templates

Follow these steps to configure TCP MSS and clear dont fragment using feature templates.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**.

Note
In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is titled **Feature**.

Step 3 Create a new CLI add-on feature template or edit one of the following templates. You can use any of the following feature templates to configure TCP MSS and clear dont fragment:

- VPN Ethernet Interface
- VPN Interface DSL IPoE
- VPN Interface DSL PPoA

- VPN Interface DSL PPPoE
- VPN Interface Multilink
- VPN Interface T1/E1
- Cellular Interfaces

Step 4 Click **Tunnel**.

Step 5 Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device to configure TCP MSS in the tunnel TCP MSS. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU so that TCP SYN packets are not fragmented.

- Range: 552 to 1460 bytes
- Default: None

TCP MSS affects any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS is examined against the MSS exchanged in the three-way handshake. The MSS in the header is lowered if the configured setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, it flows through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. If the TCP MSS is to be configured, it should be set at 40 bytes lower than the minimum path MTU.

Step 6 Click the **Clear-Dont-Fragment** option to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out the interface. When the **Don't Fragment** bit is cleared, packets larger than that interface's MTU are fragmented before being sent.

Clear-Dont-Fragment clears the **Don't Fragment** bit when there is fragmentation needed and the **Don't Fragment** bit is set. For packets that don't require fragmentation, the **Don't Fragment** bit is not affected.

Step 7 Click **Save** or **Update**.

Verify TCP MSS and dont clear fragment configurations

TCP MSS configuration

The following is sample output of the **show platform hardware qfp active feature sdwan datapath session summary** command:

```
Device# show platform hardware qfp active feature sdwan datapath session summary

Src IP          Dst IP          Src Port Dst Port   Encap    Uidb     Bfd Discrim PMTU

------          ------          -------- -------    ------   -------  ----------- -----

10.1.15.25      10.1.14.14      12347    12346      IPSEC    65526    10007       1446

10.1.15.25      10.0.5.21       12347    12357      IPSEC    65526    10009       1446

10.1.15.25      10.0.5.11       12347    12347      IPSEC    65526    10008       1446

10.1.15.25      10.1.16.16      12347    12366      IPSEC    65526    10006       1446
```

Dont fragment configuration

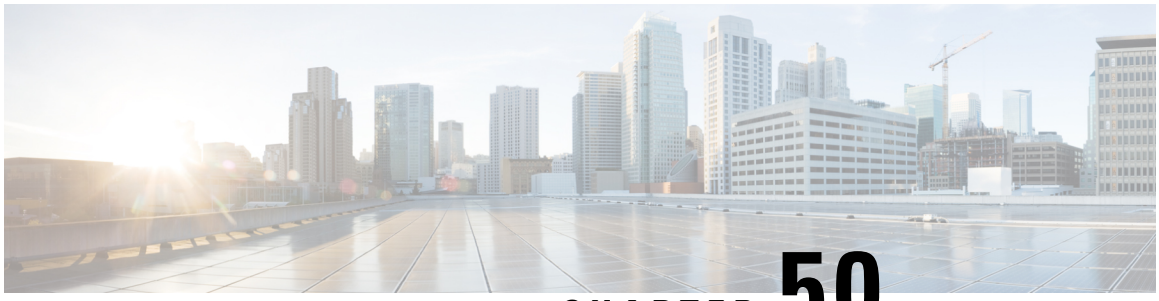
The following is sample output of the **show platform software interface rp active name Tunnel1** command to verify if **Clear-dont-fragment** is enabled or not.

```
Device# show platform software interface rp active name Tunnel1 | include dont
IP Clear-dont-fragment: TRUE
```

The following is sample output of the **show running-config interface Tunnel1** command that displays the running configuration when Clear-dont-fragment is enabled.

```
Device# show running-config interface Tunnel1
Building configuration...

Current configuration : 132 bytes
!
interface Tunnel1
ip unnumbered GigabitEthernet1
ip clear-dont-fragment
tunnel source GigabitEthernet1
tunnel mode sdwan
end
```



CHAPTER 50

Hot Standby Router Protocol

- Feature history table for hot standby router protocol, on page 787
- Hot standby router protocol , on page 787
- Configure HSRP using the CLI , on page 790
- Verify hot standby router protocol , on page 793

Feature history table for hot standby router protocol

Table 299: Feature History

Feature Name	Release Information	Description
Support for HSRP and HSRP Authentication on Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	This feature allows you to configure HSRPv2 and HSRP authentication on Cisco IOS XE Catalyst SD-WAN platforms via CLI template. HSRP is a long-standing Cisco proprietary First Hop Redundancy Protocol (FHRP) to support version 2 of the protocol and authentication.

Hot standby router protocol

Hot Standby Router Protocol (HSRP) is a First Hop Redundancy Protocol (FHRP) that allows transparent failover of the first-hop IP device and provides high network availability. HSRP offers first-hop routing redundancy for IP hosts on networks configured with a default-gateway IP address. It identifies active and standby devices, supports multiple groups for load sharing, and uses virtual addresses for gateway redundancy. HSRP includes version 2 enhancements for stability and management, provides MD5 authentication for security, and enables dynamic-priority changes through object tracking.

HSRP version 2 support

Following are the HSRP version 2 (HSRPv2) features:

- HSRPv2 advertises and learns millisecond timer values. This change ensures stability of the HSRP groups in all cases.
- HSRPv2 expands the group number range from 0 to 4095.
- HSRPv2 provides improved management and troubleshooting. The HSRPv2 packet format includes a 6-byte identifier. This field is typically populated with the interface MAC address.
- HSRPv2 uses the IP multicast address 224.0.0.102 to send hello packets. This multicast address allows Cisco Group Management Protocol (CGMP) leave processing to be enabled concurrently with HSRP.
- HSRPv2 has a different packet format that uses a type–length–value (TLV) format.

HSRP MD5 authentication

HSRP supports two authentication schemes for protocol packets: simple plain-text strings and Message Digest 5 (MD5). HSRP MD5 authentication is an advanced authentication method that generates a Message Digest 5 (MD5) digest for the HSRP portion of the multicast HSRP protocol packet. This functionality provides added security and protects against the threat from HSRP-spoofing software.

MD5 authentication provides greater security than plain text authentication. MD5 authentication allows each HSRP group member to use a secret key to generate a keyed MD5 hash, which is part of the outgoing packet. A keyed hash of an incoming packet is generated; if the hash in the incoming packet does not match the generated hash, the packet is ignored.

You can provide the MD5 hash key directly in the configuration using a key string or supply it indirectly through a key chain.

HSRP packets will be rejected if one or more of the following conditions occur:

- Authentication schemes differ on the device and in the incoming packets.
- MD5 digests differ on the device and in the incoming packets.
- Text authentication strings differ on the device and in the incoming packets.

HSRP object tracking

Object tracking separates the tracking mechanism from HSRP and creates a stand-alone tracking process. Other processes and HSRP can use this tracking process. The priority of a device can change dynamically when it has been configured for object tracking, and the object that is being tracked goes down. Examples of objects that can be tracked are the line protocol state of an interface or the reachability of an IP route. If the specified object goes down, the HSRP priority is reduced.

How HSRP topologies work

Summary

HSRP enables redundancy and reliability by allowing multiple routers to present as a single virtual gateway.

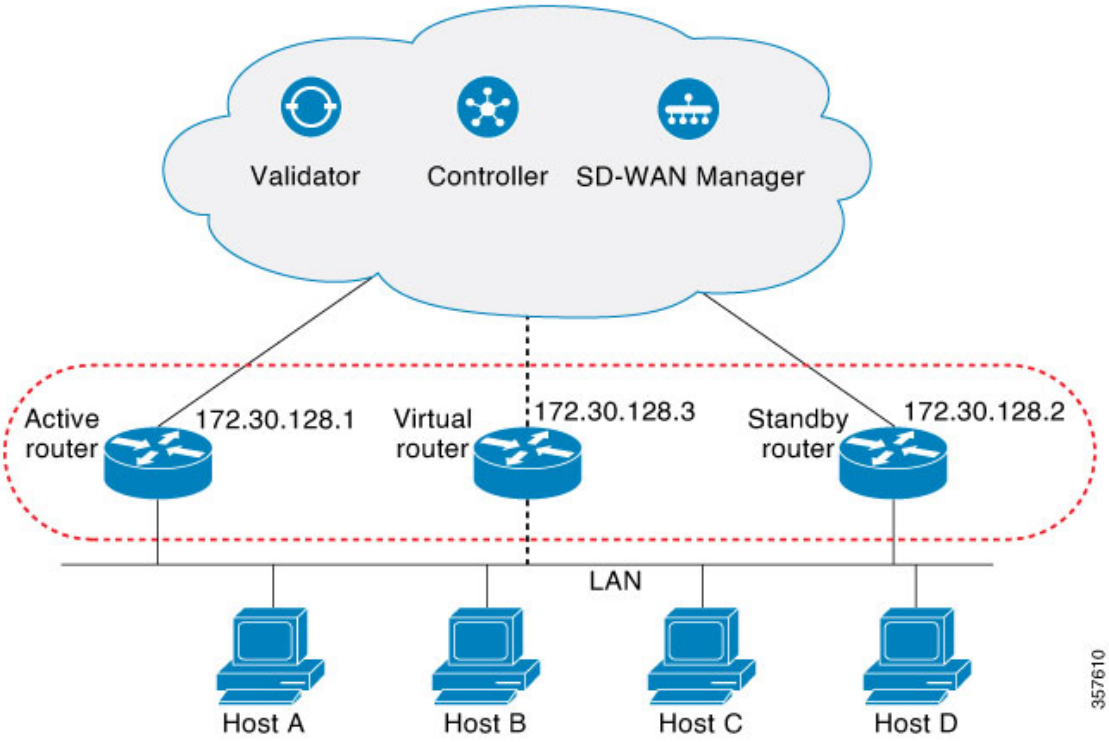
The key components involved in the process are:

- HSRP routers: Physical routers configured in a standby group.
- Virtual IP address: Shared address used by hosts as their default gateway.

- Virtual MAC address: Shared hardware address enabling failover.
- Hosts: End devices on the LAN that use the virtual gateway.

Workflow

Figure 6: HSRP Topology



The process involves the following stages:

1. The routers are configured into an HSRP standby group, sharing a virtual IP and MAC address.
2. One router assumes the active role, responding to traffic for the virtual IP.
3. Another router is in the standby role, monitoring the active router.
4. Hosts are configured with the virtual IP as their default gateway.
5. If the active router fails or does not send hello messages within a preset interval, the standby router becomes active and takes over packet forwarding.

Result

Hosts experience uninterrupted gateway service; redundancy is achieved, ensuring network reliability.

HSRP benefits

- Redundancy: HSRP employs a proven redundancy scheme and is widely deployed in large networks.

- Fast Failover: HSRP provides transparent, fast failover for the first-hop device.
- Preemption: Preemption allows a standby device to delay activation for a configurable time.
- Authentication: The HSRP Message Digest 5 (MD5) authentication algorithm safeguards against HSRP spoofing software and uses the MD5 standard to improve reliability and security.

Supported devices

- Cisco Catalyst 8500 Series Edge Platforms
- Cisco Catalyst 8300 Series Edge Platforms
- Cisco Catalyst 8200 Series Edge Platforms
- Cisco Catalyst 8200 uCPE Series Edge Platforms
- Cisco ASR 1000 Series Aggregation Services Routers
- Cisco ISR 1000 and ISR 4000 Series Integrated Services Routers (ISRs)
- Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers (ISRs)
- Cisco IR1101 Integrated Services Router Rugged
- Cisco Catalyst 8000v Series Cloud Services Router

For details on supported models for each of these device families, refer to Cisco Catalyst SD-WAN Device Compatibility page.

Configure HSRP using the CLI

Before you begin

You can configure HSRP using the Cisco SD-WAN Manager CLI Add-on feature templates and CLI device templates. For more information on configuring using CLI templates, see CLI Templates. The following commands can be used in any order.

Procedure

Step 1 Enable HSRP on the interface.

Create (or enable) the HSRP group in IPv4 using its number and virtual IP address:

```
Device(config)# interface interface-type
Device(config-if)# standby group-number ip [ip-address [secondary]]
```

Activate HSRP in IPv6:

```
Device(config)# interface interface-type
Device(config-if)# standby group-number ipv6 {link-local-address | autoconfig }
```

Step 2 Set the HSRP version.

Note that the **nostandby** or **nostandby version 2** commands are rejected when the interface has IPv6 groups.

```
Device(config)# interface interface-type
Device(config-if)# standby version {1|2}
```

Step 3 Configure group priority and preemption.

Set the priority value used in choosing the active router, and configure HSRP preemption and preemption delay:

```
Device(config)# interface interface-type
Device(config-if)# standby group-number ip [ip-address [secondary]]
Device(config-if)# standby group-number priority [priority]
Device(config-if)# standby group-number preempt [ delay{ [ minimum seconds] [ reload seconds] [ sync
 seconds]}]
```

Step 4 Enable HSRP authentication (MD5 or text authentication).

- Configure HSRP MD5 authentication using a key chain.

  Key chains allow a different key string to be used at different times according to the key chain configuration. HSRP queries the appropriate key chain to obtain the current live key and key ID for the specified key chain.

  ```
  Device(config)# interface interface-type
  Device(config-if)# ip address ip-address mask [secondary ]
  Device(config-if)# standby group-number priority [priority]
  Device(config-if)# standby group-number preempt [ delay{ [ minimum seconds] [ reload seconds] [
   sync seconds]}]
  Device(config-if)# standby group-number authentication md5 key-chain key-chain-name
  Device(config-if)# standby group-number ip [ip-address [secondary]]
  ```

- Configure HSRP text authentication.

  The authentication string can be up to eight characters in length; the default string is Cisco.

  ```
  Device(config)# interface interface-type
  Device(config-if)# ip address ip-address mask [secondary ]
  Device(config-if)# standby group-number priority [priority]
  Device(config-if)# standby group-number preempt [ delay{ [ minimum seconds] [ reload seconds] [
   sync seconds]}]
  Device(config-if)# standby group-number authentication text string
  Device(config-if)# standby group-number ip [ip-address [secondary]]
  ```

Step 5 Adjust HSRP timers.

Configure the time between the hello packets and the time before other routers declare the active router to be inactive:

```
Device(config)# interface interface-type
Device(config-if)# standby group-number ip [ip-address [secondary]]
Device(config-if)# standby group-number timers hellotime holdtime
```

Step 6 Adjust HSRP object tracking.

Configure HSRP to track an object and change the HSRP priority based on the state of the object:

```
Device(config)# interface interface-type
Device(config-if)# standby group-number track object-number [decrement priority-decrement] [shutdown]
```

Step 7 Optimize CPU and network performance with HSRP multiple group optimization.

- Configure an HSRP group as a client group:

  ```
  Device(config)# interface interface-type
  Device(config-if)# standby group-number follow group-name
  ```

- Configure the HSRP client group refresh interval:

```
Device(config)# interface interface-type
Device(config-if)# standby group-number mac-refresh seconds
```

Step 8 Configure a specific virtual MAC address.

Specify a virtual MAC address for HSRP:

```
Device(config)# interface interface-type
Device(config-if)# standby group-number mac-address mac-address
```

Step 9 Link IP redundancy clients to HSRP groups.

Configure the name of a standby group:

```
Device(config)# interface interface-type
Device(config-if)# standby group-number name [redundancy-name]
```

The configured interface participates as a member of the specified HSRP group and provides high-availability failover with other routers in the group.

Example

The following is a complete HSRP configuration example on Cisco IOS XE Catalyst SD-WAN devices through CLI:

```
config-transaction
!
    interface GigabitEthernet0/0/1.94
    encapsulation dot1Q 94
    vrf forwarding 509
    ip address 10.96.194.2 255.255.255.0
    ip directed-broadcast
    ip mtu 1500
    ip nbar protocol-discovery
    standby version 2
    standby 1 preempt
    standby 94 ip 10.96.194.1
    standby 94 timers 1 4
    standby 94 priority 110
    standby 94 preempt delay minimum 180
    standby 94 authentication md5 key-string 7 094F471A1A0A
    standby 94 track 8 shutdown
    standby 194 ipv6 2001:10:96:194::1/64
    standby 194 timers 1 4
    standby 194 priority 110
    standby 194 preempt delay minimum 180
    standby 194 authentication md5 key-string 7 094F471A1A0A
    standby 194 track 80 shutdown
    ip policy route-map clear-df
    ipv6 address 2001:10:96:194::2/64
    ipv6 mtu 1500
    arp timeout 1200
    end
```

What to do next

- Verify HSRP operation and monitor for proper failover behavior.
- Adjust settings based on observed performance as needed.

Verify hot standby router protocol

The following is a sample output from the **show standby** command displaying the standby router information:

```
Device# show standby
GigabitEthernet0/0/1.94 - Group 94 (version 2)
  State is Standby
    1 state change, last state change 01:06:09
    Track object 8 state Up
  Virtual IP address is 10.96.194.1
  Active virtual MAC address is 0000.0c9f.f05e (MAC Not In Use)
    Local virtual MAC address is 0000.0c9f.f05e (v2 default)
  Hello time 1 sec, hold time 4 sec
    Next hello sent in 0.688 secs
  Authentication MD5, key-string
  Preemption enabled, delay min 180 secs
  Active router is 10.96.194.2, priority 110 (expires in 4.272 sec)
    MAC address is cc16.7e8c.6dd1
  Standby router is local
  Priority 105 (configured 105)
  Group name is "hsrp-Gi0/0/1.94-94" (default)
  FLAGS: 0/1
GigabitEthernet0/0/1.94 - Group 194 (version 2)
  State is Standby
    1 state change, last state change 01:06:07
    Track object 80 state Up
  Link-Local Virtual IPv6 address is FE80::5:73FF:FEA0:C2 (impl auto EUI64)
    Virtual IPv6 address 2001:10:96:194::1/64
  Active virtual MAC address is 0005.73a0.00c2 (MAC Not In Use)
    Local virtual MAC address is 0005.73a0.00c2 (v2 IPv6 default)
  Hello time 1 sec, hold time 4 sec
    Next hello sent in 0.480 secs
  Authentication MD5, key-string
  Preemption enabled, delay min 180 secs
  Active router is FE80::CE16:7EFF:FE8C:6DD1, priority 110 (expires in 4.032 sec)
    MAC address is cc16.7e8c.6dd1
  Standby router is local
  Priority 105 (configured 105)
  Group name is "hsrp-Gi0/0/1.94-194" (default)
  FLAGS: 0/1
```

The following is a sample output from the **show standby** command displaying HSRP Version 2 information if HSRP Version 2 is configured:

```
Device# show standby
Ethernet0/1 - Group 1 (version 2)
  State is Speak
  Virtual IP address is 10.21.0.10
  Active virtual MAC address is unknown
   Local virtual MAC address is 0000.0c9f.f001 (v2 default)
  Hello time 3 sec, hold time 10 sec
   Next hello sent in 1.804 secs
  Preemption enabled
  Active router is unknown
  Standby router is unknown
  Priority 20 (configured 20)
  Group name is "hsrp-Et0/1-1" (default)
Ethernet0/2 - Group 1
  State is Speak
  Virtual IP address is 10.22.0.10
  Active virtual MAC address is unknown
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
```

```
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.804 secs
  Preemption disabled
  Active router is unknown
  Standby router is unknown
  Priority 90 (default 100)
    Track interface Serial2/0 state Down decrement 10
  Group name is "hsrp-Et0/2-1" (default)
```

The following is a sample output from the **show standby** command displaying HSRP authentication information if HSRP MD5 authentication is configured:

```
Device# show standby
Ethernet0/1 - Group 1
  State is Active
    5 state changes, last state change 00:17:27
  Virtual IP address is 10.21.0.10
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.276 secs
  Authentication MD5, key-string, timeout 30 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 110 (configured 110)
  Group name is "hsrp-Et0/1-1" (default)
```

The following is a sample output from the **show standby brief** command displaying HSRP information for a specific interface:

```
Device# show standby brief
Interface   Grp  Pri P State   Active                    Standby   Virtual IP
Gi0/0/1.94  94   105 P Standby 10.96.194.2                 local    10.96.194.1
Gi0/0/1.94  194  105 P Standby FE80::CE16:7EFF:FE8C:6DD1   local    FE80::5:73FF:FEA0:C2
```

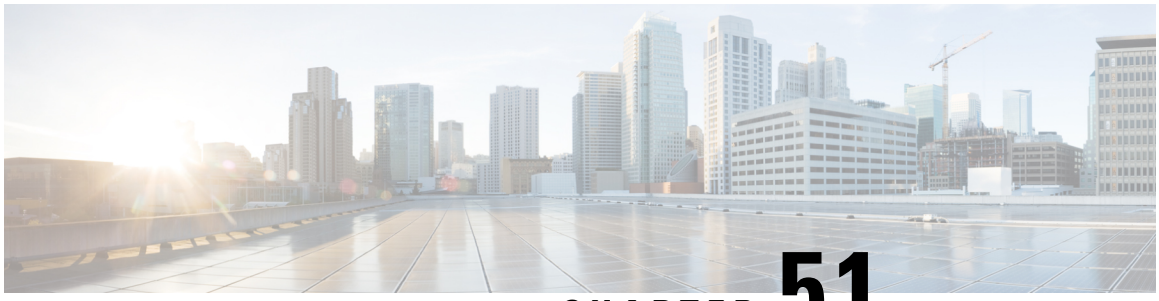
The following is a sample output from the **show standby neighbors** command displaying the HSRP neighbors on Ethernet interface 0/0. Neighbor 10.0.0.250 is active for group 2 and standby for groups 1 and 8, and is registered with BFD:

```
Device# show standby neighbors Ethernet0/0
HSRP neighbors on Ethernet0/0
  10.0.0.250
    Active groups: 2
    Standby groups: 1, 8
    BFD enabled
  10.0.0.251
    Active groups: 5, 8
    Standby groups: 2
    BFD enabled
  10.0.0.253
    No Active groups
    No Standby groups
    BFD enabled
```

The following is a sample output from the **show standby neighbors** command displaying information for all HSRP neighbors:

```
Device# show standby neighbors
HSRP neighbors on FastEthernet2/0
  10.0.0.2
    No active groups
    Standby groups: 1
    BFD enabled
```

```
HSRP neighbors on FastEthernet2/0
  10.0.0.1
    Active groups: 1
    No standby groups
    BFD enabled
```



CHAPTER 51

IP DHCP Smart-Relay

- Feature history for IP DHCP smart-relay, on page 797
- IP DHCP smart-relay, on page 797
- Benefits of IP DHCP smart-relay, on page 798
- Configure IP DHCP smart-relay agent using a CLI template, on page 798

Feature history for IP DHCP smart-relay

Table 300: Feature History Table

Feature Name	Release Information	Feature Description
IP DHCP Smart-Relay	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	With this feature, you can set the gateway address to the secondary IP address using the DHCP relay agent, when there is no IP address and DHCP service information from the DHCP server. A DHCP relay agent is any host or IP router that forwards DHCP packets between clients and servers. This functionality is useful when the DHCP server cannot be configured to use secondary pools.

IP DHCP smart-relay

A Dynamic Host Configuration Protocol (DHCP) relay agent is a network host that

- forwards DHCP packets between clients and servers on different physical subnets,
- generates new DHCP messages on another interface, setting the gateway IP address and optionally adding relay agent information (option 82), and
- supports unnumbered interfaces by automatically managing static host routes for DHCP clients.

Relay-agent forwarding differs from standard IP routing; instead of transparent packet switching, the relay agent receives DHCP messages, creates new messages with updated information, and forwards these between interfaces.

When a DHCP reply is received from the server, the relay agent removes option 82 (if present) before forwarding it to the client. With unnumbered interfaces, the relay agent borrows an IP address from another configured interface and dynamically adds or removes static host routes for DHCP clients as leases are assigned and released.

Supporting reference information

- DHCP relay agents are essential when DHCP clients and servers are not on the same subnet, as they enable message forwarding across networks.
- Relay agents specifically set the gateway IP address and can insert option 82 for added information in packets sent to the DHCP server.
- The Cisco IOS XE DHCP relay agent supports unnumbered interfaces, which helps conserve address space and network resources. Static host routes for DHCP clients on unnumbered interfaces are created and removed automatically based on the DHCP lease status.

Benefits of IP DHCP smart-relay

- Automatically assigning IP addresses at each remote site substantially reduces internet access costs. Purchasing static IP addresses is considerably more expensive than using automatically allocated IP addresses.
- Simplifies configuration, reduces operational overhead and costs related to device configuration, and makes deployment easier for nontechnical users.
- The DHCP server maintains configurations for several subnets, so an administrator needs to update only a single, central server when configuration parameters change.

Configure IP DHCP smart-relay agent using a CLI template

To forward UDP broadcasts to the DHCP server, configure helper addresses on the interface. If you have configured the secondary addresses on that interface and you want the router to step through each IP network when forwarding DHCP requests, use the `ip dhcp smart-relay` command.

If the smart relay agent forwarding is not configured, all requests are forwarded using only the primary IP address on the interface.

If the `ip dhcp smart-relay` command is configured, the relay agent counts the number of times that the client retries sending a request to the DHCP server when there is no DHCPOFFER message from the DHCP server. After three retries, the relay agent sets the gateway address to the secondary address. If the DHCP server still does not respond after three more retries, then the next secondary address is used as the gateway address.

For more information about using CLI templates, see *CLI Add-On Feature Templates* and *CLI Templates*.

Before you begin

- To configure the IP DHCP smart-relay feature, configure the IP helper address on desired interfaces using `ip helper-address` command. You can use the `service dhcp` command to enable the DHCP service or the `no service dhcp` command to disable it, depending on the requirement.
- The Cisco DHCP relay agent is enabled on an interface only when the `ip helper-address` command is configured. This command enables the DHCP broadcast to be forwarded to the configured DHCP server.

Procedure

Step 1 Enter SD-WAN configuration mode.

Example:

```
sdwan
```

Step 2 Enable DHCP server.

Example:

```
service dhcp
```

Step 3 In the SD-WAN configuration mode, configure an interface type such as **Gigabit Ethernet.**

Example:

```
interface Gigabitethernet0/0
```

Step 4 Enable the DHCP broadcast to be forwarded to the configured DHCP server.

Example:

```
 ip helper-address
```

Step 5 Configure the DHCP relay agent to switch the gateway address to a secondary address when there is no DHCPOFFER message from a DHCP server.

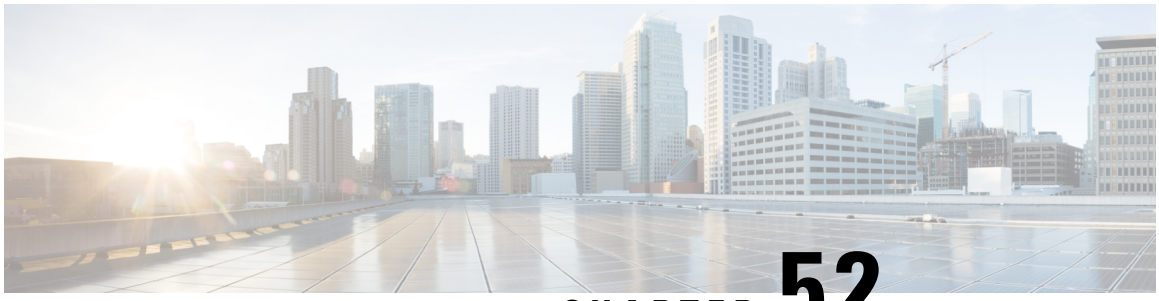
Example:

```
ip dhcp smart-relay
```

This is a DHCP smart-relay CLI configuration. In the example, the device forwards the DHCP broadcast received on Gigabitethernet interface 0/0 to the DHCP server (10.0.0.1), by inserting 192.168.255.254 in the gateway address field of the DHCP packet.

```
service dhcp
ip address 172.16.0.1 255.255.0.0
secondary ip address 192.168.255.254 255.255.0.0

interface GigabitEthernet0/0
ip helper-address 10.0.0.1
ip dhcp smart-relay
end
```



CHAPTER 52

DHCP Vendor Option Support

- Feature history for DHCP vendor option support, on page 801
- DHCP vendor option support, on page 801
- Configure a DHCP vendor option using CLI command, on page 803
- Configure a DHCPv6 client option option using a CLI template, on page 804
- Configure DHCP server using templates, on page 805

Feature history for DHCP vendor option support

Table 301: Feature History Table

Feature Name	Release Information	Description
DHCP Option Support	Cisco IOS XE Catalyst SD-WAN Release 16.12.1b	This feature allows DHCP server options, 43 and 191 to configure vendor-specific information in client-server exchanges.
DHCP vendor option support	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco Catalyst SD-WAN Control Components Release 20.10.1	This feature allows DHCP client option 124 and option 125 to configure vendor-specific information in client-server exchanges. Configure this feature using the CLI Add-on feature template in Cisco SD-WAN Manager.

DHCP vendor option support

A configurable dynamic host configuration protocol (DHCP) client is a network client feature that:

- allows use of user-specified client or class identifiers,
- supports suggestion of lease time during address requests, and
- enables configuration of vendor-class and vendor-specific information with Option 124 and Option 125.

This functionality provides flexibility for DHCP clients when requesting addresses and enables differential services, device classification, and feature enablement.

DHCP client options

The DHCP client provides flexibility by allowing the following options to be configured for a DHCP client:

- Option 124—This option is used by DHCP clients and servers to exchange vendor-class information.
- Option 125—This option is used by DHCP clients and servers to exchange vendor-specific information.

These options are used by Zero-Touch Provisioning (ZTP), Cisco Plug-and-Play (PnP), and Identity Services Engine (ISE) to support multiple use cases.

For example, the content of Option 124 is used for device classification and enabling solution-specific features.

The DHCP Vendor Option Support feature introduces new CLI parameters to make Option 124 and Option 125 flexible. You can modify and customize enabling vendor specific options to carry different values for different customer features. The combination of Option 124 and Option 125 enables various features.

The **ip dhcp client vendor-class** command provides flexibility to pack either Device PID or MAC Address of the DHCP client or any user configurable string in option-124. The default behavior for this command is to continue to send device PID when you choose option 124.

This default behavior can be overridden to carry MAC Address in Day 1 configuration mode by explicitly requesting option-125 from the server using the **ip dhcp client vendor-class** command.

By default, Cisco IOS XE DHCP client sends the following data:

Attribute	IPv4 DHCP Option	Default Value
Vendor-Identifying Vendor Class Option	124	PID



Note The **ip dhcp client vendor-class [mac-address | ascii | disable | hex]** command overrides PID with MAC Address / user defined string / disable Option 124.

DHCPv6 Client Options

Configuration parameters and other control information are carried in tagged data items that are stored in the options field of the DHCP message.

The DHCP client provides flexibility by allowing the following options to be configured for a DHCP client:

- Option 16—This option is used by DHCP clients and servers to exchange vendor-class information.
- Option 17—This option is used by DHCP clients and servers to exchange vendor-specific information

In DHCPv6, option-16 and option-17 are used by DHCP clients and servers to exchange vendor-specific information.

The **ipv6 dhcp client vendor-class** command provides flexibility to pack either Device PID or MAC Address of the DHCP Client or any user configurable string in option-16.

The default behavior for this command is to continue to send device PID when you choose option-16 but it can be overridden to carry MAC Address in Day 1 configuration mode using the **ipv6 dhcp client vendor-class** command.

By default, Cisco IOS XE DHCP client sends the following data:

Attribute	IPv4 DHCP Option	Default Value
Vendor Class Option	16	PID



Note The **ipv6 dhcp client vendor-class [mac-address | hex | ascii | disable]** command can be used to override default value of PID with MAC Address or User defined string or disable the option.

Configure a DHCP vendor option using CLI command

This section provides a sample CLI configuration to configure a DHCP vendor option.

For more information about using CLI templates, see CLI Add-On Feature Templates.

Before you begin

By default, CLI templates execute commands in global config mode.

Procedure

Step 1 Configure an interface type and enter the interface configuration mode.

Example:

```
interface type number
```

Step 2 Acquire an IP address on an interface from DHCP.

Example:

```
ip address dhcp
```

Step 3 Configure the DHCP vendor-class option.

Example:

```
ip dhcp client vendor-class [mac-address | ascii | hex | disable]
```

Note
You must first configure the **no ip dhcp-client** command before configuring the IP address.

Override the device PID with MAC address:

The DHCP vendor-class option overrides the device PID with the MAC Address.

```
interface GigabitEthernet 0/0/0
    ip address dhcp
    ip dhcp client vendor-class mac-address
    !
```

Override the device PID with user defined string in hex or in ascii format:

```
interface GigabitEthernet 0/0/0
    ip address dhcp
    ip dhcp client vendor-class hex aabbcc
    !

interface GigabitEthernet 0/0/0
    ip address dhcp
    ip dhcp client vendor-class ascii cisco
    !
```

Disable option-124 in DHCP messages:

```
interface GigabitEthernet 0/0/0
    ip address dhcp
    ip dhcp client vendor-class disable
    !
```

Configure a DHCPv6 client option option using a CLI template

By default, CLI templates execute commands in global config mode.

For more information about using CLI templates, see *CLI Add-On Feature Templates* in the *Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x*.

The section provides a sample CLI configuration to configure DHCPv6 client option.

Procedure

Step 1 Configure an interface type and enter the interface configuration mode.

Example:

```
interface type number
```

Step 2 Acquire an IPv6 address on an interface from DHCP.

Example:

```
ipv6 address dhcp
```

Step 3 Configure the DHCP vendor-class option.

Example:

```
ipv6 dhcp client vendor-class {mac-address | ascii | hex | disable}
```

Note
By default, the DHCPv6 client carries the device PID of the device in option-16.

This default behaviour can be overridden by configuring the **ipv6 dhcp client vendor-class** command.

Override the device PID with the MAC address:

The DHCP vendor-class option overrides the Device PID with the MAC Address.

```
interface GigabitEthernet 0/0/0
    ipv6 address dhcp
    ipv6 dhcp client vendor-class mac-address
    !
```

Override the device PID with user defined string in hex or in ascii format:

```
interface GigabitEthernet 0/0/0
    ipv6 address dhcp
    ipv6 dhcp client vendor-class hex aabbcc
    !

interface GigabitEthernet 0/0/0
    ipv6 address dhcp
    ipv6 dhcp client vendor-class ascii cisco
    !
```

Disable option-16 in DHCP messages:

```
interface GigabitEthernet 0/0/0
    ipv6 address dhcp
    ipv6 dhcp client vendor-class disable
    !
```

Configure DHCP server using templates

To configure a Cisco IOS XE Catalyst SD-WAN device to act as a DHCP server using Cisco SD-WAN Manager templates:

1. Create a DHCP-Server feature template to configure DHCP server parameters, as described in this topic.
2. Create one or more interface feature templates, as described in the VPN-Interface-Ethernet and the VPN-Interface-PPP-Ethernet sections.
3. Create a VPN feature template to configure VPN parameters.

To configure a Cisco IOS XE Catalyst SD-WAN device interface as a DHCP helper to broadcast DHCP requests from DHCP servers, in the **DHCP Helper** field of the applicable interfaces template, enter the addresses of the DHCP servers.

Use the DHCP-Server template for all Cisco Catalyst SD-WANs.

You enable DHCP server functionality on a Cisco IOS XE Catalyst SD-WAN device interface so it can assign IP addresses to hosts in the service-side network.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Device Templates**, and then click **Create Template**.

In Cisco vManage Release 20.7.1 and earlier releases, **Device Templates** is titled **Device**.

a) From the **Create Template** drop-down list, choose **From Feature Template**.
b) From the **Device Model** drop-down list, select the type of device for which you are creating the template.
c) Click **Service VPN** or scroll to the **Service VPN** section.
d) From **Additional VPN Templates**, click **VPN Interface**.
e) From the **Sub-Templates** drop-down list, choose DHCP Server.
f) From the **DHCP Server** drop-down list, click **Create Template**. The DHCP-Server template form is displayed.

This form contains fields for naming the template, and fields for defining the DHCP Server parameters.

g) In **Template Name**, enter a name for the template.

The name can be up to 128 characters and can contain only alphanumeric characters.

h) In **Template Description**, enter a description of the template.

The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the **Scope** drop-down list.

Step 3 Configure DHCP basic server functionality.

Table 302:

Parameter Name	Description
Address Pool*	Enter the IPv4 prefix range, in the format *prefix/length*, for the pool of addresses in the service-side network for which the router interface acts as DHCP server.
Exclude Addresses	Enter one or more IP addresses to exclude from the DHCP address pool. To specify multiple individual addresses, list them separated by a comma. To specify a range of addresses, separate them with a hyphen.
Maximum Leases	Specify the number of IP addresses that can be assigned on this interface. Range: 0 through 4294967295
Lease Time	Specify how long a DHCP-assigned IP address is valid. Range: 0 through 4294967295 seconds

Parameter Name	Description
Offer Time	Specify how long the IP address offered to a DHCP client is reserved for that client. By default, an offered IP address is reserved indefinitely, until the DHCP server runs out of addresses. At that point, the address is offered to another client. Range: 0 through 4294967295 seconds Default: 600 seconds
Administrative State	Select Up to enable or Down to disable the DHCP functionality on the interface. By default, DHCP server functionality is disabled on an interface.

Step 4 Configure a static lease to assign a static IP address to a client device on the service-side network.

Table 303:

Parameter Name	Description
MAC Address	Enter the MAC address of the client to which the static IP address is being assigned.
IP Address	Enter the static IP address to assign to the client.
Hostname	Enter the hostname of the client device.

To edit a static lease, click **pencil** icon.

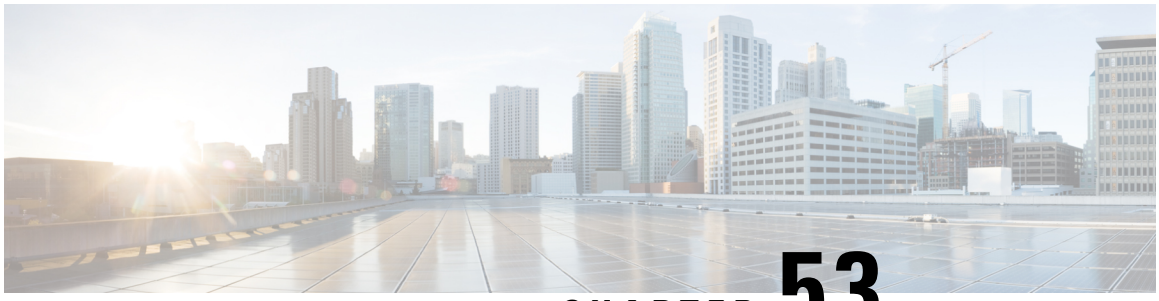
To remove a static lease, click **trash** icon.

To save the feature template, click **Save**.

Step 5 Configure advanced DHCP server options

Table 304:

Parameter Name	Description
Interface MTU	Specify the maximum MTU size of packets on the interface. Range: 68 to 65535 bytes
Domain Name	Specify the domain name that the DHCP client uses to resolve hostnames.
Default Gateway	Enter the IP address of a default gateway in the service-side network.
DNS Servers	Enter one or more IP address for a DNS server in the service-side network. Separate multiple entries with a comma. You can specify up to eight addresses.
TFTP Servers	Enter the IP address of a TFTP server in the service-side network. You can specify one or two addresses. If two, separate them with a comma.



CHAPTER 53

Geofencing

- Feature history for geofencing, on page 809
- Geofencing, on page 810
- Platforms supported for geofencing, on page 812
- Prerequisites for geofencing, on page 812
- Restrictions for geofencing, on page 812
- Configure geofencing, on page 813
- Methods for verifying the geofencing configuration, on page 817
- Geofencing alarms, on page 819

Feature history for geofencing

This table describes the developments of this feature, by release.

Table 305: Feature History

Feature name	Release information	Description
Geofencing	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature provides a way to restrict a device's location to an operational geographical boundary, and to identify a device's location and report any violations of the configured boundary. If the device is identified to be in violation, you can restrict network access to the device using Cisco SD-WAN Manager operational commands. In the CLI or a CLI template, configure geofencing coordinates for establishing the location of the device. You can also register for SMS alerts.

Feature name	Release information	Description
Added Support for Configuring Geofencing Using a Cisco System Feature Template	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	This feature adds support for configuring the geographical boundary of a device using a **Cisco System** feature template. With this feature, you can also configure automatic geolocation detection, where the device determines its own location, while configuring geofencing. A new parameter **auto-detect-geofencing-location** is added to the **geolocation (system)** command.
Added Support for LTE Advanced NIM Modules	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	Added support for Long-Term Evolution (LTE) Advanced Network Interface Modules (NIMs) for Cisco ISR 4000 routers.

Geofencing

Geofencing is a location-based feature that includes

- defining a geographical boundary within which a device can be deployed,
- configuring alerts to be sent to Cisco SD-WAN Manager or a mobile number when a device leaves the geographical boundary, and
- restricting network access when a device leaves the specified boundary.

Geographical boundary

Devices use Global Positioning System (GPS) functionality provided by a Long-Term Evolution (LTE) Pluggable Interface Module (PIM) to determine the device location.

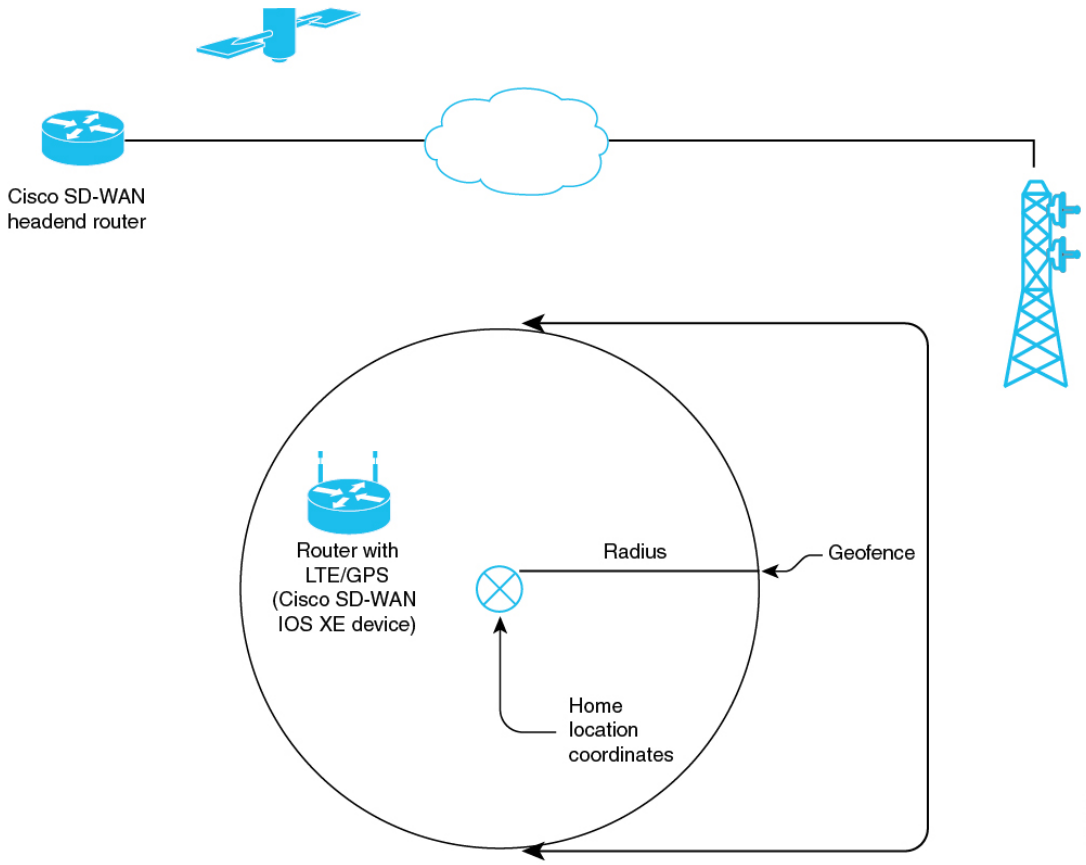
You can configure these for geofencing:

- Base location (latitude and longitude) and a geofence range for device detection
- Short message service (SMS) alert registration for sending SMS messages to a mobile number
- GPS enablement on an LTE PIM in the controller cellular 0/x/0 section

Geofencing status alerts are sent to Cisco SD-WAN Manager upon detection of device boundary violations.

Overview

Figure 7: Overview of geofencing



Configuration

- In Cisco SD-WAN Manager, you can use operational commands for restricting network access if a device exceeds its geographical boundary.

  For information on the operational commands for restricting network access, refer to the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

- From Cisco vManage Release 20.7.1, you can configure geofencing using a Cisco System feature template.

Benefits of geofencing

- Protects against inappropriate access to an organization's network if a device is beyond its geographical boundary
- Notifies end users of any displaced devices
- Supports a geofence radius for specifying the target location of the device
- Supports SMS alerts for mobile phone alerts

Platforms supported for geofencing

Supported devices:

- Cisco ISR 1000 with Long-Term Evolution (LTE) (fixed and pluggable)
- Cisco Catalyst 8K with LTE Pluggable Interface Module (PIM)
- Cisco ISR 4000 with LTE Advanced Network Interface Modules (NIMs)

Supported LTE PIMs:

- P-LTE-VZ(WP7601)
- P-LTE-US(WP7603)
- P-LTE-JN(WP7605)
- P-LTE-MNA(WP7610)
- P-LTE-GB(WP7607)
- P-LTE-IN(WP7608)
- P-LTE-AU(WP7609)
- P-LTEA-EA(EM7455)
- P-LTEA-LA(EM7430)

Supported LTE advanced NIMs:

- NIM-LTEA-EA(EM7455)
- NIM-LTEA-LA(EM7430)

Prerequisites for geofencing

Built-in LTE interface

Ensure that your Cisco IOS XE Catalyst SD-WAN C1100 series router has a built-in Long-Term Evolution (LTE) interface.

SIM card

A SIM card is mandatory in the LTE PIM for receiving SMS alerts.

Restrictions for geofencing

Device mode

Geofencing is supported only on devices in controller mode.

Configure geofencing

Geofencing is a location-based feature that enables defining a geographical boundary within which a device can operate.

Use one of these methods to configure geofencing:

- Feature template
- CLI commands

Configure geofencing using templates

Geofencing is a location-based feature that enables defining a geographical boundary within which a device can operate.

From Cisco vManage Release 20.7.1, you can configure geofencing using a Cisco System feature template.

Before you begin

Follow these steps to configure geofencing using a feature template.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**.

In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

Step 3 Click **Add Template**.

Step 4 Choose a device.

Step 5 In the **Select Template** > **Basic Information** section, click **Cisco System**.

Step 6 In the **Template Name** field, enter a name for the template.

The name can be up to 128 characters and can contain only alphanumeric characters.

Step 7 In the **Template Description** field, enter a description of the template.

The description can be up to 2048 characters and can contain only alphanumeric characters.

Step 8 In the **Basic Configuration** section of the **Cisco System** template, choose a value from the drop-down list for **Console Baud Rate (bps)**.

Console Baud Rate (bps) is a mandatory field for configuring geofencing.

Step 9 Click **GPS** or navigate to the **GPS** section of the **Cisco System** template.

Step 10 In the **Latitude** field, leave the field set to **Default** for automatic detection of a device.

Range: -90.0 - 90.0

Step 11 In the **Longitude** field, leave the field set to **Default** for automatic detection of a device.

Range: -180.0 - 180.0.

Note
If you manually specify **Latitude** and **Longitude** coordinates, you disable automatic detection of a device.

Automatic detection of a device can fail if a device does not have a last-known valid location.

Step 12 In the **Geo Fencing Enable** field, change the scope from **Default** to **Global**, and click **Yes** to enable geofencing.

The **Geo Fencing Enable** field is not enabled by default.

Step 13 (Optional) In the **Geo Fencing Range in meters** field, specify a geofencing range unit in meters.

The geofencing range specifies the radius from the base target location in meters.

The default geofencing range is 100 meters. You can configure a geofencing range of 100 to 10,000 meters.

Step 14 (Optional) In the **Enable SMS** drop-down list, change the scope to **Global**, and click **Yes** to enable SMS alerts.

An SMS alert is delivered when a device is determined to be outside the configured geofencing radius of its target location.

Note
The presence of a SIM card is mandatory in the Long-Term Evolution PIM for receiving SMS alerts.

Step 15 (Optional) In the **Mobile Number 1** field, add a mobile number for receiving SMS alerts.

Note
Mobile numbers must start with a + sign, include a country code, an area code, with no spaces between the country code and the area code, and the remaining digits.

Sample mobile number: +12344567236.

You can configure additional mobile phone numbers by clicking the **+** icon.

You can configure up to a maximum of four mobile numbers.

Step 16 Click **Save**.

Configure geofencing using CLI commands

Geofencing is a location-based feature that enables defining a geographical boundary within which a device can operate.

For information on the operational commands for restricting network access, refer to the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

Before you begin

Follow these steps to configure geofencing using CLI commands:

Procedure

Step 1 Configure latitude, longitude, a geofence range, and SMS alerts.

a) Configure a base location latitude and longitude.

Example:

```
Device(config)# system
Device(config-system)# gps-location latitude 37.317342 longitude -122.218170
```

b) Enable automatic detection of a device where the device determines its own location.

Example:

```
Router(config)# system
Router(config-system)# no gps-location latitude
Router(config-system)# no gps-location longitude
Router(config-system)# gps-location auto-detect-geofencing-location
```

Do not configure latitude and longitude coordinates when using the auto-detect-geofencing-location parameter.

You can choose to either configure a base location using latitude and longitude coordinates, or you can enable automatic detection of a device.

c) Enable, configure, and specify a geofence range.

For geofencing range, the unit is meters. Geofencing range is an optional configuration parameter, and if not configured, it takes the default value of 100 meters.

Example:

```
Device(config-system)# gps-location geo-fencing-enable
Device(config-system)# gps-location geo-fencing-config
Device(conf-geo-fencing-config)# geo-fencing-range 1000
```

d) Add mobile numbers for receiving SMS alerts.

Example:

```
Device(config-geo-fencing-config)# sms

Device(config-sms)# sms-enable
Device(config-sms)# mobile-number +12344567234
Device(config-mobile-number-+12344567234)# exit
Device(config-mobile-number-+12344567234)# mobile-number +12344567235
Device(config-mobile-number-+12344567235)# exit
Device(config-mobile-number-+12344567235)# mobile-number +12344567236
Device(config-mobile-number-+12344567236)# exit
Device(config-mobile-number-+12344567236)# mobile-number +12344567237
Device(config-mobile-number-+12344567237)# exit
Device(config-sms)# commit
```

Step 2 Enable GPS on an LTE PIM.

These are example CLI configurations for enabling GPS on an LTE PIM in the 0/x/0 section of the configuration.

a) Enable GPS on an LTE PIM in the controller cellular section.

Example:

```
Device(config)# controller Cellular 0/2/0
Device(config-Cellular-0/2/0)# lte gps enable
```

b) Enable ms-based mode with a SIM card present in an LTE PIM.

We recommend that you use ms-based with a SIM card present.

Mobile station-based assistance refers to the case where the Global Navigation Satellite System (GNSS-enabled) mobile device computes its own position locally.

Example:

```
Device(config-Cellular-0/2/0)# lte gps mode ms-based
```

c) Enable National Marine Electronics Association (NMEA) streaming.

Example:

```
Device(config-Cellular-0/2/0)# lte gps nmea
```

Configuration example using CLI commands

Configuration example for geofencing, with automatic location detection

This is an end-to-end configuration of geofencing and controller cellular, with automatic detection of a device location.

```
system
  gps-location auto-detect-geofencing-location
  gps-location geo-fencing-enable
  gps-location geo-fencing
    geo-fencing-range 1000
    sms
      sms-enable
      mobile-number +112312345676
      !
      mobile-number +112312345677
      !
      mobile-number +112312345678
      !
      mobile-number +112312345679
      !
     !
    !
  system-ip             10.1.1.35
  site-id               273
  admin-tech-on-failure
  organization-name     LTE-Test
  vbond vbond-dummy.test.info port 12346
  !
  controller Cellular 0/2/0
  lte gps enable
  lte gps mode ms-based
  lte gps nmea
  !
```

Configuration example for geofencing, with manual configuration of location

This is an end-to-end configuration of geofencing and controller cellular, with manual configuration of latitude and longitude coordinates.

```
system
   gps-location latitude 37.317342
```

```
gps-location longitude -122.218170
gps-location geo-fencing-enable
gps-location geo-fencing-config
 geo-fencing-range 1000
 sms
  sms-enable
  mobile-number +112312345676
  !
  mobile-number +112312345677
  !
  mobile-number +112312345678
  !
  mobile-number +112312345679
  !
  !
  !
```

Methods for verifying the geofencing configuration

You can use one or more of these verification commands to view information about the geofencing configuration.

Verifying that geofencing is enabled

Use the **show sdwan geofence-status** command to verify that geofencing is enabled.

In the output, `Geofence Config Status = Geofencing-Enabled` indicates that geofencing is enabled.

In the output, `Auto-Detect Geofencing Enabled = true` indicates that automatic detection of the device is enabled. If automatic detection of the device is not enabled, `Auto-Detect Geofencing Enabled = false` is displayed in the output.

```
Device# show sdwan geofence-status
geofence-status
 Geofence Config Status =                  Geofencing-Enabled
 Target Latitude =                         37.317342
 Target Longitude =                        -122.218170
 Geofence Range(in m) =                    100
 Current Device Location Status =          Location-Valid
 Current Latitude =                        37.317567
 Current Longitude =                        -122.218170
 Current Device Status =                   Within-defined-fence
 Distance from target location(in m) =     30
 Last updated device location timestamp =  2021-05-06T22:58:34+00:00
 Auto-Detect Geofencing Enabled =          true
```

Verifying GPS enablement and mode

Use the **show cellular 0/x/0 gps** command to check the GPS enablement and mode.

In the output, `GPS Feature = enabled` indicates that GPS for controller cellular is enabled.

In the output, `GPS Mode Configured = ms-based` indicates that the GPS mode is `ms-based`.

```
Device# show cellular 0/2/0 gps
GPS Feature =  enabled
GPS Mode Configured =  ms-based
GPS Port Selected =  Dedicated GPS port
GPS Status =  GPS coordinates acquired
Last Location Fix Error =  Offline [0x0]
```

```
============================
GPS Error Count =  0
NMEA packet count =  17899
NMEA unknown packet count =  0


Per talker traffic count =
        US-GPS =  5982
        GLONASS =  2560
        GALILEO =  3505
        BEIDOU =  0
        GNSS =  3409
        Unknown talker =  2443
============================
Speed over ground in km/hr =  0
============================

Latitude =  31 Deg 19 Min 14.6203 Sec North
Longitude =  122 Deg 58 Min 32.8164 Sec West
*Apr 15 23:58:45.298: GPS Mode Configured =Timestamp (GMT) =  Thu Apr 15 23:57:21 2021

Fix type index =  0, Height =  18 m
Satellite Info
---------------
Satellite #2, elevation 51, azimuth 42, SNR 24 *
Satellite #5, elevation 36, azimuth 144, SNR 34 *
Satellite #6, elevation 14, azimuth 45, SNR 24 *
Satellite #12, elevation 72, azimuth 146, SNR 33 *
Satellite #25, elevation 60, azimuth 305, SNR 25 *
============================
 Total Satellites in view =  5
 Total Active Satellites =  5
 GPS Quality Indicator =  1
 Total satellites from each constellation:
         US-GPS =  3
         GLONASS =  1
         GALILEO =  1
         BEIDOU =  0
============================
```

Displaying geofencing notifications

Use the **show sdwan notification stream viptela** command to display geofencing notifications.

```
Device# show sdwan notification stream viptela
notification
 eventTime 2021-04-13T23:05:02.881093+00:00
 system-logout-change
  severity-level minor
  host-name pm5
  system-ip 172.16.255.15
  user-name admin
  user-id 0
 !
!
notification
 eventTime 2021-04-14T00:36:31.344117+00:00
 geo-fence-alert-status
  severity-level major
  host-name pm5
  system-ip 172.16.255.15
  alert-type device-location-inside
  alert-msg Device Locking started for Geofencing Mode and device is within range
```

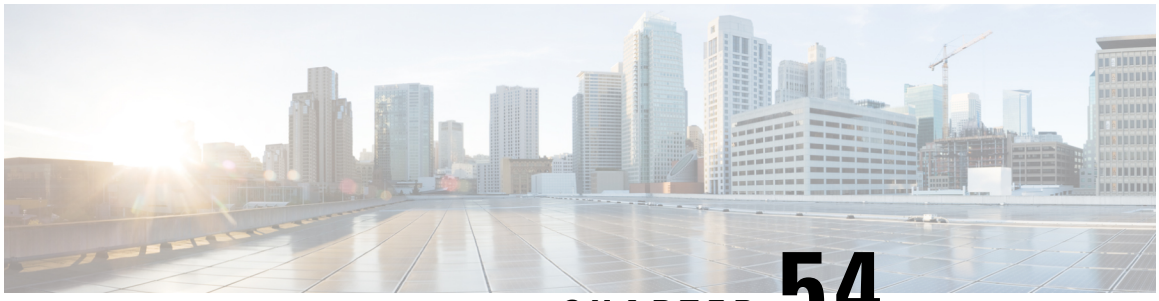
Geofencing alarms

You can monitor geofencing alarms based on severity or based on time, in Cisco SD-WAN Manager, from **Monitor** > **Logs**.

Note Cisco vManage Release 20.6.1 and earlier: **Monitor** > **Alarms**

Table 306: Geofencing alarms

Type	Severity	Description
Device Location Outside	**Critical**	This notification is sent when the device location is outside the defined geofencing range.
Device Location Inside	**Major**	This notification is sent when the device location is determined to be inside the defined geofence range when it was previously determined to be outside the defined geofence range, or the device location could not be obtained due to a GPS signal outage.
Device Location Lost	**Major**	This notification is sent when the device location cannot be determined due to a GPS outage.
Device Location Update	**Major**	This notification is sent when the device location changes by more than 20 meters either when geofencing is enabled or not. If geofencing is not enabled, this notification is sent only if the device location is available.



CHAPTER 54

Multitenancy

- Feature history for Cisco Catalyst SD-WAN multitenancy, on page 821
- Cisco Catalyst SD-WAN multitenancy, on page 821
- Feature availability, on page 825
- User roles in multitenant environment, on page 826
- Provider and tenant remote servers and images, on page 828
- Supported devices, hypervisor and persona for multitenancy, on page 828
- Supported hardware specifications for multitenancy, on page 830
- Restrictions for multitenancy, on page 830
- Initial setup for multitenancy, on page 831
- Expand a multitenant deployment to support more tenants and tenant devices, on page 839
- Upgrade SD-WAN Controller and Edge Device Software, on page 841

Feature history for Cisco Catalyst SD-WAN multitenancy

Table 307: Feature history

Feature name	Release information	Description
Multitenancy Support for Cisco Catalyst Cellular Gateways	Cisco IOS CG Release 17.14.1 Cisco Catalyst SD-WAN Control Components Release 20.14.1	Added multitenancy support for Cisco Catalyst Cellular Gateways.

Cisco Catalyst SD-WAN multitenancy

With Cisco Catalyst SD-WAN multitenancy, a service provider can manage multiple customers, called tenants, from Cisco SD-WAN Manager.

The tenants share the same set of underlying Cisco SD-WAN Control Components:

- Cisco SD-WAN Manager
- Cisco SD-WAN Validator
- Cisco SD-WAN Controller

The tenant data is logically isolated on these shared control components.

Access to multitenancy

The service provider accesses Cisco SD-WAN Manager using a domain name mapped to the IP address of a Cisco SD-WAN Manager cluster and manages the multitenant deployment.

Each tenant is provided a subdomain to access a tenant-specific Cisco SD-WAN Manager view and manage the tenant deployment.

A service provider using the domain name managed-sp.com can assign tenants Customer1 and Customer2 the subdomains:

- customer1.managed-sp.com
- customer2.managed-sp.com

This allows the service provider to manage multiple tenants on the same set of SD-WAN Controllers instead of providing each customer a single-tenant setup with a dedicated set of SD-WAN Controllers.

Full enterprise multitenancy

Cisco Catalyst SD-WAN supports multitenancy and offers enterprises the flexibility of segregated roles such as service provider and tenants. Service providers can use multitenancy to provide Cisco Catalyst SD-WAN service offerings to their customers.

Security

Send and receive AAA traffic over management VPN 512 from Cisco IOS XE Catalyst SD-WAN Release 17.16.1a.

Overlapping VPN numbers

A particular VPN or a set of common VPNs is assigned to a specific tenant, with their own configurations and monitoring dashboard environment. These VPN numbers can overlap where they are used by other tenants.

On-prem and cloud deployment models

Cisco Catalyst SD-WAN controllers can be deployed in:

- An organization data center on servers running VMware ESXi 6.7 or later, or the Kernel-based Virtual Machine (KVM) hypervisor.
- Amazon Web Services (AWS) servers hosted by Cisco CloudOps.

Tenant-specific Cisco SD-WAN Analytics

Cisco SD-WAN Analytics is a cloud-based service that offers insights into the performance of applications and the underlying SD-WAN network infrastructure.

Each tenant can obtain Cisco SD-WAN Analytics insights for their overlay network by:

- Requesting a tenant-specific Cisco SD-WAN Analytics instance.
- Enabling data collection on SD-WAN Manager.

The service provider must enable cloud services on SD-WAN Manager in the provider view to facilitate the onboarding of the Cisco SD-WAN Analytics instance for the tenant overlay network.

Single tenant environments

A single tenant environment exclusively manages, and is responsible for, its own Cisco Catalyst SD-WAN Control Components and devices. All configured resources are visible to the single tenant administrator in the Cisco SD-WAN Manager interface.

Cloud-delivered Catalyst SD-WAN

Cloud-delivered Catalyst SD-WAN operates as a tenant within a multitenant environment rather than as a single tenant. Cloud-delivered Catalyst SD-WAN users do not see controller infrastructure settings in Cisco SD-WAN Manager. Their available information is limited to their own components and WAN edge devices.

For more information on Cloud-delivered Catalyst SD-WAN, see Cloud-delivered Cisco SD-WAN Getting Started Guide.

Multitenancy

- Multitenant Cisco SD-WAN Manager
- Multitenant Cisco SD-WAN Validator
- Multitenant Cisco SD-WAN Controller
- Tenant-specific WAN edge devices

Multitenant SD-WAN Manager

Defines how SD-WAN Manager is accessed and used by service providers and tenants in a multitenant deployment.

Provider view

SD-WAN Manager is deployed and configured by the service provider. The provider enables multitenancy and creates a SD-WAN Manager cluster to serve tenants. Only the provider can access a SD-WAN Manager instance through the SSH terminal.

In the Provider view, SD-WAN Manager:

- Provides service providers with an overall view of the SD-WAN multitenant deployment.
- Allows service providers to manage all Cisco Catalyst SD-WAN Validator and SD-WAN Controller devices.
- Enables service providers to monitor and manage each tenant deployment through the Provider-as-Tenant view.

Tenant view

In the tenant view, SD-WAN Manager allows individual tenants to:

- Monitor and manage their own deployment through a dashboard.

- Deploy and configure WAN edge devices.
- Configure custom policies on Cisco Catalyst SD-WAN Controllers.

  Cisco Catalyst SD-WAN Control Component infrastructure settings are not displayed in tenant view.

Multitenant SD-WAN Validator

Describes how SD-WAN Validator function in a multitenant environment.

SD-WAN Validators are deployed and configured by the service provider.

Only the provider can access a SD-WAN Validator through the SSH terminal.

In a multitenant deployment, SD-WAN Validators:

- Serve WAN edge devices of multiple tenants.
- Authenticate and validate WAN edge devices as they are added to the overlay network.

Multitenant SD-WAN Controllers

Explains the deployment and management of SD-WAN Controller in a multitenant environment.

SD-WAN Controllers are deployed by the service provider. Only the provider can:

- Create and attach device and feature templates to SD-WAN Controllers.
- Access a SD-WAN Controller through the SSH terminal.

Tenant assignment

- When a tenant is created, SD-WAN Manager assigns two SD-WAN Controllers for the tenant.
- The SD-WAN Controllers form an active-active cluster.
- Each tenant is assigned only two SD-WAN Controllers.
- Before a tenant is created, two SD-WAN Controllers must be available to serve the tenant.

Controller selection

- When multiple pairs of SD-WAN Controllers are available:
  - SD-WAN Manager assigns the pair connected to the lowest number of forecast devices.
  - If two pairs are connected to the same number of devices, the pair serving the lowest number of tenants is assigned.
- From Cisco vManage Release 20.9.1:
  - While onboarding a tenant, you can choose the pair of multitenant SD-WAN Controllers that serve the tenant.
  - After onboarding, the tenant can be migrated to a different pair if necessary.

- For more information, refer to the information about manual and automatic tenant placement in Multitenancy, on page 907.

- Each pair of SD-WAN Controllers can serve up to 24 tenants.

Tenant policy management

- Tenants can configure custom policies on their assigned SD-WAN Controllers.
- Cisco SD-WAN Manager notifies the Controllers to pull the policy templates.
- Controllers pull the templates and deploy the policy configuration for the specific tenant.

Provider access

- Only the provider can view events, audit logs, and OMP alarms for a SD-WAN Controller on SD-WAN Manager.
- Starting from Cisco Catalyst SD-WAN Manager Release 20.16.1, a provider can view alarms and events for the sites and devices in its tenancy.

Tenant-specific WAN edge devices

A tenant or the provider acting on behalf of a tenant can:

- Add WAN edge devices to the tenant network.
- Configure the devices.
- Remove the devices from the tenant network.
- Access the device through the SSH terminal.

A provider can manage the WAN edge devices only from the provider-as-tenant view. In the provider view, SD-WAN Manager does not show any WAN edge device information. Refer to SD-WAN Manager views for providers, on page 827.

SD-WAN Manager reports WAN edge device events, logs, and alarms only in the tenant and the provider-as-tenant views.

Feature availability

Some Cisco Catalyst SD-WAN features are available only in specific tenancy configurations.

Table 308: SD-WAN feature availability

Feature	Single Tenant	Multitenant	Catalyst SD-WAN Cloud
Identity Services Engine (ISE) integration	Yes	Yes (from SD-WAN Control Components 20.18.2)	Yes (for Early Adopter releases only)

Feature	Single Tenant	Multitenant	Catalyst SD-WAN Cloud
Intent-based hub and spoke topology	Yes	No	No
Controller group affinity	Yes	No	No
Cisco duo multifactor authentication (MFA) support	Yes	No	No
SD-Routing support without an SD-WAN Controller	Yes	No	No
Data stream and packet capture setting changes at tenant level	—	No, supported at provider level	No, supported at provider level

User roles in multitenant environment

A multitenant environment includes the service provider and tenant roles. Each role has distinct privileges, views, and functions.

- Provider role
- Tenant role

Provider role

- The provider role entitles system-wide administrative privileges.
- A user with the provider role has the default username **admin**.
- The provider user can access SD-WAN Manager using the domain name of the service provider or by using the SD-WAN Manager IP address.
- When using a domain name, the domain name has the format: `https://managed-sp.com`.
- The admin user is part of the user group netadmin.

  Users in this group are permitted to perform all operations on the controllers and the WAN edge devices of the tenants. You can add additional users to the netadmin group.
- You cannot modify the privileges of the netadmin group.
- When you create a new provider user in SD-WAN Manager, including a netadmin user, by default, the user is not allowed SSH access to the SD-WAN Manager VM. To enable SSH access, configure SSH authentication using a AAA template and push the template to SD-WAN Manager. For more information on enabling SSH authentication, refer to the *Cisco Catalyst SD-WAN User Management Guide*.

SD-WAN Manager views for providers

Provider view

When a provider user logs in to multitenant SD-WAN Manager as **admin** or another **netadmin** user, SD-WAN Manager presents the provider view and displays the provider dashboard.

You can perform the following functions from the provider view:

- Provision and manage SD-WAN Manager, SD-WAN Validators, and SD-WAN Controllers.
- Add, modify, or delete tenants.
- Monitor the overlay network.
- Starting from Cisco Catalyst SD-WAN Manager Release 20.16.1, view alarms and events for the sites and devices of its tenants.

Provider-as-tenant view

When a provider user selects a specific tenant from the **Select Tenant** drop-down list at the top of the provider dashboard, SD-WAN Manager presents the provider-as-tenant view and displays the tenant dashboard for the selected tenant. The provider user has the same view of SD-WAN Manager as a tenant user would when logged in as **tenantadmin**. From this view, the provider can manage the tenant deployment on behalf of the tenant.

In the provider dashboard, a table of tenants presents a status summary for each tenant. A provider user can also launch the provider-as-tenant view by clicking on a tenant name in this table.

Tenant role

- The tenant role entitles tenant administrative privileges.
- A user with the tenant role has the default username **tenantadmin**.
- The default password is **`Cisco#123@Viptela`**.

  We recommend that you change the default password on first login.
- The **tenantadmin** user is part of the user group **tenantadmin**. Users in this group are permitted to perform all operations on the WAN edge devices of the tenants. You can add additional users to the **tenantadmin** group.
- You cannot modify the privileges of the **tenantadmin** group. On SD-WAN Manager, you can view the privileges of the user group from the **Administration** > **Manage Users** > **User Groups** page.

  For more information about configuring users and user groups, refer to the *Cisco Catalyst SD-WAN User Management Guide*.
- A tenant user can log in to SD-WAN Manager using a dedicated URL and the default username **tenantadmin**.

  For example, the dedicated URL of a tenant could be `https://customer1.managed-sp.com` for a provider using the domain name `https://managed-sp.com`. When the user logs in, SD-WAN Manager presents the tenant view and displays the tenant dashboard.

- If you cannot access the dedicated tenant URL, update the subdomain details in the /etc/hosts file on the local machine. Alternatively, if you use an external DNS server, add a DNS entry for the tenant subdomain.

A tenant user with administrative privileges can perform these functions:

- Provision and manage tenant routers
- Monitor overlay network of the tenant
- Create custom policies on the assigned Cisco SD-WAN Controller
- Upgrade the software on the tenant routers.
- Starting from Cisco Catalyst SD-WAN Manager Release 20.16.1, view tenant-specific information of controller connections and OMP statistics in a Cisco Catalyst SD-WAN network.

Provider and tenant remote servers and images

Cisco Catalyst SD-WAN Manager Release 20.14.1 and earlier releases

In these releases, remote servers and images operate as follows:

- Only the provider can add remote servers and images.
- The remote servers and images are visible to all tenants. Tenants can use the remote servers and images but can't edit them.

Cisco Catalyst SD-WAN Manager Release 20.15.1

In these releases, remote servers and images operate as follows:

- A tenant can add a remote server and remote image for both software images and virtual images. The remote server and image are visible only to the corresponding tenant and not to the provider or other tenants.
- The provider can add a remote server, a remote image, and a local image for both software images and virtual images in SD-WAN Manager.

Supported devices, hypervisor and persona for multitenancy

The following Cisco Catalyst SD-WAN edge devices support multitenancy.

Supported devices

Table 309: Supported devices

Platform	Device Models
Cisco IOS XE Catalyst SD-WAN device	• Cisco ASR 1000 Series Aggregation Services Routers • Cisco ISR 1000 Series Integrated Services Routers • Cisco ISR 4000 Series Integrated Services Routers • Cisco Catalyst 8200 Series Edge Platforms • Cisco Catalyst 8300 Series Edge Platforms • Cisco Catalyst 8500 Series Edge Platforms • Cisco Catalyst 8000V Edge Software • Cisco ENCS Platforms
Cisco Catalyst Cellular Gateways	(From Cisco IOS CG Release 17.14.1 and Cisco Catalyst SD-WAN Control Components Release 20.14.1) • CG418-E • CG522-E

Supported hypervisors for multitenancy

- VMware ESXi 6.7 or later
- KVM
- AWS (cloud-hosted and managed by Cisco CloudOps)
- Microsoft Azure (cloud-hosted and managed by Cisco CloudOps)

SD-WAN Manager personas

The personas enable a predefined set of services on the Cisco SD-WAN Manager instance.

From Cisco vManage Release 20.6.1, a multitenant Cisco SD-WAN Manager instance can have one of these three personas.

Table 310: SD-WAN Manager personas

Persona	Services
Compute+Data	Cluster Oracle, Service Proxy, Messaging Service, Coordination Service, Configuration Database, Data Collection Agent, Statistics Database, and Application Server

Persona	Services
Data	Cluster Oracle, Service Proxy, Application Server, Data Collection Agent, and Statistics Database
Compute	Cluster Oracle, Service Proxy, Messaging Service, Coordination Service, Configuration Database, and Application Server

Supported hardware specifications for multitenancy

The supported hardware specifications for the SD-WAN Validator, SD-WAN Manager, and the SD-WAN Controllers are as follows:

Hardware specifications to support 50 tenants and 1000 devices

For more information on supported hardware specifications for the SD-WAN Validator, SD-WAN Manager, and the Cisco SD-WAN Controllers see, Cisco Catalyst SD-WAN Controller Compatibility Matrix and Recommended Computing Resources.

Hardware specifications to support 75 tenants and 2500 devices

For more information on supported hardware specifications for the SD-WAN Validator, SD-WAN Manager, and the Cisco SD-WAN Controllers see, Cisco Catalyst SD-WAN Controller Compatibility Matrix and Recommended Computing Resources.

Hardware specifications to support 100 tenants and 5000 devices

For more information on supported hardware specifications for the SD-WAN Validator, SD-WAN Manager, and the Cisco SD-WAN Controllers see, Cisco Catalyst SD-WAN Controller Compatibility Matrix and Recommended Computing Resources.

Hardware specifications to support 150 tenants and 7500 devices

For more information on supported hardware specifications for the SD-WAN Validator SD-WAN Manager, and the Cisco SD-WAN Controllers see, Cisco Catalyst SD-WAN Controller Compatibility Matrix and Recommended Computing Resources.

Restrictions for multitenancy

Defines the limitations and unsupported configurations in a multitenant Cisco SD-WAN deployment.

- Connecting to a device by SSH

  Do not use a user-configured system IP address to connect to a device through SSH. Instead, use the IP address of the `vmanage_system` interface; this IP address is assigned by SD-WAN Manager.

- IP address of the `vmanage_system` interface

  To find the IP address of the `vmanage_system` interface, use only one of these methods:

  - Launch the device SSH terminal from SD-WAN Manager and find the `vmanage_system` IP address from the first line of the log-in prompt, or

- Run the **show interface description** command and find the `vmanage_system` IP address from the command output.
- If you add a second tenant immediately after adding a tenant, SD-WAN Manager adds them sequentially, and not in parallel.
- If you are adding a WAN edge device that you had previously invalidated and deleted from an overlay network, you must reset the device software after adding the device.

  To reset the software on a Cisco IOS XE Catalyst SD-WAN device, use the command, **request platform software sdwan software reset**.
- For Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and earlier releases, single-node SD-WAN Manager is not supported on a multitenant deployment.
  - A minimum of a 3-node SD-WAN Managercluster is required for a multitenant deployment.

- Upgrading devices during SD-WAN Controller or SD-WAN Validator upgrade

  When a SD-WAN Controller or SD-WAN Validator upgrade is in progress, upgrade of tenant edge devices is not supported.
- SD-WAN Controller group feature

  The SD-WAN Controller group feature is not supported in multitenant mode.
- Device site ID

  The WAN edge device's site ID must be different from the SD-WAN Control Components site ID when the SD-WAN Manager has different public and private IP addresses.
- Cannot change a SD-WAN Manager back to single tenant mode

  After you enable SD-WAN Manager for multitenancy, you cannot change it back to single tenant mode.

Initial setup for multitenancy

- Prerequisites for Cisco Catalyst SD-WAN multitenancy
- Initial setup for Cisco Catalyst SD-WAN multitenancy

Prerequisites for Cisco Catalyst SD-WAN multitenancy

Ensure these prerequisites are met to successfully deploy and enable Cisco Catalyst SD-WAN multitenancy.

- Download and install software versions as recommended in the table below:

Table 311: Minimum software prerequisites for Cisco Catalyst SD-WAN multitenancy

Device	Software Version
Cisco SD-WAN Manager	Cisco vManage Release 20.6.1
Cisco SD-WAN Validator	Cisco SD-WAN Release 20.6.1

Device	Software Version
Cisco SD-WAN Controller	Cisco SD-WAN Release 20.6.1
Cisco IOS XE Catalyst SD-WAN Device	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a

A configuration in which one or more controllers, or WAN edge devices, are running software versions earlier than those mentioned in the table above is not supported.

- Ensure a new SD-WAN Manager software image is downloaded and installed instead of migrating an existing single-tenant instance to multitenant mode, even if all devices are invalidated or deleted.
- Follow the recommended hardware specifications in the Supported Devices and Hardware specifications section of this document.

Initial setup for Cisco Catalyst SD-WAN multitenancy

Follow these steps to set up Cisco Catalyst SD-WAN multitenancy.

Procedure

Step 1 Log in to SD-WAN Manager as the provider **admin** user.

Step 2 Create SD-WAN Manager cluster.

a) To support 50 tenants and 1000 devices across all tenants, create a 3-node Cisco SD-WAN Manager Multitenant cluster.

b) To support 100 tenants and 5000 devices across all tenants, create a 6-node Cisco SD-WAN Manager Multitenant cluster.

c) From Cisco IOS XE Release 17.6.3a, Cisco vManage Release 20.6.3, to support 150 tenants and 7500 devices across all tenants, create a 6-node Cisco SD-WAN Manager Multitenant cluster.

Step 3 Create and configure Cisco SD-WAN Validator instances. Refer to the Deploy SD-WAN Validator topic in the Overlay Network Bring-Up Process section of the *Cisco Catalyst SD-WAN Getting Started Guide*.

While configuring Cisco SD-WAN Validator instances, configure the service provider organization name (`sp-organization-name`) and the organization name (`organization-name`). Refer to the information about configuring an organization name in the *Cisco Catalyst SD-WAN Getting Started Guide*.

Example:

```
sp-organization-name multitenancy
organization-name multitenancy
```

Step 4 Create Cisco SD-WAN Controller instances. Refer to the Deploy SD-WAN Controller topic in the Overlay Network Bring-Up Process section of the *Cisco Catalyst SD-WAN Getting Started Guide*.

- To support 50 tenants and 1000 devices across all tenants, deploy 6 Cisco SD-WAN Controller instances.
- To support 100 tenants and 5000 devices across all tenants, deploy 10 Cisco SD-WAN Controllers.
- From Cisco IOS XE Release 17.6.3a, Cisco vManage Release 20.6.3, to support 150 tenants and 7500 devices across all tenants, deploy 16 Cisco SD-WAN Controllers.

Step 5 Add Cisco SD-WAN Controller to the overlay network.

Step 6 Onboard new tenants. See Add a new tenant, on page 845.

- Create a 3-node Cisco SD-WAN Manager Multitenant cluster
- Create a 6-node Cisco SD-WAN Manager Multitenant cluster
- Enable Multitenancy on Cisco SD-WAN Manager
- Add Cisco SD-WAN Controller

Create a 3-Node SD-WAN Manager multitenant cluster

To deploy and configure a 3-node SD-WAN Manager cluster to support a multitenant environment.

Procedure

Step 1 Download the Cisco vManage Release 20.6.1 or later software image from Cisco Software Download.

Step 2 Create three SD-WAN Manager instances by installing the downloaded software image file. Refer to the Deploy SD-WAN Manager topic in the Overlay Network Bring-Up Process section of the *Cisco Catalyst SD-WAN Getting Started Guide*.

- Deploy SD-WAN Manager servers with these hardware specifications: Hardware Specifications to Support 50 Tenants and 1000 Devices section of this document
- Choose the Compute+Data persona for each SD-WAN Manager instance. Example: vManage1, vManage2, and vManage3.

Step 3 Complete the following operations on the first SD-WAN Manager instance:

a) Configure the following using CLI:

- System IP address
- Site ID
- Service Provider organization name (`sp-organization-name`)
- Organization-name
- Cisco SD-WAN Validator IP address
- VPN 0 Transport/Tunnel interface
- VPN 0 Out-of-band (OOB) interface: Ensure that you assign a static IP address to this interface. Do not enable DHCP.
- VPN 512 Management interface
- Configure only one default route in VPN 0.

b) Enable Multitenancy on Cisco SD-WAN Manager.

c) (Optional) Using the CLI, install the Root CA certificate for the first SD-WAN Manager instance.

Skip this step if you are using a Symantec or Cisco PKI certificate.

d) Complete these steps through SD-WAN Manager:

1. Generate a certificate signing request. Refer to the Certificate Management section of the *Cisco Catalyst SD-WAN Getting Started Guide*.
2. After getting the certificate signed, install the certificate.

e) Configure the cluster IP address of the SD-WAN Manager server. Refer to the cluster management section of the *Cisco Catalyst SD-WAN Getting Started Guide*.

Before proceeding to the next step, ensure that the Manager IP Address field on the **Administration** > **Cluster Management** page shows the OOB interface address.

Step 4 Complete the following operations on the second and third SD-WAN Manager instances (vManage2 and vManage 3 in the example):

a) Configure the following using the CLI:

- System IP address
- Site ID
- Service Provider organization name (`sp-organization-name`)
- Organization-name
- Cisco SD-WAN Validator IP address
- VPN 0 Transport/Tunnel interface
- VPN 0 Out-of-band (OOB) interface: Ensure that you assign a static IP address to this interface. Do not enable DHCP.
- VPN 512 Management interface

b) (Optional) Using the CLI, install the Root CA certificate for the first SD-WAN Manager instance.

Skip this step if you are using a Symantec or Cisco PKI certificate.

c) Complete the following through SD-WAN Manager:

1. Generate a certificate signing request. Refer to the Certificate Management section of the *Cisco Catalyst SD-WAN Getting Started Guide*.
2. After getting the certificate signed, install the certificate.

d) Log in to the SD-WAN Manager web application server. Refer to the Cisco Catalyst SD-WAN Manager How-Tos section of the *Cisco Catalyst SD-WAN Getting Started Guide*.

e) Ping the OOB interfaces on the other two SD-WAN Manager instances and ensure they are reachable.

f) Configure the cluster IP address of the SD-WAN Manager server. Refer to the cluster management section of the *Cisco Catalyst SD-WAN Getting Started Guide*.

Before proceeding to the next step, ensure that the Manager IP Address field on the **Administration** > **Cluster Management** page shows the OOB interface address.

Enable multitenancy only on the first SD-WAN Manager instance.

Step 5 Log in to the first SD-WAN Manager instance and add the second instance to the cluster.

- The second instance reboots before being added to the cluster.
- While the second instance is being added to the cluster, on the **Administration** > **Cluster Management** page, the **Configure Status** for the second instance shows **Pending**. You can monitor the System Generated Cluster Sync transaction to check the progress of adding the second instance to the cluster.
- When the operation is completed, on the **Administration** > **Cluster Management** page, you can view both the first and second instances, and their node personas.

Step 6 Repeat the previous step to add additional SD-WAN Manager instances to the cluster.

After rebooting, you have to select persona (non-cloud setup) from CLI and services start running on the node according to the selected persona.

Create a 6-node SD-WAN Manager multitenant cluster

To deploy and configure a 6-node SD-WAN Manager cluster to support a multitenant environment.

Procedure

Step 1 Download the Cisco vManage Release 20.6.1 or later software image from Cisco Software Download.

Step 2 Create six SD-WAN Manager instances by installing the downloaded software image file. Refer to the Deploy SD-WAN Manager topic in the Overlay Network Bring-Up Process section of the *Cisco Catalyst SD-WAN Getting Started Guide*.

- To support 100 tenants and 5000 devices across all tenants, deploy SD-WAN Manager servers with the hardware specifications in the table Hardware Specifications to Support 100 Tenants and 5000 Devices of this document.
- From Cisco IOS XE Release 17.6.3a and Cisco vManage Release 20.6.3, to support 150 tenants and 7500 devices across all tenants, deploy SD-WAN Manager servers with these hardware specifications: Hardware Specifications to Support 150 Tenants and 7500 Devices
- Choose the Compute+Data persona for three SD-WAN Manager instances. Example: SD-WAN Manager1, SD-WAN Manager2, and SD-WAN Manager3. Choose the Data persona for the other three SD-WAN Manager instances. Example: SD-WAN Manager4, SD-WAN Manager5, and SD-WAN Manager6.

Step 3 Complete the following operations on the first SD-WAN Manager instance:

a) Configure the following using the CLI:

- System IP address
- Site ID
- Service Provider organization name (`sp-organization-name`)
- Organization-name
- Cisco SD-WAN Validator IP address
- VPN 0 Transport/Tunnel interface
- VPN 0 Out-of-band (OOB) interface: Ensure that you assign a static IP address to this interface. Do not enable DHCP.

- VPN 512 Management interface
- Configure only one default route in VPN 0.

b) Enable Multitenancy on Cisco SD-WAN Manager.

c) (Optional) Using the CLI, install the Root CA certificate for SD-WAN Manager1.

Skip this step if you are using a Symantec or Cisco PKI certificate.

d) Complete the following through SD-WAN Manager:

1. Generate a certificate signing request. Refer to the Certificate Management section of the *Cisco Catalyst SD-WAN Getting Started Guide*.
2. After getting the certificate signed, install the certificate.

e) Configure the cluster IP address of the SD-WAN Manager server. Refer to the cluster management section of the *Cisco Catalyst SD-WAN Getting Started Guide*.

Before proceeding to the next step, ensure that the Manager IP Address field on the **Administration** > **Cluster Management** page shows the OOB interface address.

Step 4 Complete the following operations on the second and third SD-WAN Manager instances (SD-WAN Manager2 and SD-WAN Manager3 in the example):

a) Configure the following using the CLI:

- System IP address
- Site ID
- Service Provider organization name (`sp-organization-name`)
- Organization-name
- Cisco SD-WAN Validator IP address
- VPN 0 Transport/Tunnel interface
- VPN 0 Out-of-band (OOB) interface: Ensure that you assign a static IP address to this interface. Do not enable DHCP.
- VPN 512 Management interface

b) (Optional) Using the CLI, install the Root CA certificate for SD-WAN Manager1.

Skip this step if you are using a Symantec or Cisco PKI certificate.

c) Complete the following through the Cisco SD-WAN Manager:

1. Generate a certificate signing request. Refer to the Certificate Management section of the *Cisco Catalyst SD-WAN Getting Started Guide*.
2. After getting the certificate signed, install the certificate.

d) Log in to the SD-WAN Manager web application server. Refer to the Cisco Catalyst SD-WAN Manager How-Tos section of the *Cisco Catalyst SD-WAN Getting Started Guide*.

e) Ping the OOB interfaces on the other two SD-WAN Manager instances and ensure they are reachable.

f) Configure the cluster IP address of the SD-WAN Manager server. Refer to the cluster management section of the *Cisco Catalyst SD-WAN Getting Started Guide*.

Before proceeding to the next step, ensure that the Manager IP Address field on the **Administration** > **Cluster Management** page shows the OOB interface address.

Do not enable multitenancy on SD-WAN Manager2 and SD-WAN Manager3.

Step 5 Log in to the first SD-WAN Manager instance and add the second instance to the cluster.

- The second instance (SD-WAN Manager2 in the example) reboots before being added to the cluster.
- While the second instance is being added to the cluster, on the **Administration** > **Cluster Management** page, the **Configure Status** for the second instance shows **Pending**. You can monitor the System Generated Cluster Sync transaction to check the progress of the adding the second instance to the cluster.
- When the operation is completed, on the **Administration** > **Cluster Management** page, you can view both the first and second instances, and their node personas.

Step 6 Repeat the previous step to add additional SD-WAN Manager instances to the cluster (SD-WAN Manager3 through SD-WAN Manager6 in the example).

Enable multitenancy on SD-WAN Manager

Administrator triggered disaster recovery is supported for multitenant clusters from Cisco Release 20.6.1 or later releases.

After you enable multitenancy on SD-WAN Manager, you cannot migrate it back to single tenant mode.

SD-WAN Manager reboots in multitenant mode and when a provider user logs in to SD-WAN Manager, the provider dashboard appears.

Before you begin

Do not migrate an existing single-tenant SD-WAN Manager into multitenant mode, even if you invalidate or delete all devices from the existing SD-WAN Manager. Instead, download and install a new software image of Cisco Release 20.6.1 or a later release.

Procedure

Step 1 Launch SD-WAN Manager using the URL https://<ip-address>:<port>. Log in as the provider **admin** user.

Step 2 From the SD-WAN Manager menu, choose **Administration** > **Settings** > **Tenancy Mode**. If you are using SD-WAN Manager Release 20.12.x or earlier, click **Edit**.

Step 3 In the Tenancy field, click **Multitenant**.

Step 4 In the **Domain** field, enter the domain name of the service provider (for example, managed-sp.com).

Step 5 Enter a Cluster Id (for example, cluster-1 or 123456).

Step 6 Click **Save**. If you are using SD-WAN Manager Release 20.12.x or earlier, click **Proceed** to confirm that you want to change the tenancy mode.

The Domain and Cluster Id values created in steps 5 and 6 serve as the Provider FQDN. Ensure these values conform to current DNS naming conventions. You cannot modify these values after the configuration is saved. To change these

values, a new SD-WAN Manager cluster needs to be deployed. For more details on provider and tenant DNS requirements, refer to step 3d in Add a new tenant, on page 845.

Add SD-WAN Controller

Follow these steps to add SD-WAN Controller

Procedure

Step 1 Log in to SD-WAN Manager as the provider **admin** user.

Step 2 From the SD-WAN Manager menu, choose **Configuration** > **Devices**.

Step 3 Click **Controllers**.

Step 4 Click **Add Controller**.

Step 5 In the **Add Controller** dialog box, do the following:

a) In the **Controller Management IP Address** field, enter the system IP address of the SD-WAN Controller.
b) Enter the **Username** and **Password** required to access the Cisco SD-WAN Controller.
c) Select the protocol to use for control-plane connections. The default is **DTLS**.
d) If you select **TLS**, enter the port number to use for TLS connections. The default is 23456.
e) Check the **Generate CSR** check box for SD-WAN Manager to create a Certificate Signing Request.
f) Click **Add**.

Step 6 From the SD-WAN Manager menu, choose **Configuration** > **Certificates**.

For the newly added SD-WAN Controller, the Operation Status reads CSR Generated.

a) For the newly added SD-WAN Controller, click **More Options** icon and click **View CSR**.
b) Submit the CSR to the Certificate Authority (CA) and obtain a signed certificate.

Step 7 Install certificate.

a) From the SD-WAN Manager menu, choose **Configuration** > **Certificates**.
b) Click **Install Certificate**.
c) In the **Install Certificate** dialog box, paste the **Certificate Text** or click **Select a file** to upload the certificate file.
d) Click **Install**.

a. SD-WAN Manager installs the certificate on the SD-WAN Controller. SD-WAN Manager also sends the serial number of the certificate to other controllers.

b. On the **Configuration** > **Certificates** page, the **Operation Status** for the newly added SD-WAN Controller reads as **Validator Updated**.

c. On the **Configuration** > **Devices** page, the new controller is listed in the Controller table with the controller type, hostname of the controller, IP address, site ID, and other details. The Mode is set to CLI.

Step 8 Change the mode of the newly added SD-WAN Controller to **Manager Mode** by attaching a template to the device.

a) From the SD-WAN Manager menu, choose **Configuration** > **Templates**.
b) Click **Device Templates**.

In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled as**Device**

c) Find the template to be attached to the SD-WAN Controller.
d) Click **...**, and click **Attach Devices**.
e) In the **Attach Devices** dialog box, move the new controller to the **Selected Device** list and click **Attach**.
f) Verify the Configure Preview and click **Configure Devices**.

1. SD-WAN Manager pushes the configuration from the template to the new controller.
2. In the **Configuration** > **Devices** page, the **Mode** for the SD-WAN Controller shows **Manager Mode**. The new SD-WAN Controller is ready to be used in your multitenant deployment.

Expand a multitenant deployment to support more tenants and tenant devices

As a service provider, suppose you have deployed a cluster to the overlay to support up to 100 tenants and 5000 devices. From Cisco IOS XE Release 17.6.3a, Cisco vManage Release 20.6.3, you can expand the Cisco SD-WAN Manager cluster and add additional Cisco SD-WAN Controllers to the overlay to support up to 150 tenants and 7500 devices.

- Prerequisites to expand a multitenant deployment
- Restrictions for expanding a 3-node cluster to a 6-node cluster
- Expand a 3-node cluster to a 6-node cluster

Prerequisites to expand a multitenant deployment

A multitenant Cisco Catalyst SD-WAN overlay that supports up to 50 tenants and 1000 devices, deployed according to the steps outlined in the Initial Setup for Multitenancy section of this document.

- Expand the existing 3-node Cisco SD-WAN Manager cluster to a 6-node cluster.
- To support up to 100 tenants and 5000 devices, you must have 10 SD-WAN Controllers in the overlay. So, deploy 4 SD-WAN Controllers in addition to the 6 existing SD-WAN Controllers in the overlay.
- To support up to 150 tenants and 7500 devices, you must have 16 SD-WAN Controllers in the overlay. So, deploy 10 SD-WAN Controllers in addition to the 6 existing SD-WAN Controllers in the overlay.
    - Create SD-WAN Controller instances. Refer to the information about deploying an SD-WAN Controller in the Overlay Network Bring-Up Process section of the *Cisco Catalyst SD-WAN Getting Started Guide*.
    - Add Cisco SD-WAN Controllers to the overlay network.
    - You can now add more tenants or allow your existing tenants to add more devices subject to the relevant limits.
    - Starting from Cisco SD-WAN Manager Release 20.13.1, you can expand a single node cluster into 3 or 6 node clusters.

Restrictions for expanding a 3-node cluster to a 6-node cluster

You can only expand a 3-node Cisco SD-WAN Manager cluster to a 6-node Cisco SD-WAN Manager cluster. Expansion of the 3-node cluster to other cluster sizes is not supported.

Expand a 3-node cluster to a 6-node cluster

- To support 100 tenants and 5000 devices: Upgrade the three SD-WAN Manager servers in the existing 3-node cluster to the hardware specifications in the table Hardware Specifications to Support 100 Tenants and 5000 Devices of this document.
- From Cisco IOS XE Release 17.6.3a, Cisco vManage Release 20.6.3, to support 150 tenants and 7500 devices: Upgrade the three SD-WAN Manager servers in the existing 3-node cluster to the hardware specifications in the table Hardware Specifications to Support 150 Tenants and 7500 Devices of this document.

Procedure

Step 1 Download the Cisco vManage Release 20.6.1 or a later release software image from Cisco Software Download.

Step 2 Create three SD-WAN Manager instances (for example, vManage1, vManage2, and vManage3) by installing the downloaded software image file. Refer to the information about deploying an SD-WAN Manager in the Overlay Network Bring-Up Process section of the *Cisco Catalyst SD-WAN Getting Started Guide*.

- Deploy SD-WAN Manager servers having the hardware specifications in the table Hardware Specifications to Support 100 Tenants and 5000 Devices of this document.

  From Cisco IOS XE Release 17.6.3a, Cisco vManage Release 20.6.3, to support 150 tenants and 7500 devices, deploy SD-WAN Manager servers with these hardware specifications: Hardware Specifications to Support 150 Tenants and 7500 Devices of this document.

- Choose the **Data** persona for each SD-WAN Manager instance.

Step 3 Complete the following operations on the first through third SD-WAN Manager instances (vManage1 through vManage3 in the example):

a) Configure the following using the CLI:

- System IP address
- Site ID
- Service Provider organization name (`sp-organization-name`)
- Organization-name
- Cisco SD-WAN Validator IP address
- VPN 0 Transport/Tunnel interface
- VPN 0 Out-of-band (OOB) interface: Ensure that you assign a static IP address to this interface. Do not enable DHCP.
- VPN 512 Management interface

- Configure only one default route in VPN 0.
- Do not enable multitenancy on vManage1 through vManage3.

b) (Optional) Using the CLI, install the Root CA certificate for vManage1.

Skip this step if you are using a Symantec or Cisco PKI certificate.

c) Complete these steps through the SD-WAN Manager:

1. Generate a certificate signing request. Refer to the Certificate Management section of the *Cisco Catalyst SD-WAN Getting Started Guide*.
2. After getting the certificate signed, install the certificate.
3. Log in to the SD-WAN Manager web application server. Refer to the Cisco Catalyst SD-WAN Manager How-Tos section of the *Cisco Catalyst SD-WAN Getting Started Guide*.
4. Ping the OOB interfaces on the other SD-WAN Manager instances and ensure they are reachable.
5. Configure the cluster IP address of the SD-WAN Manager server. Refer to the *Cisco Catalyst SD-WAN Getting Started Guide*.

Before proceeding to the next step, ensure that the Manager IP Address field on the **Administration** > **Cluster Management** page shows the OOB interface address.

Step 4 Log in to SD-WAN Manager on the existing 3-node cluster and add an SD-WAN Manager instance to the cluster.

a. The instance reboots before being added to the cluster.

While the instance is being added to the cluster, on the **Administration** > **Cluster Management** page, the **Configure Status** for the instance shows **Pending**. You can monitor the System Generated Cluster Sync transaction to check the progress of the adding the instance to the cluster.

When the operation is completed, on the **Administration** > **Cluster Management** page, you can view the instance and its node persona listed along with the three SD-WAN Manager instances that were part of the original 3-node cluster.

Step 5 Repeat the previous step and add the remaining SD-WAN Manager instances to the cluster.

Upgrade SD-WAN Controller and Edge Device Software

Use these steps to upgrade all Cisco SD-WAN components to the required software versions for multitenancy support.

We recommend that you upgrade the WAN edge device software in the same maintenance window. If the WAN edge device software is not upgraded within the OMP graceful restart window, traffic may be lost.

Before you begin

Minimum software requirements for SD-WAN Controllers and WAN edge devices:

Device	Software Version
SD-WAN Manager	Cisco vManage Release 20.4.1 or later

Device	Software Version
SD-WAN Validator	Cisco SD-WAN Release 20.4.1 or later
SD-WAN Controller	Cisco SD-WAN Release 20.4.1 or later
Cisco IOS XE Catalyst SD-WAN device	Cisco IOS XE Release 17.4.1 or later

Procedure

Step 1 Upgrade the software on the three SD-WAN Manager instances in the cluster to Cisco vManage Release 20.6.1 or a later release. For more information, refer to the cluster management section of the *Cisco Catalyst SD-WAN Getting Started Guide*.

Skip the step to upgrade the configuration-db service using the command **request nms configuration-db upgrade**.

Step 2 After the SD-WAN Manager software is upgraded to Cisco vManage Release 20.6.1 or a later release, log in to SD-WAN Manager.

Step 3 Upload the Cisco SD-WAN Release 20.6.1 or a later release and the Cisco IOS XE Catalyst SD-WAN Release 17.6.1a or a later release software to SD-WAN Manager. Refer to the information about adding an image to the software repository in the Manage Software and Upgrade section of the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

Step 4 Upgrade the Cisco SD-WAN Validator software to Cisco SD-WAN Release 20.6.1 or a later release.

Refer to:

- Information about upgrading the software image on a device in the Manage Software Upgrade and Repository section of the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*
- Information about activating a new software image in the Manage Software Upgrade and Repository section of the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*

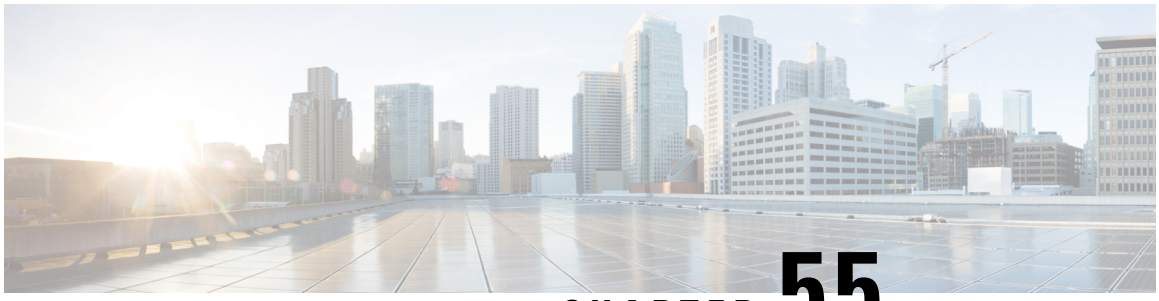
Step 5 Enable maintenance window on SD-WAN Manager. Refer to the information about configuring or canceling an SD-WAN Manager server maintenance window in the Basic Settings for Cisco SD-WAN Manager section of the *Cisco Catalyst SD-WAN Control Components and Device Management Guide*.

Step 6 Upgrade the SD-WAN Controller software to Cisco SD-WAN Release 20.6.1 or a later release.

Step 7 Upgrade the Cisco IOS XE Catalyst SD-WAN device software to Cisco IOS XE Catalyst SD-WAN Release 17.6.1a or a later release.

Refer to:

- Information about upgrading the software image on a device in the Manage Software Upgrade and Repository section of the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*
- Information about activating a new software image in the Manage Software Upgrade and Repository section of the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*



CHAPTER 55

Multitenancy Tenant Management

- Feature history for tenant management, on page 843
- Tenant management, on page 843
- Add a new tenant, on page 845
- Manage tenant WAN edge devices, on page 849
- Manage tenant data, on page 851
- View tenants associated with a Cisco SD-WAN Controller, on page 855
- View OMP statistics per tenant on a Cisco SD-WAN Controller, on page 856

Feature history for tenant management

Developments in tenant management, by release.

Table 312: Feature history

Feature name	Release information	Description
Tenant Device Forecasting	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	With this feature, a service provider can control the number of WAN edge devices a tenant can add to their overlay network. By doing so, the provider can utilize Cisco Catalyst SD-WAN controller resources efficiently.

Tenant management

A tenant or the provider acting on behalf of a tenant can:

- Add WAN edge devices to the tenant network.
- Configure the devices.
- Remove the devices from the tenant network.
- Access the device through the SSH terminal.

Tenant device forecasting

When a service provider adds a new tenant to the multitenant Cisco Catalyst SD-WAN deployment, they can forecast the number of WAN edge devices the tenant may deploy in their overlay network. Cisco SD-WAN Manager enforces this forecast limit. If the tenant tries to add devices beyond this limit, Cisco SD-WAN Manager returns an appropriate error message, and the device addition fails.

From Cisco IOS XE Release 17.6.2 and Cisco vManage Release 20.6.2, you can modify a tenant's device forecast after adding the tenant.

Benefits of tenant device forecasting

- The service provider uses Cisco Catalyst SD-WAN controller resources more efficiently.
- A multitenant deployment supports a fixed number of WAN edge devices across all tenants, depending on the configuration. By forecasting how many devices each tenant may add, the service provider assigns a quota for each tenant from the overall pool of supported edge devices.

Restrictions for tenant management

In a multitenant deployment, a tenant can only add up to 1000 devices to their overlay network.

Each pair of SD-WAN Controllers can serve a maximum of 24 tenants and 1000 tenant devices.

Prerequisites for adding a tenant

Follow these prerequisites to prevent configuration or synchronization failures when adding a tenant.

- Ensure at least two Cisco SD-WAN Controllers are operational and in Manager mode before adding a new tenant.
  - A controller enters Manager mode when a template is pushed from SD-WAN Manager.
  - SD-WAN Controllers in CLI mode cannot serve multiple tenants.
- Ensure that at least two controllers can serve the new tenant. If not, add two controllers and change their mode to Manager.
- When adding a second tenant immediately after another, SD-WAN Manager processes them sequentially, not in parallel.
- Each tenant must have a unique Virtual Account (VA) on Plug and Play Connect within Cisco Software Central. The tenant VA must belong to the same Smart Account (SA) as the provider VA.
- For on-premises deployments, create a **Validator** controller profile for the tenant on Plug and Play Connect.

Table 313: Controller profile fields

Field	Description/Value
Profile Name	Enter a name for the controller profile.
Multitenancy	From the drop-down list, select **Yes**.
SP Organization Name	Enter the provider organization name.

Field	Description/Value
Organization Name	Enter tenant organization in the format <SP Org Name>-<Tenant Org Name>. The organization name can contain up to 50 characters. A mismatch between the controller profile organization name and the tenant organization name causes device synchronization to fail.
Primary Controller	Enter the host details for the primary Cisco SD-WAN Validator.

Add a new tenant

Use these steps to add a new tenant in SD-WAN Manager for multitenancy deployment.

Procedure

Step 1 Log in to SD-WAN Manager as the provider admin user.

Step 2 Navigate to **Administration** > **Tenant Management**.

Step 3 Click **Add Tenant**.

Step 4 Enter tenant information.

Table 314: Tenant information

Item	Description
Tenant Name	Enter a name for the tenant. The name must match the Virtual Account used for the tenant.
Tenant Description	Enter a description with up to 256 alphanumeric characters.
Organization Name	Enter the organization name (case-sensitive, unique per tenant). • Format: <Provider Org Name>-<Tenant Org Name> • Maximum length: 50 characters Example: If the provider organization name is 'EFT20.17-VA-Main – 841534' and the tenant organization name is 'T1', enter the organization name as **`EFT20.17-VA-Main – 841534-T1`**. The tenant organization name can be T1 for Tenant 1, T2 for Tenant 2, and so on.

Step 5 Enter the **URL Subdomain Name**.

Enter the fully qualified subdomain of the tenant.

The URL must include the service provider's domain (example: `customer1.managed-sp.com`) and follow the domain naming convention set in **Administration** > **Settings** > **Tenancy Mode**.

Step 6 Configure DNS.

a) For on-premises deployment, add the tenant's FQDN to DNS and map it to all three SD-WAN Manager cluster IPs.

Provider level:

Create DNS A record and map it to the IP addresses of the SD-WAN Manager instances running in the Cisco SD-WAN Manager cluster. The A record is derived from the domain and cluster ID created while enabling multitenancy.

For example, if domain is `sdwan.cisco.com` and Cluster ID is `vmanage123`, then configure the A record as `vmanage123.sdwan.cisco.com`.

If you do not update the DNS entries, SD-WAN Manager fails to authenticate when you log in. To verify if DNS is configured correctly, execute `nslookup vmanage123.sdwan.cisco.com`.

Tenant level:

Create a DNS CNAME record for each tenant and map it to the FQDN created at the provider level. You do not need to include the cluster ID for the CNAME record.

For example, if the domain is `sdwan.cisco.com` and the tenant name is `customer1`, configure the CNAME record as `customer1.sdwan.cisco.com`.

To verify if DNS is configured correctly, execute **`nslookup customer1.sdwan.cisco.com`**.

b) For a cloud deployment, SD-WAN Manager automatically adds the tenant's fully qualified sub-domain name (FQDN) to DNS during tenant creation. After adding the tenant, it may take up to one hour for the FQDN to resolve.

Step 7 In the **Number of Devices** field, enter the number of WAN edge devices the tenant can deploy.

Adding more devices than allowed will trigger an error.

Step 8 Click **Save**.

When you add a tenant, SD-WAN Manager automatically:

- Creates the tenant.
- Assigns two SD-WAN Controllers to the tenant and pushes a CLI template to configure tenant information on them.
- Sends the tenant and controller details to the SD-WAN Validator.

What to do next

The **Create Tenant** window appears, and the status of the tenant creation reads **In progress**. To view status messages related to the creation of a tenant, click the > button to the left of the status.

After the **Status** column changes to **Success**, you can view the tenant information on the **Administration** > **Tenant Management** page.

View tenant information

From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1, you can view detailed tenant information.

Use these steps to view detailed information about a tenant.

Procedure

Step 1 From Cisco SD-WAN Manager menu, click **Administration** > **Tenant Management**.

Step 2 Click **Tenant** to view detailed tenant information.

Table 315: Tenant details

Field	Description
Tenant Name	Name of the tenant.
Description	Tenant description
Controllers	SD-WAN Controllers assigned to the tenant.
Forecasted Edge Count	Predicted number of WAN edge devices.
Total Edge Count	Total number of both multitenant and single-tenant edge devices.
Multitenant WAN Edge Devices	Click the non-zero number to view the number of multitenant edge devices.
Tenant-Provider VPN Mapping	Click the non-zero number to view tenant and device VPN mappings.
Service Connector	Shows the multitenant edge device that provides VXLAN connectivity to tenants.
Notifications	Indicates whether webhook notifications are managed by the tenant or provider.
AAA	Indicates whether remote AAA is managed by the tenant or provider.
Controller Visibility	Indicates whether controller visibility is enabled or disabled.

Delete a tenant

Before you delete a tenant, delete all tenant WAN edge devices. See Delete a WAN edge device from a tenant network, on page 850.

Use these steps to delete a tenant.

Procedure

Step 1 Log in to Cisco SD-WAN Manager as the provider admin user.

Step 2 From the Cisco SD-WAN Manager menu, choose **Administration** > **Tenant Management**.

Step 3 In the left pane, click the name of the tenant.

The tenant information is displayed in a pane on the right.

Step 4 In the right pane, click the trash icon.

Step 5 In the Delete Tenant dialog box, enter the provider admin password and click **Save**.

Add a tenant in a Cisco-hosted multitenant environment

Use these steps to add a new tenant in a Cisco-hosted multitenant environment.

Procedure

Step 1 Log in to Cisco SD-WAN Manager as the provider admin user.

Step 2 Navigate to **Administration** > **Tenant Management**.

Step 3 Click **Add Tenant**.

Step 4 Enter tenant information.

Table 316: Tenant information

Item	Description
Tenant Name	Enter a name for the tenant.
Tenant Description	Enter a description with up to 256 alphanumeric characters.

Item	Description
Organization Name	Enter the organization name (case-sensitive, unique per tenant). • Format: <SP Org Name>-<Tenant Org Name> • Maximum length: 50 characters Example: If the provider organization name is 'multitenancy' and the tenant organization name is 'Customer1', while adding the tenant, enter the organization name as multitenancy-Customer1. Any mismatch with controller profile causes device sync failure

Step 5 Enter the sub-domain URL in FQDN format.

The sub-domain name must include `sdwan.cisco.com`.

For example, a valid sub-domain could be `Efttl.sdwan.cisco.com`.

Ensure the sub-domain is unique by performing a nslookup or ping on the expected domain. If the domain already exists, choose a different URL.

The tenant's FQDN is automatically added to DNS during the tenant creation process. After adding the tenant, it may take up to one hour for the FQDN to resolve.

Step 6 In the **Number of Devices** field, enter the maximum number of WAN edge devices the tenant can deploy.

Exceeding this limit will cause Cisco SD-WAN Manager to report an error and prevent additional device additions.

Step 7 Choose **Auto placement** or **manual** option for controller assignment.

Step 8 Click Save.

After tenant creation completes, Cisco SD-WAN Manager automatically generates the controller profile in the tenant's Virtual Account and creates the FQDN. You will receive an email notification once the process is finished.

Manage tenant WAN edge devices

Use these procedures to add or delete a WAN edge device from a tenant network.

• Add a WAN edge device to a tenant network
• Delete a WAN edge device from a tenant network

Add a WAN edge device to a tenant network

Register and configure a WAN edge device in SD-WAN Manager for a tenant.

If you are adding a WAN edge device that you had previously invalidated and deleted from an overlay network, you must reset the device software after adding the device.

To reset the software on a Cisco IOS XE Catalyst SD-WAN device, use the command request platform software sdwan software reset.

Procedure

Step 1 Log in to SD-WAN Manager.

- If you are a provider user, log in as **admin**. From the provider dashboard, choose a tenant from the drop-down list to enter the provider-as-tenant view.
- If you are a tenant user, log in as **tenantadmin**.

Step 2 Upload the file containing the device serial numbers to Cisco SD-WAN Manager.

Step 3 Validate the uploaded device and send the details to the controllers.

Step 4 Create a configuration template for the device and attach the device to the template.

Enter the organization-name in the format `<SP Org Name>-<Tenant Org Name>`.

While configuring the device, set the **Service Provider Organization Name** and the **Tenant Organization Name** as shown in the example below:

```
sp-organization-name multitenancy
organization-name multitenancy-Customer1
```

Step 5 Bootstrap the device using the bootstrap configuration generated through SD-WAN Manager, or manually create the initial configuration on the device.

Step 6 If using Enterprise Certificates for authentication, follow these steps:

a) Download the CSR from SD-WAN Manager.
b) Get the CSR signed by the Enterprise CA.
c) Install the certificate on SD-WAN Manager.

Delete a WAN edge device from a tenant network

Follow these steps to remove a WAN Edge device from a tenant's network in SD-WAN Manager.

Procedure

Step 1 Log in to SD-WAN Manager.

- If you are a provider user, log in as **admin**. From the provider dashboard, choose the tenant from the drop-down list to enter the provider-as-tenant view.
- If you are a tenant user, log in as **tenantadmin**.

Step 2 Detach the device from any configuration templates.

Step 3 Delete the device.

Manage tenant data

You can back up, restore, and manage tenant configuration data in SD-WAN Manager.

- Back up tenant data
- Create data backup file
- Restore tenant data backup file
- Monitor data backup restore
- Delete tenant data backup file

Back up tenant data

You can back up configuration data for a tenant in SD-WAN Manager.

The tenant data backup solution of SD-WAN Manager multitenancy provides these functionalities:

- Create, list, and extract configuration backup files.
- Back up configuration database of a specific tenant with an option to restore it later.
- Delete back up files of a tenant stored in SD-WAN Manager.

Usage

Tenant data backup operations can be performed:

- By a tenant administrator in the tenant view.
- By a provider administrator in the provider-as-tenant view.

Allowed backup operations

At any given time, a tenant is allowed to perform only one backup operation. The operation must complete before starting a new one. These operations are supported:

- Back up a single configuration database
- Download the backup file
- Restore or import backup files
- Delete backup files
- List backup files

Limitations

Defines the limitations of provider access for backing up data.

- A provider cannot back up provider data using this solution.
- A provider can back up all tenant information at once only by backing up all tenants' configuration databases using CLI.

View back up data

The tenant data backup solution creates a task in the tenant view of SD-WAN Manager.

Tenants can monitor the progress of the operation from the task view of the tenant dashboard.

Backup and restore guidelines for tenant data

You can enable tenants to securely back up, store, and restore configuration data in Cisco SD-WAN Manager while maintaining consistency and operational limits.

Follow these guidelines for tenant backup and restore operations.

- The tenant backup file follows the format: `Bkup_tenantId_MMDDYY-HHMMSS_taskIdWithoutDash.tar.gz`.
- Backup operation is read-only on the configuration database.
- To ensure data consistency, do not perform major network changes while the operation is in progress.
- Multiple tenants can perform backup and restore operations in parallel.
- A tenant cannot start other backup operations when a restore operation is in progress.
- Backup and restore operations must be performed on Cisco SD-WAN Manager instances running identical software versions.
- A tenant can store a maximum of three backup files in Cisco SD-WAN Manager.

  If three files already exist, the earliest backup file is deleted when a new backup is generated.
- Backup files can also be downloaded and stored outside the Cisco SD-WAN Manager repository.
- Ensure the following parameter values match in both the backup file and the target setup:
  - Tenant ID
  - Organization Name

- SP Organization Name

Create data backup file

To create, verify, extract, and list tenant configuration backup files using Cisco SD-WAN Manager APIs.

Procedure

Step 1 Log in to Cisco SD-WAN Manager.

- If you are a provider user, log in as the **admin**.

  In the provider dashboard, choose a tenant from the drop-down list to enter the **provider-as-tenant** view.
- If you are a tenant user, log in as the **tenantadmin**.

Step 2 Modify the URL path for REST API access.

In the address bar, update the URL path with `dataservice`.

Example:

https://<tenant_URL>/dataservice

Step 3 Create a configuration backup file by using the following API:

https://<tenant_URL>/dataservice/tenantbackup/export.

Step 4 Once the backup file is created, Cisco SD-WAN Manager task view shows the generated process ID.

Example:

{ "processId": "72d69805-b987-436f-9b7a-afef2f3f9061", "status": "in-progress" }

Step 5 Verify the task status.

Use the obtained process ID with the following API, the response provides task details in JSON format.

Example:

https://<tenant_URL>/dataservice/device/action/status/72d69805-b987-436f-9b7a-afef2f3f9061

Step 6 Extract or download the backup file.

After the task completes, the backup file appears under the **data** section of the JSON task file. To extract or download it, use:

`https://<tenant_URL>/dataservice/tenantbackup/download/1570057020772/backup_1570057020772_100919-181838.tar.gz`

Step 7 List available backup files.

Use the following API to list all backup files stored in Cisco SD-WAN Manager.

`https://<tenant_URL>/dataservice/tenantbackup/list`

Restore tenant data backup file

Use these steps to restore tenant data backup file.

Before you begin

To run the restore API, use Postman or an equivalent API testing tool. Postman is used here as an example. You can download it from the Postman website.

Procedure

Step 1 Open Google Chrome or another browser and enable Developer Mode.

Step 2 Log in to Cisco SD-WAN Manager.

- If you're a provider user, log in as the admin and from the provider dashboard, choose a tenant from the drop-down list to enter the provider-as-tenant view.
- If you're a tenant user, log in as the tenantadmin.

Step 3 Get header information for the restore API:

- Click the **Network** tab to view network capture.
- In the network capture view, click the **Name** column to sort listed items.
- Search and click **index.html**.
- Click the **Headers** tab and expand **Request Headers**.
- Copy all text under Request Headers to the clipboard.

Step 4 Open Postman UI to import backup files using Postman:

a) To disable SSL certificate verification, go to **Postman** > **Preferences** > **General** > **Request** and turn off SSL Certificate Verification.
b) Create a new tab.
c) Click **Headers**, then **Bulk Edit**, and paste the copied text from Request Headers.
d) From the GET drop-down, choose **POST**.
e) In the **Request URL** field, enter the tenant URL with the restore API:

```
https://<tenant_URL>/dataservice/tenantbackup/import
```

f) Click the **Body** tab and select **form-data**.
g) Under the KEY column, enter *bakup.tar.gz*
h) Click **Send** to run the API.
i) In the Response section, view the JSON confirmation showing that the file was restored.

Example:

```
{
  "processId": "40adb6c0-eacc-4ad4-ba6c-2c2da2e96d1d",
  "status": "Import Successfully Submitted for tenant 1579026919487"
}
```

Monitor backup data restore

You can monitor the progress of the restoration in either of these ways:

- Use Cisco SD-WAN Manager task view that indicates whether the backup file is imported successfully. You can view the process identifier of the created process or task.

```
{"processId": "40adb6c0-eacc-4ad4-ba6c-2c2da2e96d1d",
    "status": "Import Successfully Submitted for tenant 1579026919487"
}
```

- Use the following URL with the process ID to check status directly:

```
https://<tenant_URL>/dataservice/device/action/status/<processId>
```

Example:

```
https://customer1.managed-sp.com/dataservice/device/action/status/40adb6c0-eacc-4ad4-ba6c-2c2da2e96d1d
```

Delete a tenant

Before you delete a tenant, delete all tenant WAN edge devices. See Delete a WAN edge device from a tenant network, on page 850.

Use these steps to delete a tenant.

Procedure

Step 1 Log in to Cisco SD-WAN Manager as the provider admin user.

Step 2 From the Cisco SD-WAN Manager menu, choose **Administration** > **Tenant Management**.

Step 3 In the left pane, click the name of the tenant.

The tenant information is displayed in a pane on the right.

Step 4 In the right pane, click the trash icon.

Step 5 In the Delete Tenant dialog box, enter the provider admin password and click **Save**.

View tenants associated with a Cisco SD-WAN Controller

Use these steps to view tenants associated with a Cisco SD-WAN Controller.

Procedure

Step 1 Log in to Cisco SD-WAN Manager as the provider admin user.

Step 2 Click a **Controller** connection number to display a table with detailed information about each connection.

Cisco SD-WAN Manager displays a table that provides a summary of the Cisco SD-WAN Controllers and their connections.

Step 3 For a Cisco SD-WAN Controller, click **...** and click **Tenant List**.

Cisco SD-WAN Manager displays a summary of tenants associated with the Cisco SD-WAN Controller.

View OMP statistics per tenant on a Cisco SD-WAN Controller

Use these steps to view OMP statistics per tenant on a Cisco SD-WAN Controller.

Procedure

Step 1 Log in to Cisco SD-WAN Manager as the provider admin user.

Step 2 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

Step 3 In the table of devices, click on the hostname of a Cisco SD-WAN Controller.

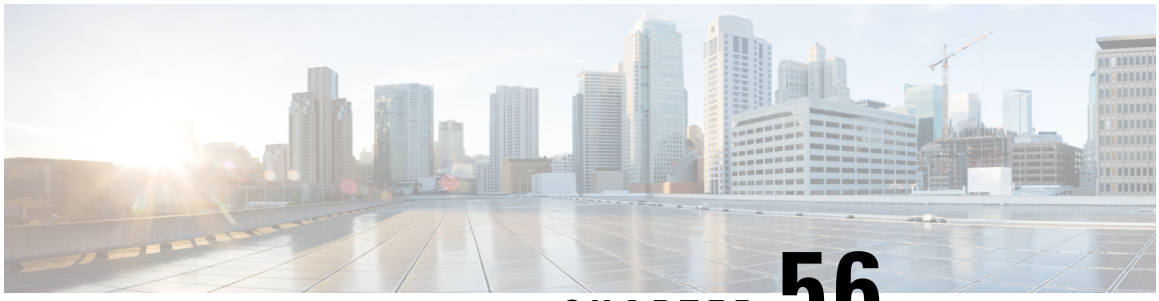
Step 4 In the left pane, click **Real Time**.

Step 5 In the **Device Options** field, enter **OMP** and select the OMP statistics you wish to view.

Step 6 In the **Select Filters** dialog box, click **Show Filters**.

Step 7 Enter the **Tenant Name** and click **Search**.

Cisco SD-WAN Manager displays the selected OMP statistics for the particular tenant.



CHAPTER 56

Multitenant WAN Edge Devices

- Feature history for multitenant WAN edge devices, on page 857
- Multitenant WAN edge devices, on page 858
- Enable multitenant WAN edge device deployment, on page 863
- Onboard WAN edge devices at the provider level using a template, on page 864
- Enable multitenancy on provider-level WAN edge devices using a template, on page 864
- Create a resource profile (tier), on page 865
- Onboard tenants to a multitenant WAN edge device using a template, on page 867
- Create a tenant VPN for onboarded tenants using a template, on page 868
- Remove a tenant from a multitenant WAN edge device using a template, on page 870
- Delete a resource profile (tier), on page 870

Feature history for multitenant WAN edge devices

This table shows the feature history of multitenant WAN edge devices.

Table 317: Feature history

Feature Name	Release Information	Description
Multitenant WAN Edge Devices	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	With this feature, a service provider can deploy, configure, and manage multitenant WAN edge devices in a multitenant Cisco Catalyst SD-WAN deployment.

Feature Name	Release Information	Description
Distribute Device Resources Among Tenants Using Tiers	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	With this feature, you can define tiers and assign tenants to tiers. While defining a tier, you limit the amount of a multitenant WAN edge resource that is allocated to a tenant in the tier, when the tenant is onboarded to a multitenant WAN edge device. From this release, you can specify how many tenant VPNs can be created for a tenant belonging to a tier. In subsequent releases, tiers will be enhanced to support limits on the usage of additional device resources such as firewall, NAT, and TLOCs.
Enhanced Multitenant Tier Definition to include Route and TLOC Resource-Usage Limits	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco vManage Release 20.10.1	This feature is enhanced to support route and TLOC resource-usage limits. A service provider can assign a tier to limit the routes and TLOC resource-usage to the tenant based on the service agreement.
Enhanced Multitenant Tier Definition to include NAT Limits	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	With this feature, you can configure maximum limit on NAT translations per tenant. From this release **Tier** is called **Resource Profile** in Cisco SD-WAN Manager.

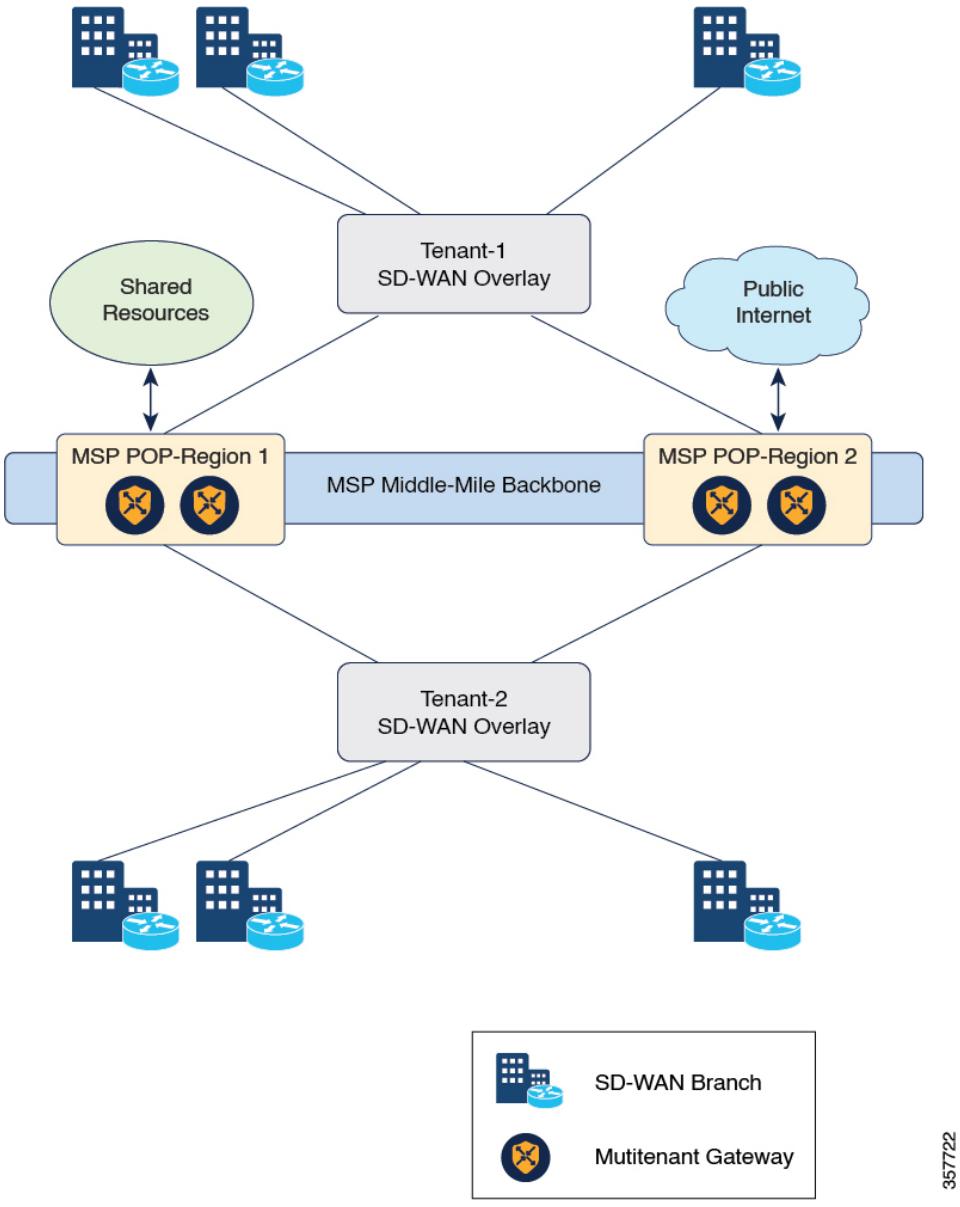
Multitenant WAN edge devices

A multitenant WAN edge device is an edge device in a Cisco Catalyst SD-WAN network that

- operates in a multitenancy environment, and
- can serve multiple tenants.

As a service provider managing a multitenant Cisco Catalyst SD-WAN deployment, you can deploy a multitenant WAN edge device in the overlay network to serve as a shared gateway for traffic belonging to multiple tenants. For example, you can deploy such a shared gateway in each regional point of presence (PoP). You can carry inter-region traffic belonging to multiple tenants through these shared gateways and the transport backbone linking the PoPs.

Figure 8: Multitenant WAN edge devices as shared gateways



Multitenant WAN edge devices isolate traffic belonging to different tenants by mapping a tenant service VPN (referred to as tenant VPN) to a device VPN (also referred to as the device VRF). Cisco SD-WAN Manager performs the mapping between the tenant and device VPNs when you onboard a tenant on a multitenant WAN edge device.

Multitenant WAN edge devices establish control connections with the Cisco SD-WAN Validator nodes specified in the bootstrap configuration, and then connect to nodes in the Cisco SD-WAN Manager cluster. When you onboard a tenant to a multitenant WAN edge device, the device establishes control connections to the Cisco SD-WAN Controller assigned to the tenant.

The service provider must deploy, configure, and manage multitenant WAN edge devices. The devices and their states are displayed only in the Cisco SD-WAN Manager provider view. The provider, acting on behalf

of the tenant, must deploy, configure, and manage single-tenant WAN edge devices owned by a tenant. The devices and their states are displayed in the tenant view or the provider-as-tenant view. When a tenant is onboarded to a multitenant WAN edge device, the multitenant WAN edge device can interoperate with single-tenant WAN edge devices owned by the tenant and other multitenant WAN edge devices to which the tenant is onboarded.

Benefits of multitenant WAN edge devices

These are the benefits of a multitenant WAN edge device.

As a managed service provider, by deploying multitenant WAN edge devices, you can

- reuse the edge devices and the interconnecting transport backbone to serve multiple tenants
- lower capital and operational expenditure
- provide faster access to tenants to shared resources, SaaS, and IaaS through the shared transport backbone, and
- manage tenant association with the devices, tenant-specific policies, and QoS requirements with Cisco SD-WAN Manager as the unified management interface.

Device resource tiers

A device resource tier is a structure for managing multitenant WAN edge devices that defines how much of each device resources a tenant assigned to the tier can consume.

When you onboard many tenants on a multitenant WAN edge device, you may need to distribute the limited device resources among the tenants to ensure fair usage of resources or to implement different service-level agreements (SLAs). A tier lets you define and limit how much of each device resource a tenant assigned to the tier can consume. After creating a tier, when you onboard a tenant, you assign a tenant to a particular tier to apply the resource-usage limits to the tenant.

Usage notes

- After you create a tier, you cannot modify the device-resource-usage limits specified in the tier. To apply a different set of limits to tenants, you must create a new tier and assign the relevant tenants to the new tier.
- You can delete a tier only when no tenants are assigned to it.

Device resource tiers

This section describes the resources governed by tier.

Table 318: Resources governed by tier

Resource usage limit	Description	Available from
Number of VPNs	Maximum number of tenant VPNs that can be created for a tenant belonging to the tier. Cisco SD-WAN Manager enforces the limit when you create a new tenant VPN for a tenant. • If you have already created the maximum number of tenant VPNs specified in the tier, Cisco SD-WAN Manager reports the error and doesn't apply the configuration.	Cisco IOS XE Release 17.8.1 and Cisco vManage Release 20.8.1
Route-limit	The number of IPv4 unicast and IPv6 unicast routes that can be created for a tenant belonging to the tier. Route limit on a tenant is the sum of routes from all VRFs.	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco vManage Release 20.10.1
TLOC	TLOC allows you to map transport interfaces to tenants. At least one TLOC needs to be selected per tier and you can include up to 16 TLOCs in a tier.	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco vManage Release 20.10.1
NAT limit	The maximum limit on the number of NAT translations per tenant. Once the maximum limit has been reached for a tenant, the packets are dropped and further translations are not allowed.	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1

Supported devices for multitenant WAN edge devices

This table describes the devices that can operate as multitenant WAN edge devices.

Table 319: Supported devices

Device family	Model
Cisco ASR 1000 Series Aggregation Services Routers	ASR 1001-HX ASR 1001-X ASR 1002-HX ASR 1002-X **Note** Cisco IOS XE Catalyst SD-WAN Release 17.9.1a is the last supported release for ASR 1001-X and ASR 1002-X.
Cisco Catalyst 8000V Edge Software	Catalyst 8000V
Cisco Catalyst 8300 Series Edge Platforms	C8300-1N1S-4T2X C8300-1N1S-6T C8300-2N2S-4T2X C8300-2N2S-6T
Cisco Catalyst 8500 Series Edge Platforms	C8500-12X C8500-12X4QC C8500L-8S4X
Cisco ISR 4000 Series Integrated Services Routers	ISR 4461

Restrictions for multitenant WAN edge devices

Unsupported services and technologies

Multitenant WAN edge devices do not support these services and technologies:

- Cloud Express and Multicloud workflows
- Zone-Based Firewall (ZBFW) and advanced security features
- Per-tenant DPI statistics
- Dynamic on-demand tunnels
- SNMP
- Per-tenant management of NAT resources
- OMP IPv6 route filtering
- OMP notifications

Provider ownership of devices

The provider must own, deploy, and manage all multitenant WAN edge devices in the deployment. The provider must also deploy and manage any single-tenant device owned by a specific tenant.

Unique system IP addresses

Configure a unique system IP address for each WAN edge device in the multitenant Cisco Catalyst SD-WAN deployment, irrespective of whether the device is a multitenant device owned and managed by the provider or a single-tenant device owned by a tenant and managed by the provider on behalf of the tenant.

Maximum SLA classes

You can configure a maximum of 16 SLA classes. You can either assign specific SLA classes to tenants or share SLA classes among tenants.

Migration of device from the tenant level to be multitenant device

You cannot migrate a single-tenant WAN edge device from the tenant level to serve as a multitenant WAN edge device at the provider level. You must decommission the single-tenant device and delete it from Cisco SD-WAN Manager, perform a factory reset on the device to erase the existing configuration, and onboard the device at the provider level.

Precedence in VRF limits

Tenant limits takes precedence when VRF limits are also configured.

Enable multitenant WAN edge device deployment

Before you begin

Ensure that every WAN edge device in the deployment, across tenants, is configured with a unique system IP address.

Follow these steps to enable multitenant WAN edge deployment.

Procedure

Step 1 Log in to Cisco SD-WAN Manager as the provider admin user.

Step 2 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Step 3 Find **MT Edge Deployment Settings** and click **Edit**.

Step 4 For **Enable MT Edge Deployment**, click **Enabled**.

By default, **Enable MT Edge Deployment** is **Disabled**.

Step 5 Click **Save**.

What to do next

If two or more WAN edge devices in the deployment are configured with the same system IP address, Cisco SD-WAN Manager reports an error. Modify the configuration of the WAN edge devices and try to enable multitenant WAN edge deployment.

Onboard WAN edge devices at the provider level using a template

Before you begin

Follow these steps to onboard WAN edge devices at the provider level.

Procedure

Step 1 Log in to Cisco SD-WAN Manager as the provider admin user.

Step 2 Upload the device serial number file to Cisco SD-WAN Manager. While uploading the file, choose the option to validate and send the device list to controllers.

Step 3 Bootstrap the device using bootstrap configuration generated through Cisco SD-WAN Manager or manually create the initial configuration on the device.

Step 4 If you are using Enterprise Certificates to authenticate the device, download the Certificate Signing Request (CSR) from Cisco SD-WAN Manager and get the CSR signed by the Enterprise CA. Install the certificate on Cisco SD-WAN Manager.

Step 5 Create a configuration template for the device and attach the device to the template.

While configuring the device, configure the service provider organization name as `sp-organization-name` and the tenant `organization-name`.

Enable multitenancy on provider-level WAN edge devices using a template

You can enable multitenancy on a provider-level WAN edge using the Multi Tenant parameter in the System template.

A provider-level WAN edge device can serve more than one tenant.

Before you begin

Follow these steps to enable multitenancy on provider-level WAN edge devices.

Procedure

Step 1 Log in to Cisco SD-WAN Manager as the provider admin user.

Step 2 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 3 Click **Feature**.

Step 4 Find the System template of the provider-level WAN edge device for which you wish to enable multitenancy.

Step 5 For the System template, click **…** and click **Edit**.

Step 6 In the Basic Configuration area, find the **Multi Tenant** parameter. Initially, the parameter has a default scope and the default value **Off**. For the **Multi Tenant** parameter, do this:

a) Click the scope drop-down list and choose **Global** scope.

b) Click **On** to enable multitenancy.

Step 7 Click **Update** to save and apply the modified configuration.

Create a resource profile (tier)

Before you begin

Follow these steps to create a resource profile (previously called a tier).

Procedure

Step 1 Log in to Cisco SD-WAN Manager as the provider admin user.

Step 2 From the Cisco SD-WAN Manager menu, choose **Administration** > **Tenant Management**.

Step 3 Click **Resource Profiles**.

In Cisco vManage Release 20.11.1 and earlier releases, **Resource Profiles** is called **Tiers**.

Any existing tiers are displayed in a table.

Step 4 Click **Add a Resource Profile**.

In Cisco vManage Release 20.11.1 and earlier releases, **Add a Resource Profile** is called **Add Tier**.

Step 5 In the **Add Tier** slide-in pane, do this:

a) Enter these details:

Field	Description
Resource Profile Name In Cisco vManage Release 20.11.1 and earlier releases, **Resource Profile Name** is called **Tier Name**.	Enter a unique name for the tier.
Maximum VPN	Enter the maximum number of VPNs that can be created on a multitenant WAN edge device for a tenant assigned to this tier. Minimum value: 1 Maximum value: The maximum number of VPNs that you can specify for a tier depends on the device model.
NAT Limit (Optional)	Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1 Enter the maximum number of NAT translations that are allowed on each tenant.

Field	Description
Route Limit (Optional)	Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Cisco vManage Release 20.10.1 (Optional) Specify IPv4 unicast or IPv6 unicast route limits. Route limit on a tenant is the sum of routes from all VRFs. Default value is 0. **Note** The value 0 means there is no route limit configured in the tier definition.
Route Limit Type	Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Cisco vManage Release 20.10.1 The following two route limit types can be configured for IPv4 or IPv6 routes on the device: • **Warning-only**: This option allows to install new tenant IPv4 or IPv6 routes even after total exceeds their respective limit. A warning message is shown on device console when IPv4 route limit or IPv6 route limit is exceeded. • **Warning with threshold**: This option allows to configure a warning threshold, which is the percentage of the route limit. A warning message is shown on device console when the threshold percentage of IPv4 route limit or IPv6 route limit is reached. When a tenant's total IPv4 or IPv6 routes exceed the configured IPv4 or IPv6 route limit, routes are rejected.
Threshold	Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Cisco vManage Release 20.10.1 Specify the route limit threshold value when you chose **Warning with threshold** option. When threshold percentage of IPv4 or IPv6 route limit is reached, a warning message is displayed on the device console. Range: 1 to 100.
Allowed Transport In Cisco vManage Release 20.11.1 and earlier releases, **Allowed Transport** is called **TLOC**.	Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Cisco vManage Release 20.10.1 Add TLOC details for the tier. For a tier, add at least one TLOC and up to 16 TLOCs. A TLOC definition includes the TLOC color and the encapsulation type. Range: 1 to 16
Color	Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Cisco vManage Release 20.10.1 Select the color from the drop-down list. The color attribute helps to identify an individual WAN transport tunnel.

Field	Description
Encapsulation	Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Cisco vManage Release 20.10.1 Select encapsulation type as either GRE or IPSec per TLOC configuration.

Table 320: Maximum number of VPNs supported by each device model

Device model	Maximum number of VPNs
ASR1001-X	80
ASR1001-HX	336
ASR1002-X	336
ASR1002-HX	336
C8500-12X4QC	336
C8500-12X	336
C8500L-8S4X	336
C8300-1N1S-6T	200
C8300-1N1S-4T2X	200
C8300-2N2S-6T	200
C8300-2N2S-4T2X	200
Catalyst 8000V	300
ISR4461	80

b) To add the tier, click **Save**. To discard your entries and close the slide-in pane, click **Cancel**.

After you click **Save**, the slide-in pane is closed and the new tier is listed in the table along with any existing tiers.

Onboard tenants to a multitenant WAN edge device using a template

You can onboard tenants to a multitenant WAN edge device using the Tenant template.

- If you haven't onboarded a tenant to the device, create a Tenant template, add tenants, and attach the tenant template to the device template.
- If you have onboarded tenants to the device, to onboard a new tenant, update the existing Tenant template attached to the device.

When you onboard a new tenant to the multitenant WAN edge device, the device establishes control connections to the Cisco SD-WAN Controllers assigned to the tenant.

Before you begin

Before onboarding the tenant to a multitenant WAN edge device, add the tenant to the multitenant deployment and create the tier with which you wish to associate the tenant.

Follow these steps to onboard tenants to a multitenant WAN edge device.

Procedure

Step 1 Log in to Cisco SD-WAN Manager as the provider admin user.

Step 2 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 3 Find the device template for the multitenant WAN edge device to which you are onboarding tenants.

Step 4 For the device template, click **…** and select **Edit**.

The device template is displayed.

Step 5 Click **Additional Templates**.

Step 6 In the **Additional Templates** area, click the **Tenant** template drop-down list and select **Create Template**.

Step 7 In the Tenant template form, do this:

a) Enter a unique template name. The template name can contain up to 128 alphanumeric characters.

b) Enter a description for the template. The description can contain up to 2048 alphanumeric characters.

c) In the **Tenant** area, click **New Tenant**.

d) From the **Tenant Name** drop-down list, select the tenant organization name.

In Cisco vManage Release 20.11.1 and earlier releases, **Tenant Name** is called **Org Name**.

e) From the **Resource Profile Name** drop-down list, select a tier for the tenant.

In Cisco vManage Release 20.11.1 and earlier releases, **Resource Profile Name** is called **Tier Name**.

f) Click **Add**.

g) Repeat these steps to add additional tenants.

Step 8 Click **Save**.

Step 9 For the device template, click **Update** to save and apply the modified configuration.

Step 10 Select the target device in the left pane and click **Configure Devices**.

Create a tenant VPN for onboarded tenants using a template

After onboarding a tenant to a multitenant WAN edge device, use the Cisco VPN template to create tenant VPNs. To isolate VPN traffic of one tenant from the VPN traffic of other tenants onboarded on the multitenant WAN edge device, Cisco SD-WAN Manager maps a tenant VPN ID to a device VPN ID while you create the tenant VPN.

When you attempt to apply the tenant VPN configuration to a device, Cisco SD-WAN Manager checks these:

- Maximum number of tenant VPNs

The number of tenant VPNs that can be created for a tenant is restricted by the maximum number of the VPNs that is specified by the tier to which the tenant belongs. If the maximum number of tenant VPNs is already created for the tenant, Cisco SD-WAN Manager reports an error and does not apply the VPN configuration to the device.

- Maximum number of device VPNs

  Each device model supports a certain maximum number of device VPNs. On a multitenant WAN edge device, each tenant VPN is mapped to device VPN. If the maximum number of device VPNs supported by the device are already created and mapped to tenant VPNs, Cisco SD-WAN Manager reports an error and does not apply the configuration to the device.

Before you begin

Follow these steps to create a tenant VPN for onboarded tenants.

Procedure

Step 1 Log in to Cisco SD-WAN Manager as the provider admin user.

Step 2 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 3 Find the Device template for the multitenant WAN edge device to which you wish to onboard tenants.

Step 4 For the device template, click **…** and select **Edit**.

This displays the device template.

Step 5 Click **Service VPN**.

Step 6 In the **Service VPN** area, click **Add VPN**.

Step 7 In the **Add VPN** slide-in pane, click **Create VPN Template**.

Step 8 In the **Create VPN Template** slide-in pane, do the following:

a) Enter a unique template name. The template name can contain up to 128 alphanumeric characters.

b) Enter a description for the template. The description can contain up to 2048 alphanumeric characters.

c) In the **Basic Configuration** area, map the tenant VPN ID to a device VPN ID:

1. From drop-down list corresponding to **Tenant VPN**, select the tenant organization name.
2. In the text field corresponding to **Tenant VPN**, enter the tenant VPN ID.
3. Click **Generate VPN ID**.

   A read-only **VPN** field displays the device VPN ID for the tenant VPN ID. SD-WAN Manager performs this mapping. For a tenant, SD-WAN Manager maps a particular tenant VPN ID to the same device VPN ID on all the multitenant WAN edge devices.

d) Configure other properties of the tenant VPN in the template.

e) Click **Save**.

Step 9 In the **Add VPN** slide-in pane, move the template created in **Step 8** from **Available VPN Templates** to **Selected VPN Templates**.

Step 10 Click **Next**.

Step 11 Add any additional Cisco VPN templates as needed.

Step 12 Click **Add**.

Step 13 For the device template, click **Update** to save and apply the modified configuration.

Step 14 Select the target device in the left pane and click **Configure Devices**.

Remove a tenant from a multitenant WAN edge device using a template

To remove a tenant from a multitenant WAN Edge Device, you must detach the tenant service VPN template from the device template and delete the tenant from the Tenant template.

Before you begin

Follow these steps to remove a tenant from a multitenant WAN edge device.

Procedure

Step 1 Log in to Cisco SD-WAN Manager as the provider admin user.

Step 2 Remove the tenant service VPN template from the Device template.

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
b) Find the device template for the multitenant WAN edge device to which you wish to onboard tenants.
c) For the device template, click **…** and click **Edit**.

The device template is displayed.

d) Click **Service VPN**.
e) In the **Service VPN** area, check the check box for the VPN template to be removed.
f) Click **Remove VPN**.
g) Click **Update** to save and apply the modified configuration.

Step 3 Delete tenant from the Tenant template.

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
b) Click **Feature**.
c) Find the Tenant template from which you should delete the tenant.
d) For the Tenant template, click **…** and click **Edit**.
e) In the Tenant section, find the organization name of the tenant you wish to delete.
f) Click the Trash icon corresponding to the tenant organization name.
g) Click **Update** to save and apply the modified configuration.

Delete a resource profile (tier)

Before you begin

Follow these steps to delete a tier.

Procedure

Step 1 Log in to Cisco SD-WAN Manager as the provider admin user.

Step 2 From the Cisco SD-WAN Manager menu, choose **Administration** > **Tenant Management**.

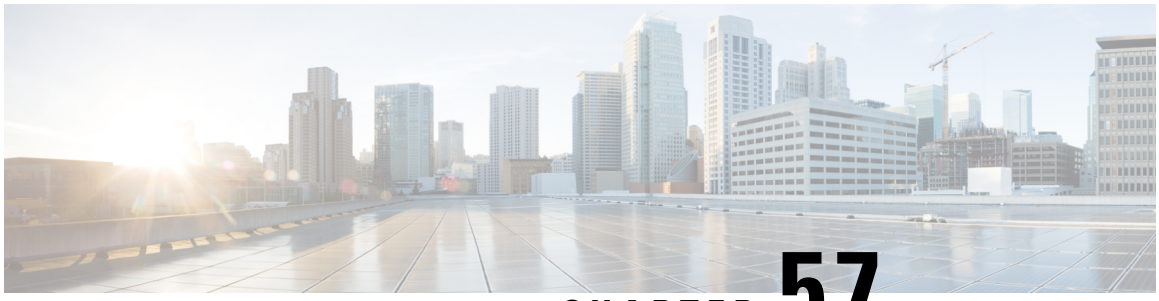
Step 3 Click **Tiers**.

A table displays the existing tiers.

Step 4 For a tier, click **…** in the **Actions** column and select **Delete**.

Step 5 Confirm the deletion.

The tier is deleted and is no longer listed in the table.



CHAPTER 57

Multitenancy Migration

- Feature history for multitenancy migration, on page 873
- Tenant migration in a multitenant deployment, on page 874
- Restrictions for migration of a tenant from a multitenant overlay to a single-tenant deployment, on page 874
- Migrate single-tenant Cisco Catalyst SD-WAN overlay to multitenant Cisco Catalyst SD-WAN deployment, on page 875
- Migrate a tenant from a multitenant Cisco Catalyst SD-WAN overlay to single-tenant Cisco Catalyst SD-WAN deployment, on page 879
- Migrate multitenant Cisco Catalyst SD-WAN overlay, on page 883
- Verify the migration, on page 885

Feature history for multitenancy migration

Table 321: Feature history

Feature name	Release information	Description
Migrate Multitenant Cisco Catalyst SD-WAN Overlay	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature enables you to migrate a multitenant Cisco Catalyst SD-WAN overlay comprising shared Cisco SD-WAN Manager instances and Cisco SD-WAN Validator, and tenant-specific Cisco SD-WAN Controllers to a multitenant overlay comprising shared Cisco SD-WAN Manager instances, Cisco SD-WAN Validator, and Cisco SD-WAN Controllers.

Feature name	Release information	Description
Migration of a tenant from a multitenant overlay to a single-tenant deployment	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	This feature supports the migration of a tenant from a multitenant overlay to a single-tenant deployment. To migrate a tenant between two Cisco Catalyst SD-WAN deployments, move the tenant configurations, statistical data, and WAN edge devices from one deployment to another.

Tenant migration in a multitenant deployment

The tenant migration involves

- export of tenant data from the source Cisco SD-WAN Manager instance, and
- and import of data to the destination Cisco SD-WAN Manager instance.

After the data migration is complete, the tenant WAN edge devices with active control connections with the source Cisco SD-WAN Manager migrate and form connections with the destination Cisco SD-WAN Manager.

Availability

- From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1, migration of a single-tenant overlay to a multitenant deployment is supported only with Cisco Catalyst SD-WAN controllers deployed on-premises.
- From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1, migration of a tenant from a multitenant overlay to a single-tenant deployment is supported.

Restrictions for migration of a tenant from a multitenant overlay to a single-tenant deployment

Defines the restrictions during tenant migration in Cisco Catalyst SD-WAN deployments.

- Change in the tenant organization name is not supported when the tenant moves from the Cisco Catalyst SD-WAN source to destination deployment.
- Tenant migration with multitenant WAN edge devices is not supported.
- Data traffic loss is expected during migration as devices are migrating from one set of SD-WAN Controllers to another.
- All user passwords are set to the default Cisco password on the destination overlay. The default password is `Cisco#123@Viptela`.
- Statistical data of the tenant that can be relearned by destination SD-WAN Manager is not migrated.

- The migration procedure does not support multiple imports on the same destination SD-WAN Manager. Reinitialize the destination SD-WAN Manager to allow import again.

Migrate single-tenant Cisco Catalyst SD-WAN overlay to multitenant Cisco Catalyst SD-WAN deployment

- Prerequisites to migrate single-tenant SD-WAN overlay to multitenant SD-WAN deployment
- Migrate single-tenant SD-WAN overlay to multitenant SD-WAN deployment

Prerequisites to migrate single-tenant SD-WAN overlay to multitenant SD-WAN deployment

Follow these prerequisites to ensure a successful migration.

- Ensure that the edge devices in the single-tenant deployment can reach the SD-WAN Validator in the multitenant deployment
- Ensure that the template, routing, and policy configuration on the edge devices is synchronized with the current configuration on SD-WAN Manager.
- Configure a maintenance window for the single-tenant overlay before performing this procedure.
- We recommend that you use a custom script or a third-party application like Postman to execute the API calls.
- The software versions of the SD-WAN Controllers and WAN edge devices must be identical in both the single-tenant and multitenant deployments.

Minimum software requirements to migrate a single-tenant overlay

Table 322: Software requirements

Device	Software version
Cisco SD-WAN Manager	Cisco vManage Release 20.6.1
Cisco SD-WAN Validator	Cisco SD-WAN Release 20.6.1
Cisco SD-WAN Controller	Cisco SD-WAN Release 20.6.1
Cisco IOS XE Catalyst SD-WAN device	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a

Minimum software requirements for the multitenant deployment to which the single-tenant overlay must be migrated

Table 323: Software requirements

Device	Software version
Cisco SD-WAN Manager	Cisco vManage Release 20.6.1
Cisco SD-WAN Validator	Cisco SD-WAN Release 20.6.1
Cisco SD-WAN Controller	Cisco SD-WAN Release 20.6.1
Cisco IOS XE Catalyst SD-WAN device	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a

Migrate single-tenant SD-WAN overlay to multitenant SD-WAN deployment

Migration of a single-tenant overlay to a multitenant deployment is only supported with the SD-WAN Controllers deployed on-premises. Migration is yet to be supported with cloud-hosted SD-WAN Controllers.

Procedure

Step 1 Export the single-tenant deployment and configuration data from a SD-WAN Controller instance controlling the overlay.

While exporting the data, SD-WAN Controller attempts to detach any CLI templates from the edge devices in preparation for the migration to the multitenant deployment. If prompted by SD-WAN Manager, detach CLI templates from the edge devices and execute the export API call again.

Method	`POST`
URL	`https://ST-vManage-IP-address`
Endpoint	`/dataservice/tenantmigration/export`
Authorization	Admin user credentials.

Body	Required Format: Raw JSON `{ "desc": <tenant_description>, "name": <tenant_name>, "subdomain": <tenant_name>.<domain>, "orgName": <tenant_orgname > }` Field Description: • `desc`: A description of the tenant. The description can be up to 256 characters and can contain only alphanumeric characters. • `name`: Unique name for the tenant in the multitenant deployment. • `subdomain`: Fully qualified sub-domain name of the tenant. The sub-domain name must include the domain name of the service provider. For example, if `managed-sp.com` is the domain name of service provider, and the tenant name is `Customer1`, the tenant sub-domain name would be `customer1.managed-sp.com`. • `orgName`: Name of the tenant organization. The organization name is case-sensitive.
Response	Format: JSON `{ "processId": <vManage_process_ID>, }`

Step 2 Check the status of the data export task in SD-WAN Manager.

When the task succeeds, download the data using the URL
`https://ST-vManage-IP-address/dataservice/tenantmigration/download/default.tar.gz`

Step 3 Import the data exported from the single-tenant overlay, on a multitenant SD-WAN Manager instance.

When the task succeeds, on the multitenant Cisco SD-WAN Manager, you can view the devices, templates, and policies imported from the single-tenant overlay.

Method	`POST`
URL	`https://MT-vManage-IP-address`
Endpoint	`/dataservice/tenantmigration/import`
Authorization	Provider admin user credentials.

Body	**Required** Format: form-data Key Type: File Value: `default.tar.gz`

Response	Format:
	JSON
	{
	"processId": <vManage_process_ID>,
	"migrationTokenURL": <token_URL>,
	}

Step 4 Obtain the migration token using the token URL obtained in response to the API call in step 3.

Method	`GET`
URL	`https://MT-vManage-IP-address`
Endpoint	`migrationTokenURL` obtained in **Step 3**.
Authorization	Provider Admin user credentials.
Response	The migration token as a large blob of encoded text.

Step 5 On the single-tenant SD-WAN Manager instance, initiate the migration of the overlay to the multitenant deployment.

Method	`POST`
URL	`https://ST-vManage-IP-address`
Endpoint	`dataservice/tenantmigration/networkMigration`
Authorization	Admin user credentials.
Body	**Required** Format: Raw text Content: Migration token obtained in Step 4.

Response	Format: JSON
	{
	"processId": <vManage_process_ID>,
	}

As part of the migration task, the address of the multitenant Cisco SD-WAN Validator, and the service provider and tenant organization names are pushed to the WAN edge devices of the single-tenant overlay.

If the task succeeds, WAN edge devices form control connections to controllers in the multitenant deployment; the WAN edge devices are no longer connected to the controllers of the single-tenant overlay.

What to do next

In SD-WAN Manager, check the status of the migration task.

Attach any CLI templates detached from the edge devices (in Step 1) after migration to the multitenant deployment. Before you attach the templates, update the Cisco SD-WAN Validator IP address and the Organization name to match the configuration of the multitenant deployment.

In the single-tenant deployment, if Cisco SD-WAN Manager-signed certificates are installed on cloud-based WAN edge devices, the certificates are cleared when the devices are migrated to the multitenant deployment.

You must re-certify the devices on the multitenant SD-WAN Manager. If enterprise certificates are installed on the cloud-based WAN edge devices, the certificates are not affected by the migration.

Migrate a tenant from a multitenant Cisco Catalyst SD-WAN overlay to single-tenant Cisco Catalyst SD-WAN deployment

- Prerequisites to migrate a tenant from a multitenant SD-WAN overlay to single-tenant SD-WAN deployment
- Migrate a tenant from a multitenant SD-WAN overlay to single-tenant SD-WAN deployment

Prerequisites to migrate a tenant from a multitenant SD-WAN overlay to single-tenant SD-WAN deployment

Ensure these prerequisites are met for a successful migration.

- Manually migrate the serial number of the WAN edge device associated to a virtual account on the source Cisco SD-WAN Manager overlay in Cisco PNP to the destination virtual account.
- Ensure that you manually create the controller profile on the destination virtual account for on-prem to on-prem or cloud to on-prem deployments.
- Ensure that the source and destination Cisco SD-WAN Manager instances use the same Certificate Authority (CA) and software release; a mismatch can block tenant data import and cause migration failure.
- Ensure that you check the CPU, memory, and disk size requirements of the destination overlay Cisco SD-WAN Controller before the migration to meet the WAN edge forecast requirements.
- Ensure that there is no overlap between the configured system IP addresses of edge devices and the destination overlay controllers.
- Ensure that all devices in a tenant have connectivity to the Cisco SD-WAN Validator in the destination single-tenant overlay. The migration procedure supports a Cisco SD-WAN Validator on the single-tenant deployment configured either with IP or DNS.

  Push any required static route configuration to the devices before initiating any of the migration steps.
- Ensure that there are valid control connections from Cisco SD-WAN Manager to the WAN edge devices in the source overlay.

Configuration

- Ensure that the destination single-tenant Cisco SD-WAN Manager does not have any configurations before migration. You can configure only mandatory admin settings and all other configurations can be done after data import.
- Configure a maintenance window for the multitenant overlay before performing this procedure. Refer to the information about configuring a maintenance window in the basic settings section of the *Cisco Catalyst SD-WAN Control Components and Device Management Guide*.
- Ensure that the WAN edge devices that are configured using CLI, device template, or configuration groups, have an IP host mapping to the Cisco SD-WAN Validator in the destination single-tenant overlay.
- We recommend that you use a custom script or a third-party application like Postman to execute the API calls.

Migrate a tenant from a multitenant SD-WAN overlay to single-tenant SD-WAN deployment

Use these steps to migrate a tenant from a multitenant SD-WAN overlay to single-tenant SD-WAN deployment.

Procedure

Step 1 Export the multitenant deployment configuration and statistical data from a Cisco SD-WAN Manager instance controlling the source overlay.

Method	`POST`
URL	`https://MT-vManage-IP-address`
Endpoint	`/dataservice/tenantmigration/export`
Authorization	Administrator user credentials.

Body	Required Format: Raw JSON Example: `{ "name": "tenant1", "desc": "This is tenant1", "orgName": "vIPtela Inc MT to ST Migration Regression-Tenant1 Inc", "subDomain": "tenant1.mtreg.com", "wanEdgeForecast": 100, "migrationKey="tenant1TenantMigrationKey123", "isDestinationOverlayMT": false }` Field descriptions: **Note** Ensure that the `name`, `desc`, `orgName`, `subdomain`, and `wanEdgeForecast` match the tenant you wish to migrate. • `name`: Unique name for the tenant in the multitenant deployment. The name should be between 8-32 characters and can contain only alphanumeric characters. • `desc`: Description of the tenant. The description can be up to 256 characters and can contain only alphanumeric characters. • `orgName`: Name of the tenant organization. The organization name is case-sensitive. • `subdomain`: Fully qualified sub-domain name of the tenant. The sub-domain name must include the domain name of the service provider. For example, if `managed-sp.com` is the domain name of service provider, and the tenant name is `Customer1`, the tenant sub-domain name would be `customer1.managed-sp.com`. • `wanEdgeForecast`: Number of WAN edge devices that the tenant can deploy. • `migrationKey`: Migration key which is used to encrypt sensitive data during migration. The migration key should be between 8-32 characters and can contain only alphanumeric characters. • `isDestinationOverlayMT`: Boolean variable which specifies if the migration is happening to a multitenant overlay or not.
Response	Format: JSON `{ "processId": <vManage_process_ID>, }`

Step 2 Check the status of the data export task in SD-WAN Manager When the task is successfully complete, download the data from the following URL: `https://MT-vManage-IP-address/dataservice/tenantmigration/download/default.tar.gz`

Step 3 Import the data to the single-tenant instance, as follows:

a) Execute the following API:

Method	`POST`
URL	`https://ST-vManage-IP-address`

Endpoint	`/dataservice/tenantmigration/import/{migrationKey}` Use the same migration key specified earlier.
Authorization	Provider administrator user credentials.
Body	Required Format: form-data Key Type: File Value: `default.tar.gz`

Response	Format:
	JSON
	`{`
	`"processId": <vManage_process_ID>,`
	`"migrationTokenURL": <token_URL>,`
	`}`

b) When the task is complete, on the single-tenant SD-WAN Manager you can view the devices, templates, and policies imported from the multitenant overlay.

Step 4 After the import, update information related to the device templates, policies, and other deployment-specific parameters.

a) Check and update the administrator settings as some of the administrator settings specific to the source overlay are not exported. The import does not override the administrator settings that are already configured in destination SD-WAN Manager.

Step 5 If a centralized policy is present on the source tenant, the migration copies the policy to the destination overlay.

We recommend creating Cisco SD-WAN Controller templates and attaching them to the devices. Apply the centralized policy to devices in the destination overlay before proceeding.

Step 6 Obtain the migration token using the token URL from the previous step.

Method	`GET`
URL	`https://ST-vManage-IP-address`
Endpoint	`migrationTokenURL` obtained in the previous step.
Authorization	Provider administrator user credentials.
Response	The migration token as a large encoded text.

Step 7 On the multitenant SD-WAN Manager instance, initiate the migration of the overlay to the single-tenant deployment.

Method	`POST`
URL	`https://MT-vManage-IP-address`
Endpoint	`dataservice/tenantmigration/networkMigration`
Authorization	Administrator user credentials.
Body	Required Format: Raw text Content: Migration token obtained in the previous step.

Response	Format: JSON
	{
	"processId": <vManage_process_ID>,
	}

When the task succeeds, WAN edge devices form control connections to controllers in the single-tenant deployment; the WAN edge devices are no longer connected to the controllers of the multitenant overlay.

What to do next

In SD-WAN Manager, check the status of the migration task.

After the migration is successfully complete, perform the following tasks:

- If WAN edge devices have SD-WAN Manager signed certificates in the source setup, the certificates are cleared from the device during migration and control connections are lost. Recertify the devices in the destination.
- The passwords are updated to the default password in the destination overlay for users created on a tenant in the source overlay. Make any configuration changes specific to the destination overlay.
- Delete the tenant on the source overlay after migration and verification is complete.

Migrate multitenant Cisco Catalyst SD-WAN overlay

- Restrictions for migrating multitenant Cisco Catalyst SD-WAN overlay
- Migrate multitenant Cisco Catalyst SD-WAN overlay

Restrictions for migrating multitenant Cisco Catalyst SD-WAN overlay

Defines restrictions for migrating a multitenant Cisco Catalyst SD-WAN overlay.

- This migration procedure applies only to SD-WAN Controllers deployed on premises.
- The multitenant overlay can only be migrated to a setup in which Cisco SD-WAN Manager instances run Cisco vManage Release 20.6.1 software and SD-WAN Controllers run Cisco SD-WAN Release 20.6.1 software.
- This migration procedure cannot be used to merge two or more multitenant overlays. Only one multitenant overlay can be migrated to the new setup at a time.

Migrate multitenant Cisco Catalyst SD-WAN overlay

Before you begin

Minimum software requirements for SD-WAN Controllers and WAN edge devices in the multitenant overlay to be migrated:

Device	Software version
Cisco SD-WAN Manager	Cisco vManage Release 20.3.3
Cisco SD-WAN Validator	Cisco SD-WAN Release 20.3.3
Cisco SD-WAN Controller	Cisco SD-WAN Release 20.3.3
Cisco IOS XE Catalyst SD-WAN device	Cisco IOS XE Release 17.3.3

Procedure

Step 1 Upgrade the software on the three SD-WAN Manager instances in the cluster to Cisco vManage Release 20.6.1.

Refer to the cluster management section of the *Cisco Catalyst SD-WAN Getting Started Guide*.

Run the **request nms configuration-db upgrade** command on only one of the SD-WAN Manager instances.

Step 2 After the SD-WAN Manager software is upgraded to Cisco vManage Release 20.6.1, log in to the SD-WAN Manager.

You're prompted to set a new password. Enter a new password that adheres to the password guidelines.

Step 3 Upload the Cisco SD-WAN Release 20.6.1 software to SD-WAN Manager.

Refer to the information about adding an image to the software repository in the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

Step 4 Upgrade the Cisco SD-WAN Validator software to Cisco SD-WAN Release 20.6.1.

Refer to the information about upgrading the software image of a device in the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

Step 5 Create two SD-WAN Controllers instances running Cisco SD-WAN Release 20.6.1 software.

Refer to the information about deploying an SD-WAN Controller in the *Cisco Catalyst SD-WAN Getting Started Guide*.

With two SD-WAN Controller instances, you can support up to 24 tenants. To support up to 50 tenants, create six SD-WAN Controller instances.

Step 6 Add Cisco SD-WAN Controllers to the overlay network.

The Provider Dashboard shows the new SD-WAN Controller running Cisco SD-WAN Release 20.6.1 software.

The Tenant Dashboard shows the older SD-WAN Controller running Cisco SD-WAN Release 20.3.3 software.

Step 7 Enable the maintenance window on SD-WAN Manager. For more information, see Configure or Cancel SD-WAN Manager Server Maintenance Window.

Refer to the information about configuring a maintenance window in the basic settings section of the *Cisco Catalyst SD-WAN Control Components and Device Management Guide*.

A maintenance window of 3 to 4 hours is recommended.

Step 8 Migrate the tenant configuration from the older tenant-specific SD-WAN Controller running Cisco SD-WAN Release 20.3.3 software to the new shared SD-WAN Controller running Cisco SD-WAN Release 20.6.1 software.

Method	`POST`

URL	`https://<vmanageip>:<port>`
Endpoint	`dataservice/tenant/vsmart-mt/migrate`
Authorization	Provider **admin** user credentials.
Body	Required Format: Raw JSON `{}`
Response	Format: JSON `{ "processId": <vManage_process_ID>, }`

Step 9 Upgrade the Cisco IOS XE Catalyst SD-WAN device software to Cisco IOS XE Catalyst SD-WAN Release 17.6.1a.

Refer to the information about upgrading the software image on a device, and about activating a new software image, in the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

It is not necessary to upgrade the tenant WAN edge device software in the same maintenance window in which you migrate the multitenant overlay. However, we recommend that you upgrade the tenant WAN edge device software within a few weeks of the migration.

During the migration task, the following changes are affected:

1. The older SD-WAN Controllers are invalidated and deleted from the overlay network.
2. In the tenant view, the older SD-WAN Controllers are removed from the Tenant Dashboard, and the Devices and the Certificates page.
3. The tenant WAN edge devices are connected to the new SD-WAN Controller.

What to do next

In SD-WAN Manager check the status of the migration task using the `processId` from the API response.

Verify the migration

Use these steps to verify multitenant migration.

Procedure

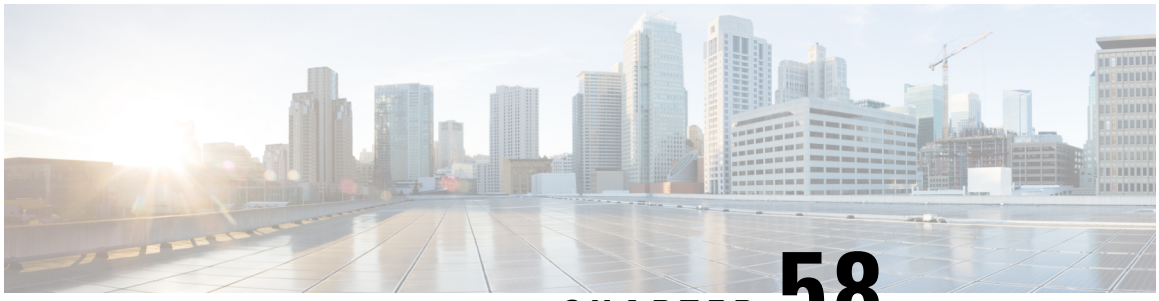
Step 1 In the provider view, perform these checks:

a) From the **Main Dashboard** page, verify whether the tenant WAN edge devices are connected to the new multitenant SD-WAN Controllers.

b) View tenants associated with a Cisco SD-WAN Controller, on page 855.

c) On the SD-WAN Controller CLI, run the command **show control connections**. In the command output, verify that control connections are established between the SD-WAN Controller and the tenant WAN edge devices.

Step 2 In the provider-as-tenant view, verify whether the multitenant SD-WAN Controllers appear on the **Tenant Dashboard**.



CHAPTER 58

Multitenancy Disaster Recovery

- Disaster recovery for a multitenant Cisco SD-WAN Manager cluster, on page 887
- Disaster recovery in an overlay network with virtual routers, on page 892
- Disaster recovery after a failed data center becomes operational, on page 896
- Replace faulty SD-WAN Controller, on page 897

Disaster recovery for a multitenant Cisco SD-WAN Manager cluster

Summary

If a Multitenant Cisco SD-WAN Manager cluster or the data center hosting the SD-WAN Manager nodes in the cluster fail, you can recover from the failure by activating a standby SD-WAN Manager cluster. You can perform disaster recovery as follows:

Workflow

1. Deploy and configure a standby SD-WAN Manager cluster.

   The standby SD-WAN Managercluster is not part of the overlay network and is not active.

2. Back up the configuration database of the active SD-WAN Manager cluster periodically.

   Choose a SD-WAN Manager node in the cluster that hosts the configuration database service and back up the configuration database.

3. If the active SD-WAN Manager cluster fails, restore the most recent configuration database on the standby SD-WAN Manager cluster, activate the standby SD-WAN Manager cluster, and remove the previously active CSD-WAN Manager cluster from the overlay network.

4. Choose a SD-WAN Manager node in the cluster that hosts the configuration database service and restore the configuration database backed up from the previously active SD-WAN Manager cluster.

What's next

To test disaster recovery, you can simulate a scenario in which the active SD-WAN Manager cluster fails. One way to simulate such a failure would be by disabling the tunnel interface as described in this document.

Prerequisites for a multitenant disaster recovery

Follow these prerequisites for a successful migration.

- The number of SD-WAN Manager nodes in the active and standby clusters must match.
- Each SD-WAN Manager node in the active and standby clusters must run the same SD-WAN Manager software release.
- Each SD-WAN Manager node in the active and standby clusters must connect to the WAN transport IP address of the SD-WAN Validator in the overlay network.
- Initially, disable the tunnel interfaces of the SD-WAN Manager nodes in the standby cluster.
- Certify the SD-WAN Manager nodes in the standby cluster.
- Synchronize the clock of every SD-WAN Manager node in the standby cluster with the clocks of the SD-WAN Controller and WAN edge devices in the overlay network. If NTP is configured on the overlay, configure the same on the standby SD-WAN Manager nodes.
- Use identical Neo4j credentials on the SD-WAN Manager nodes in the active and standby clusters.

Restrictions for a multitenant disaster recovery

Defines restrictions to backup and restore process during disaster recovery of a SD-WAN Manager cluster.

- Do not interrupt any active processes while backing up the configuration database.
- Enable SD-AVC before restoring the configuration database on the standby SD-WAN Manager node.

Configure a standby SD-WAN Manager cluster

To prepare standby SD-WAN Manager nodes with a unique yet synchronized configuration for disaster recovery without impacting the active overlay network.

Procedure

Step 1 Configure the standby SD-WAN Manager nodes with a running configuration similar to the active SD-WAN Manager nodes and install local certificates.

The running configuration on a standby node is usually identical to an active node, but ensure settings such as system IP address and tunnel interface IP address are unique.

Step 2 On the standby nodes, shut down the transport interface in VPN 0 using the CLI shutdown command in the transport interface configuration.

Step 3 Create a standby cluster using the configured standby SD-WAN Manager nodes.

Step 4 With this configuration, the overlay network remains unaware of the standby SD-WAN Manager cluster.

Back up the active SD-WAN Manager cluster configuration

Back up the full configuration database of the active Cisco vManange cluster periodically. Additionally, take snapshots of the active SD-WAN Manager virtual machines.

Procedure

Step 1 Choose an active SD-WAN Manager node that hosts the configuration database service.

Step 2 On the CLI of the selected node, run the following command to back up the configuration database: **request nms configuration-db backup path <file-path>**

The command saves the configuration database as a `.tar.gz` file in the specified file path.

Example:

In the example below, the database is backed up to a file named db_backup.tar.gz in the /home/admin/ directory.

```
Active-vManage#
request nms configuration-db backup path /home/admin/db_backup
Successfully saved database to /home/admin/db_backup.tar.gz
```

Step 3 Choose a standby SD-WAN Manager node that hosts the configuration database service and copy the configuration database backup to this node.

Example:

In the following example, db_backup.tar.gz is copied from the active SD-WAN Managernode to the /home/admin/ directory of a standby SD-WAN Manager node.

```
Active-vManage#
request execute vpn 512 scp /home/admin/db_backup.tar.gz admin@10.126.93.92:/home/admin
The authenticity of host '10.126.93.92 (10.126.93.92)' can't be established.
ECDSA key fingerprint is SHA256:jTjJWQ0UNHvlrBUxWzNjd8mUz819gPf51MeopsgDlAc.
Are you sure you want to continue connecting (yes/no)?
yes
Warning: Permanently added '10.126.93.92' (ECDSA) to the list of known hosts.
viptela 18.4.5

admin@10.126.93.92's password:
db_backup.tar.gz                              100%  399KB   4.4MB/s   00:00
```

Restore SD-WAN Manager cluster using the configuration database backup

Restore the most recent backup of the configuration database from the active SD-WAN Manager cluster on the standby SD-WAN Manager node to which the backup was copied.

- The restore operation does not restore all configuration details. Settings such as users and repositories must be configured on the standby SD-WAN Manager node after restoring the backup.
- When you complete the steps that follow, the previously active SD-WAN Manager nodes cannot be reused. To reuse the nodes, you must perform additional steps that are beyond the scope of this document.

Procedure

Step 1 On the CLI of the standby SD-WAN Manager node, run the following command: r**equest nms configuration-db restore path** *file-path*.

Example:

In the following example, the configuration database is restored using the backup file db_backup.tar.gz.

```
Standby-vManage#
request nms configuration-db restore path /home/admin/db_backup.tar.gz
Configuration database is running in a standalone mode
Importing database...Successfully restored database
```

Step 2 Verify standby SD-WAN Manager nodes.

a) Verify that all appropriate services are running on each standby SD-WAN Manager node.

On the CLI of each standby node, run: **request nms all status**

From the command output, confirm that the necessary services are active.

b) Verify that every standby node maintains a list of all active and standby SD-WAN Manager nodes:

1. From the SD-WAN Manager, navigate to **Configuration** > **Devices** > **Controllers**.
2. Confirm that the page displays all active and standby SD-WAN Manager nodes.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed **Control Components** to align with Cisco Catalyst SD-WAN rebranding.

Step 3 On the standby SD-WAN Manager nodes, enable the transport interface on VPN 0 using one of these two methods:

a) Enable the transport interface in VPN 0: On the CLI of each standby SD-WAN Manager node, run the **no shutdown** command.

Example:

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# no shutdown
Active-vManage(config-interface)# commit and-quit
```

b) Activate the tunnel interface in VPN 0: On the CLI of each standby SD-WAN Manager node, run the **tunnel-interface** command.

Example:

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# tunnel-interface
Active-vManage(config-interface)# commit and-quit
```

Step 4 Add each standby SD-WAN Manager node to the overlay network.

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
b) Click **Controllers**.
c) For a SD-WAN Validator, click **...** and click **Edit**.
d) In the **Edit** dialog box, enter the following details of the SD-WAN Validator: WAN transport IP address, username, and password.

e) Repeat **Step 4c** and **Step 4d** for every SD-WAN Validator.

Step 5 Disconnect the active SD-WAN Manager nodes from the overlay network using one of these methods.

a) Shut down the transport interface in VPN 0: On the CLI of each active SD-WAN Manager node, run the **shutdown** command.

Example:

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# shutdown
Active-vManage(config-interface)# commit and-quit
```

b) Deactivate the tunnel interface in VPN 0: On the CLI of each active SD-WAN Manager node, run the **no tunnel-interface** command.

Example:

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# no tunnel-interface
Active-vManage(config-interface)# commit and-quit
```

In a lab environment, where you are simulating a disaster scenario, you can perform this step. However, if you cannot reach SD-WAN Manager instances in an actual disaster scenario, you may not be able to perform this step and can omit the step.

Step 6 From the standby SD-WAN Manager send the updated controller and device list to the SD-WAN Validator, including the list of controllers:

a) From the SD-WAN Manager menu, choose **Configuration** > **Certificates**.
b) Click **Controllers**.
c) Click **Send to Validator**.

Wait for the configuration task to complete. When the task is complete,

- The standby SD-WAN Manager nodes become the active Cisco SD-WAN Manager nodes.
- The previously active SD-WAN Manager nodes are no longer part of the overlay network.
- The active SD-WAN Manager nodes have the configuration from the most recent configuration database backup.
- Every controller establishes connection with the other controllers in the network.

d) Click **WAN Edge List.**
e) Click **Send to Controllers**.

Step 7 Verify configuration and connectivity

a) Verify that policies, templates, and the controller and WAN edge device lists are intact.
b) Verify valid SD-WAN Manager nodes:

1. On each SD-WAN Validator, log in to the CLI and run: **show orchestrator** *valid-vmanage-id*.
2. Confirm that the chassis numbers of the active and previously active Cisco SD-WAN Manager nodes are listed.
3. On a WAN edge device, log in to the CLI and run: **show control** *valid-vmanage-id*.
4. Confirm that the chassis numbers of the active and previously active SD-WAN Manager nodes are listed.

5. Check that the device is connected to the active Cisco SD-WAN Manager nodes and the Cisco Catalyst SD-WAN Controller.

Step 8 Invalidate the previously active SD-WAN Manager nodes.

After you invalidate the SD-WAN Manager, the nodes cannot be reused without performing additional steps that are beyond the scope of this document.

a) From the SD-WAN Manager menu, choose **Configuration** > **Certificates**.
b) Click **Controllers**.
c) For each previously active SD-WAN Manager node, click **...** and click **Invalidate**.

Verify the valid SD-WAN Manager nodes

Procedure

Step 1 Log in to the CLI of each SD-WAN Validator and run the **show orchestrator valid-vmanage-id** command.

In the command output, verify that the chassis numbers of only the active SD-WAN Manager nodes are listed.

Step 2 Log in to the CLI of WAN edge device and run the **show control valid-vmanage-id** command.

In the command output, verify that the chassis numbers of only the active SD-WAN Manager nodes are listed. Also, check whether the device is connected to the active SD-WAN Manager nodes and the Cisco Catalyst SD-WAN Controller.

Disaster recovery in an overlay network with virtual routers

The following disaster recovery procedure applies to an overlay network in which Cisco vEdge Cloud routers are deployed at branch locations.

Summary

If a Multitenant SD-WAN Manager cluster or the data center hosting the SD-WAN Manager nodes in the cluster fail, you can recover from the failure by activating a standby SD-WAN Manager cluster. You can perform disaster recovery as follows:

Workflow

1. Deploy and configure a standby SD-WAN Manager cluster.

   The standby SD-WAN Manager cluster is not part of the overlay network and is not active.

2. Back up the configuration database of the active SD-WAN Manager cluster periodically.

   Choose a SD-WAN Manager node in the cluster that hosts the configuration database service and back up the configuration database.

3. If the active SD-WAN Manager cluster fails, restore the most recent configuration database on the standby SD-WAN Manager cluster, activate the standby SD-WAN Manager cluster, and remove the previously active SD-WAN Manager cluster from the overlay network.
4. Choose a SD-WAN Manager node in the cluster that hosts the configuration database service and restore the configuration database backed up from the previously active SD-WAN Manager cluster.
5. To test disaster recovery, you can simulate a scenario in which the active SD-WAN Manager cluster fails. One way to simulate such a failure would be by disabling the tunnel interface as described in this document.

What's next

See these sections, before you proceed.

- Restrictions for a multitenant disaster recover
- Prerequisites for a multitenant disaster recovery
- Configure a standby SD-WAN Manager cluster
- Back up the active SD-WAN Manager cluster configuration

Restore SD-WAN Manager cluster using the configuration database backup

Restore the most recent backup of the configuration database from the active SD-WAN Manager cluster on the standby SD-WAN Manager node to which you copied this backup.

- The restore operation does not restore all the information included in the configuration database. SD-WAN Manager configurations such as users and repositories must be configured on the standby SD-WAN Manager node after the configuration database is restored using the backup.
- When you complete the steps that follow, the previously active SD-WAN Manager nodes cannot be reused. To reuse the nodes, you must perform additional steps that are beyond the scope of this document.

Procedure

Step 1 On the CLI of the standby SD-WAN Manager node, run the following command: **request nms configuration-db restore path** *file-path*

Example:

In the following example, the configuration database is restored using the backup file db_backup.tar.gz.

```
Standby-vManage# request nms configuration-db restore path /home/admin/db_backup.tar.gz
Configuration database is running in a standalone mode
Importing database...Successfully restored database
```

Step 2 Verify services and node list on the standby SD-WAN Manager nodes

a) Verify that the appropriate services are running on the standby SD-WAN Manager nodes: On the CLI of each standby SD-WAN Manager node, run the **request nms all status** command.

From the command output, verify the services running on the node.

b) Verify that every standby SD-WAN Manager node has a list of all the active and standby SD-WAN Manager nodes.

1. From the SD-WAN Manager menu, choose **Configuration** > **Devices** > **Controllers**.
2. Verify that the page displays all active and standby SD-WAN Manager nodes.

Step 3 Run these commands:

a) Log in to the CLI of each Cisco SD-WAN Validator and run the **show orchestrator valid-vmanage-id** command.

b) Log in to the CLI of Cisco vEdge Cloud router and run the **show control valid-vmanage-id** command.

In the command output, verify that the chassis numbers of the active and previously active SD-WAN Manager nodes are listed.

Step 4 Enable the transport interface on VPN 0 on the standby SD-WAN Manager nodes using either of the following methods:

a) Enable the transport interface in VPN 0: On the CLI of each standby SD-WAN Manager node, run the **no shutdown** command.

Example:

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# no shutdown
Active-vManage(config-interface)# commit and-quit
```

b) Activate the tunnel interface in VPN 0: On the CLI of each standby SD-WAN Manager node, run the **tunnel-interface** command.

Example:

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# tunnel-interface
Active-vManage(config-interface)# commit and-quit
```

Step 5 Add each standby SD-WAN Manager node to the overlay network.

a) From the SD-WAN Manager menu, choose **Configuration** > > **Devices**.

b) Click **Controllers**.

c) For a Cisco SD-WAN Validator, click **...** and click **Edit**.

a) In the **Edit** dialog box, enter the following details of the Cisco SD-WAN Validator: WAN transport IP address, username, and password.

b) Repeat **Step 5c** and **Step 5d** for every Cisco SD-WAN Validator.

Step 6 Disconnect the active SD-WAN Manager nodes from the overlay network using one of the following two methods.

a) Shut down the transport interface in VPN 0: On the CLI of each active SD-WAN Manager node, run the **shutdown** command.

Example:

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# shutdown
Active-vManage(config-interface)# commit and-quit
```

b) Deactivate the tunnel interface in VPN 0: On the CLI of each active SD-WAN Manager node, run the **no tunnel-interface** command.

Example:

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# no tunnel-interface
Active-vManage(config-interface)# commit and-quit
```

Step 7 From the standby SD-WAN Manager, send the updated controller and device list to the Cisco SD-WAN Validator.

a) From the SD-WAN Manager menu, choose **Configuration** > **Certificates** .
b) Click **Controllers**.
c) Click **Send to Validator**.

Wait for the configuration task to complete. When the task is complete,

- The standby SD-WAN Manager nodes become the active SD-WAN Manager nodes.
- The previously active SD-WAN Manager nodes are no longer part of the overlay network.
- The active SD-WAN Manager nodes have the configuration from the most recent configuration database backup.
- Every controller establishes connection with the other controllers in the network.

d) Click **WAN Edge List**.
e) Click **Send to Controllers**.

Step 8 Verify configuration and connectivity.

a) Verify that policies, templates, and the controller and WAN edge device lists are intact.
b) Verify valid SD-WAN Manager nodes:

1. Log in to the CLI of each Cisco SD-WAN Validator and run the **show orchestrator valid-vmanage-id** command.
2. Log in to the CLI of a Cisco vEdge Cloud router and run the **show control valid-vmanage-id** command.
3. In the command output, verify that the chassis numbers of the active and previously active SD-WAN Manager nodes are listed.
4. Check whether the device is connected to the active SD-WAN Manager nodes and the Cisco Catalyst SD-WAN Controller.

Step 9 Invalidate the previously active SD-WAN Manager nodes.

a) From the SD-WAN Manager menu, choose **Configuration** > **Certificates**.
b) Click **Controllers**.
c) For each previously active SD-WAN Manager node, click **...** and click **Invalidate**.

a. The previously active SD-WAN Manager is the certificate issuer for the cloud WAN edge devices. The active SD-WAN Manager issues certificates to the cloud WAN edge devices only after the previously active SD-WAN Manager nodes are invalidated.

b. After you invalidate the SD-WAN Manager nodes, the nodes cannot be reused without performing additional steps that are beyond the scope of this document.

c. When you invalidate the previously active SD-WAN Manager nodes, SD-WAN Manager marks the nodes as invalid and sends an update to all controllers. However, SD-WAN Manager does not send an updated list of valid SD-WAN Manager UUIDs to Cisco SD-WAN Validator immediately because the previously active SD-WAN Manager is the CA for the cloud WAN edge devices. So, the output of the **show orchestrator valid-vmanage-id** command on a Cisco SD-WAN Validator includes the UUIDs of the invalidated SD-WAN Manager nodes.

d. SD-WAN Manager has a scheduled task that runs every 24 hours and checks to see if all the cloud WAN edges have been moved to the active SD-WAN Manager. SD-WAN Manager sends the updated list of valid SD-WAN Manager UUIDs to Cisco SD-WAN Validator only after the cloud WAN edge devices have been moved to the active SD-WAN Manager. After this list is received, the output of the **show orchestrator valid-vmanage-id** command on a Cisco SD-WAN Validator does not include the UUIDs of the invalidated SD-WAN Manager nodes.

What to do next

To verify SD-WAN Manager nodes, see Verify the valid SD-WAN Manager nodes.

Disaster recovery after a failed data center becomes operational

This procedure applies to a scenario in which an initially active SD-WAN Manager cluster or the data center hosting the cluster failed and the standby SD-WAN Manager cluster was configured to be the active SD-WAN Manager cluster. If the cluster that was initially active becomes operational again, it serves as a standby cluster. By completing the following procedure, you can turn this standby cluster into the active cluster.

Summary

If a Multitenant SD-WAN Manager cluster or the data center hosting the SD-WAN Manager nodes in the cluster fail, you can recover from the failure by activating a standby SD-WAN Manager cluster. You can perform disaster recovery as follows:

Workflow

1. Deploy and configure a standby SD-WAN Manager cluster.

   The standby SD-WAN Manager cluster is not part of the overlay network and is not active.

2. Back up the configuration database of the active SD-WAN Manager cluster periodically.

   Choose a SD-WAN Manager node in the cluster that hosts the configuration database service and back up the configuration database.

3. If the active SD-WAN Manager cluster fails, restore the most recent configuration database on the standby SD-WAN Manager cluster, activate the standby SD-WAN Manager cluster, and remove the previously active SD-WAN Manager cluster from the overlay network.

4. Choose a SD-WAN Manager node in the cluster that hosts the configuration database service and restore the configuration database backed up from the previously active SD-WAN Manager cluster.

5. To test disaster recovery, you can simulate a scenario in which the active SD-WAN Manager cluster fails. One way to simulate such a failure would be by disabling the tunnel interface as described in this document.

What's next

- Back Up the Active Cisco SD-WAN Manager Cluster Configuration
- Restore Cisco SD-WAN Manager Cluster Using the Configuration Database Backup

Replace faulty SD-WAN Controller

To replace a faulty SD-WAN Controller with a new instance, follow these steps:

Procedure

Step 1 Create a SD-WAN Controller instance.

Step 2 Add the SD-WAN Controller to the overlay network.

Step 3 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.

Step 4 Click **Controllers**.

Step 5 For the faulty SD-WAN Controller, click **...** and click **Invalidate**.

The **Invalidate** dialog box appears.

If you have not added a new SD-WAN Controller that can replace the faulty SD-WAN Controller, Cisco SD-WAN Manager indicates this through an error message. Click **Cancel** in the **Invalidate** dialog box and add a new SD-WAN Controller before invalidating the faulty instance.

Step 6 In the **Invalidate** dialog box, do the following:

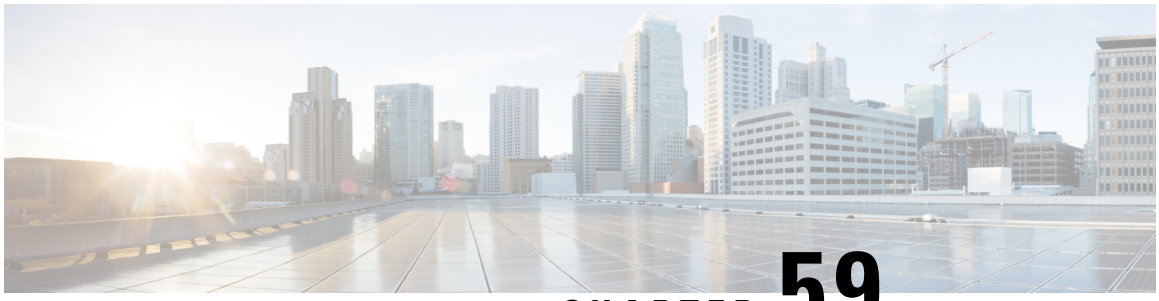
a) Check the **Replace Controller** check box.

b) From the **Select Controller** drop-down list, choose the new SD-WAN Controller that should replace the faulty instance.

c) Click **Invalidate**.

SD-WAN Manager launches the Invalidate Device and Push CLI Template Configuration task. When these tasks are completed, the faulty SD-WAN Controller is invalidated and removed from the overlay network.

The tenants that were served by the faulty SD-WAN Controller are now served by the new SD-WAN Controller that you chose as the replacement.



CHAPTER 59

Multitenancy Dashboard

- Cisco SD-WAN Manager dashboard for multitenancy, on page 899
- View Cisco SD-WAN Validator health dashlet, on page 900
- View Cisco SD-WAN Manager health dashlet, on page 900
- View Cisco SD-WAN Controller health dashlet, on page 900
- View multitenant WAN edge health dashlet, on page 900
- View tenant activity, device, and network information, on page 901
- View detailed information of a tenant setup, on page 901
- View all network connections in the tenant overlay network, on page 902
- View information about device reboots, on page 902
- View state of data connections for a site, on page 902
- View interface usage for WAN edge interfaces, on page 903
- View WAN edge device counts, on page 903
- View aggregated state of WAN edge devices, on page 903
- View WAN edge device loss, latency, and jitter, on page 904
- View SAIE flow information of WAN edge devices, on page 904
- View tunnels data, on page 904
- View tenant alarms in provider dashboard, on page 905
- View tenant events in provider dashboard, on page 905
- View OMP statistics per tenant on a Cisco SD-WAN Controller, on page 905
- View tenants associated with a SD-WAN Controller, on page 906

Cisco SD-WAN Manager dashboard for multitenancy

Cisco SD-WAN Manager multitenant dashboard is a portal where the provider or tenant can view and provision the underlying system.

After enabling SD-WAN Manager for multitenancy, you can view the multitenant dashboard when you log in to SD-WAN Manager, under **Monitor** > **Overview**.

In Cisco vManage Release 20.6.1 and earlier, information related to the **Monitor** > **Devices** page can be viewed under the **Monitor** > **Network** page.

The bar at the top of every SD-WAN Manager multitenant screen includes icons that allow smooth navigation.

View Cisco SD-WAN Validator health dashlet

You can view the state of each Cisco SD-WAN Validator in the **Validator Health** dashlet on the **Monitor Overview** dashboard. This dashlet displays the cumulative state of the Cisco Catalyst SD-WAN Validators within a selected time window, along with the number of Validators in each state.

You can filter the dashlet view based on health status using the drop-down list for **Good Devices**, **Fair Devices**, and **Poor Devices**, as well as for **CPU Load**.

You can use the **View Details** option to access a detailed table view of device health on the **Monitor** > **Devices** page.

View Cisco SD-WAN Manager health dashlet

You can view the state of the SD-WAN Manager in the **Manager Health** dashlet on the **Monitor Overview** dashboard. This dashlet displays the health status of the SD-WAN Manager.

You can filter the dashlet view based on health status using the drop-down list for **Good Devices**, **Fair Devices**, and **Poor Devices**, as well as for **CPU Load**.

You can use the **View Details** option to access a detailed table view of device health on the **Monitor** > **Devices** page.

View Cisco SD-WAN Controller health dashlet

You can view the list of tenants hosted on a particular device by clicking the **Controller bar**.

You can view the state of each SD-WAN Controller in the **Controller Health** dashlet on the **Monitor Overview** dashboard. This dashlet displays the cumulative state of the SD-WAN Controller within a selected time window, along with the number of controllers in each state.

You can filter the dashlet view based on health status using the drop-down list for **Good Devices**, **Fair Devices**, and **Poor Devices**, as well as for **CPU Load**.

You can use the **View Details** option to access a detailed table view of device health on the **Monitor** > **Devices** page.

View multitenant WAN edge health dashlet

You can view the state of each WAN edge device in the **Multi Tenant WAN Edge Health** dashlet on the **Monitor Overview** dashboard. This dashlet displays the cumulative state of the devices within a selected time window, along with the number of WAN edge devices in each state.

You can view the list of tenants hosted on a particular device by clicking the multitenant WAN edge device bar. You can filter the dashlet view based on health status using the drop-down list for **Good Devices**, **Fair Devices**, and **Poor Devices**, as well as for **CPU Load**.

You can use the **View Details** option to access a detailed table view of device health on the **Monitor** > **Devices** page.

View tenant activity, device, and network information

To provide administrators with an overview and detailed insights into tenant, device, and network status in a multitenant Cisco SD-WAN environment.

When you log in to a multitenant SD-WAN Manager as an administrator, the Provider Dashboard displays the following components.

- Device pane: Runs across the top of the multitenant dashboard screen. It displays the number of active SD-WAN Controllers, SD-WAN Validators, and SD-WAN Manager instances, along with the connectivity status of devices and information on certificates that have expired or are about to expire.
- Tenants pane: Displays the total number of tenants and a summary of the control status, site health, router health, and SD-WAN Controller status for all tenants.
- Table of tenants in the overlay network: Lists individual tenants with separate information on control status, site health, WAN edge device health, and SD-WAN Controller status for each tenant.

Use these steps to display tenant specific status summary information:

To return to the provider dashboard from other SD-WAN Manager screens, click **Dashboard**.

Procedure

Step 1 Click a tenant name from the tenant list.

A dialog box opens on the right side of the screen that provides additional information about the status of the tenant.

Step 2 Click **Tenant name** > **Dashboard**, to access the tenant dashboard.

SD-WAN Manager switches to the provider-as-tenant view and displays the tenant dashboard.

Step 3 Click **Provider** at the top of the page, to return to the provider view.

Step 4 Click the tenant name from the tenant list, to close the dialog box.

Step 5 To return to the provider dashboard from other SD-WAN Manager screens, click **Dashboard**.

View detailed information of a tenant setup

Cisco SD-WAN Manager displays the tenant dashboard, which provides information about a tenant deployment in the following scenarios:

- When a **provider admin** user selects a specific tenant from the **Select Tenant** drop-down list in the provider dashboard. This view is referred to as the provider-as-tenant view.
- When a **tenantadmin** user logs in to SD-WAN Manager. This view is referred to as the tenant view.

View all network connections in the tenant overlay network

The Device pane runs across the top of the tenant dashboard and displays the number of control connections from SD-WAN Manager to the SD-WAN Controllers and routers in a tenant's overlay network.

For each WAN edge device, the device pane shows:

- Total number of control connections between SD-WAN Controllers and WAN edge devices
- Number of valid control connections between SD-WAN Controllers and WAN edge devices
- Number of invalid control connections between SD-WAN Controllers and WAN edge devices

You can use a connection number or the Up/Down arrow to view a table with detailed information about each connection, and use the **More Actions** icon at the right of each table row to access additional options.

You can also use the **More Actions** icon at the right of each table row to access the **Device Dashboard** or **Real Time view** from the **Monitor** > **Devices** screen, or the **Tools** > **SSH Terminal** screen.

View information about device reboots

The **Reboot pane** displays the total number of device reboots in the last 24 hours for all devices in the network. It includes soft and cold reboots, as well as reboots caused by power-cycling a device.

For each reboot, the following information is listed:

- System IP and hostname of the device that rebooted.
- Time of the device reboot.
- Reason for the device reboot.

If the same device reboots multiple times, each reboot is reported separately.

You can use the **Reboot pane** opens the **Reboot** dialog box. In the dialog box, the **Crashes** tab lists information for all device crashes, including:

- System IP and hostname of the device on which the crash occurred.
- Crash index of the device.
- Core time when the device crashed.
- File name of the device crash log.

View state of data connections for a site

The **Site Health** pane displays the state of data connections for a site. For sites with multiple WAN edge devices, the pane shows the state for the entire site rather than individual devices.

The Site Health pane includes three connectivity states:

- Full WAN Connectivity: Total number of sites where all BFD sessions on all routers are in the up state.

- Partial WAN Connectivity: Total number of sites where some tunnels or BFD sessions on routers are down, but limited data plane connectivity remains.
- No WAN Connectivity: Total number of sites where all BFD sessions on all routers are down, resulting in no data plane connectivity.

You can view a table with detailed information about each site, node, or tunnel in the **Site Health** dialog box.

The **More Actions** icon at the right of each table row provides access to the **Device Dashboard**, or **Real Time view** from the **Monitor** > **Devices** screen, or the **Tools** > **SSH Terminal** screen.

View interface usage for WAN edge interfaces

The **Transport Interface Distribution** pane displays interface usage for the last 24 hours for all WAN edge interfaces in VPN 0, including all TLOC interfaces.

You can view detailed interface usage information in the **Transport Interface Distribution** dialog box.

View WAN edge device counts

The **WAN Edge Inventory** pane provides four WAN edge device counts:

- Total: Total number of authorized serial numbers for WAN edge devices uploaded on SD-WAN Manager. The serial number is uploaded on the **Configuration** > **Devices** screen.
- Authorized: Total number of authorized WAN edge devices in the overlay network. These devices are marked as 'Valid' in the **Configuration** > **Certificates** > **WAN Edge List** screen.
- Deployed: Total number of deployed WAN edge devices. These devices are marked as 'Valid' and are operational in the network.
- Staging: Total number of WAN edge devices configured at a staging site before they become part of the overlay network. These devices do not participate in routing decisions and do not affect network monitoring through SD-WAN Manager.

You can view hostname, system IP, site ID, and other details of each router in the **WAN Edge Inventory** dialog box.

View aggregated state of WAN edge devices

The **WAN Edge Health** pane provides an aggregated view of the state of WAN edge devices by showing the number of devices in each state, reflecting the overall health of the hardware nodes.

The three WAN edge device states are:

- Normal: Number of WAN edge devices with memory, hardware, and CPU in a normal state. Using less than 70% of total memory or CPU is classified as 'Normal'.
- Warning: Number of WAN edge devices with memory, hardware, or CPU in a warning state. Using between 70% and 90% of total memory or CPU is classified as 'Warning'.

- Error: Number of WAN edge devices with memory, hardware, or CPU in an error state. Using more than 90% of total memory or CPU is classified as 'Error'.

You can view a table displaying the last 12 or 24 hours of memory usage, CPU utilization, and hardware-related alarms (such as temperature, power supply, and PIM modules) by selecting a number or device state in the pane.

Use the **More Actions** icon at the right of each row in the table to access the following:

- Hardware Environment
- Real Time view from the **Monitor** > **Network** screen.

  Tools > **SSH Terminal** screen.

View WAN edge device loss, latency, and jitter

The **Transport Health** pane displays the aggregated average loss, latency, and jitter for all links and all combinations of colors (for example, LTE-to-LTE links or LTE-to-3G links).

You can use the **Type** drop-down arrow to select **loss**, **latency**, or **jitter**, and adjust the time period to display the relevant transport health data.

The **Transport Health** dialog box provides a more detailed view, with the **Details** tab displaying the information in a tabular format. You can also change the displayed health type and time period from this dialog box.

View SAIE flow information of WAN edge devices

The **Top Applications** pane displays SD-WAN Application Intelligence Engine (SAIE) flow information for traffic transiting routers in the overlay network.

SAIE flow information is available for the last 24 hours. To view data beyond this period, you must check the information for the specific device.

You can select a time period and a VPN from the respective drop-down lists to display SAIE flow information for all flows in that VPN. The **Top Applications** dialog box provides a more detailed view of the same information, allowing changes to the VPN and time period.



Note In Cisco vManage Release 20.7.x and earlier, SAIE flow information is referred to as deep packet inspection (DPI).

View tunnels data

The **Application-Aware Routing** pane allows selection of tunnel criteria from the **Type** drop-down arrow:

- Loss
- Latency

- Jitter

Based on the selected criteria, the pane displays the 10 worst tunnels. For example, selecting **Loss** shows the 10 tunnels with the highest average loss over the last 24 hours.

A graphical representation of the data can be viewed for each tunnel, with the option to select a time period or specify a custom time period.

The **Application-Aware Routing** dialog box provides a more detailed view, displaying the 25 worst tunnels based on the chosen criteria: **Loss**, **Latency**, or **Jitter**.

View tenant alarms in provider dashboard

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.16.1a and Cisco Catalyst SD-WAN Manager Release 20.16.1

Procedure

Step 1 Log in to Cisco SD-WAN Manager as the provider admin user.

Step 2 From the SD-WAN Manager menu, choose **Operated as Provider** > **Provider** > **Logs**.

Step 3 In the **Alarms** tab, toggle **View tenant alarms**.

Step 4 Optional: Filter alarms using **Advanced Filter** based on Tenant, Object Type, Object List, Severity, and Type.

Step 5 Optional: Click the bell icon on top to view all the notifications for tenant's alarms.

View tenant events in provider dashboard

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.16.1a and Cisco Catalyst SD-WAN Manager Release 20.16.1

Procedure

Step 1 Log in to Cisco SD-WAN Manager as the provider admin user.

Step 2 From the Cisco SD-WAN Manager menu, choose **Operated as Provider** > **Provider** > **Logs**.

Step 3 In the **Events** tab, toggle **View tenant** events.

Step 4 Optional: Filter events using **Advanced Filter** based on Tenant, Object Type, Object List, Severity, and Type.

View OMP statistics per tenant on a Cisco SD-WAN Controller

To view OMP statistics for a specific tenant on a selected SD-WAN Controller.

Procedure

Step 1 Log in to Cisco SD-WAN Manager as the provider admin user.
Step 2 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
Step 3 In the table of devices, click on the hostname of a SD-WAN Controller.
Step 4 In the left pane, click **Real Time**.
Step 5 In the **Device Options** field, enter `OMP` and select the OMP statistics you wish to view.
Step 6 In the **Select Filters** dialog box, click **Show Filters**.
Step 7 Enter the Tenant Name and click **Search**.

Cisco SD-WAN Manager displays the selected OMP statistics for the particular tenant.

View tenants associated with a SD-WAN Controller

Use these steps to view detailed connection information and the list of tenants associated with a SD-WAN Controller.

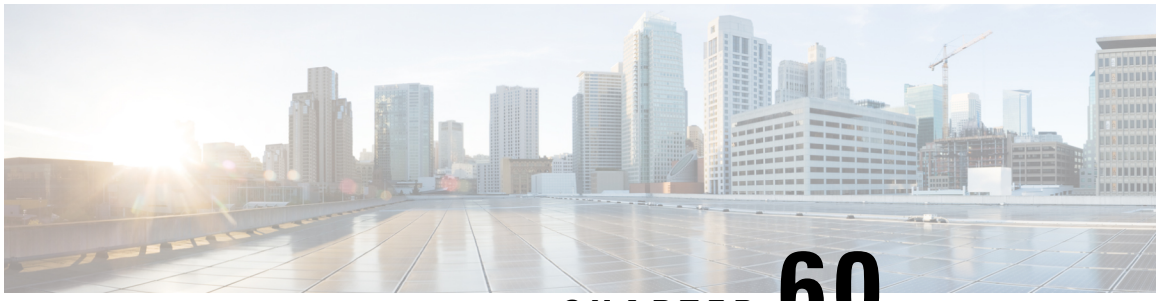
Procedure

Step 1 Log in to Cisco SD-WAN Manager as the provider admin user.
Step 2 Click a **Controller** connection number to display a table with detailed information about each connection.

Cisco SD-WAN Manager displays a table that provides a summary of the SD-WAN Controller and its connections.

Step 3 For a SD-WAN Controller, click **...** and click **Tenant List**.

Cisco SD-WAN Manager displays a summary of tenants associated with the SD-WAN Controller.



CHAPTER 60

Assigning SD-WAN Controllers to Tenants in a Multitenancy Environment

- Feature history for assigning Cisco SD-WAN Controllers to tenants, on page 907
- Multitenancy, on page 907
- Benefits of automatic tenant placement on multitenant SD-WAN Controllers, on page 909
- Restrictions for automatic tenant placement on multitenant SD-WAN Controllers, on page 909
- Prerequisites for automatic tenant placement on multitenant SD-WAN Controllers, on page 910
- Assign SD-WAN Controllers to tenants during onboarding, on page 911
- Update SD-WAN Controller placement for a tenant , on page 913

Feature history for assigning Cisco SD-WAN Controllers to tenants

Table 324: Feature history

Feature name	Release information	Description
Flexible tenant placement on multitenant Cisco Catalyst SD-WAN Controllers	Cisco vManage Release 20.9.1	With this feature, while onboarding a tenant to a multitenant deployment, you can choose the pair of multitenant Cisco SD-WAN Controllers that serve the tenant. After onboarding a tenant, you can migrate the tenant to a different pair of multitenant Cisco SD-WAN Controller, if necessary.

Multitenancy

Multitenancy is a Cisco SD-WAN deployment model that

- allows multiple tenants to share the same Cisco SD-WAN infrastructure,

- assigns dedicated logical resources (such as controllers and organization names) to each tenant for isolation, and
- supports automatic or flexible placement of Cisco SD-WAN Controllers during tenant onboarding.

Types of multitenancy assignments

There are two types of multitenancy assignments in Cisco SD-WAN:

- Automatic tenant placement: Cisco SD-WAN Manager automatically assigns controllers to tenants using an internal algorithm during onboarding.
- Manual tenant placement: You can manually select the pair of SD-WAN Controllers for a tenant based on utilization and resource availability.

Manual tenant placement

With manual tenant placement, you can select controller pairs during onboarding, view controller capacity (such as tenants, edge devices, CPU, and memory), and migrate tenants or add SD-WAN Controllers to optimize utilization.

Availability and configuration

From Cisco vManage Release 20.9.1, you can use manual tenant placement as an optional feature. By default, SD-WAN Manager performs automatic tenant placement, but you can enable manual placement to gain more control during onboarding.

SD-WAN Controller capacity limits

A multitenant SD-WAN Controller supports up to 24 tenants and 1000 tenant WAN edge devices across all tenants. During onboarding, the network administrator must select a pair of SD-WAN Controllers that can host one more tenant and connect to the tenant's forecasted number of WAN edge devices.

Optimization and migration

If a tenant adds more devices than forecast and the assigned SD-WAN Controllers cannot support them, the network administrator migrates the tenant to another SD-WAN Controller pair that has capacity. If no SD-WAN Controller pair has enough capacity, the network administrator migrates other tenants to different SD-WAN Controllers to free up resources and balance utilization. If this optimization still doesn't create enough capacity, the network administrator adds a new SD-WAN Controller pair and then migrates the tenant there.

Automatic tenant placement

With automatic tenant placement you can rely on the system to assign SD-WAN Controller pairs during onboarding, adjust forecasts if existing SD-WAN Controllers can handle more WAN Edge devices, or re-onboard/add controllers if capacity is exceeded.

Availability

Cisco supports automatic tenant placement in vManage in Release 20.8.x and earlier.

Algorithm criteria

The internal algorithm assigns SD-WAN Controllers by considering three factors:

- the number of tenant WAN edge devices forecasted for the tenant,
- the number of tenants already served by each SD-WAN Controller pair, and
- the number of WAN edge devices already connected to each SD-WAN Controller pair.

Benefits of automatic tenant placement on multitenant SD-WAN Controllers

This section highlights how strategic tenant placement enhances controller efficiency, performance, and overall network resilience.

Reliability & availability

Reduces the risk of simultaneous controller failures by allowing you to choose controllers deployed in different failure zones or regions in a cloud environment.

Performance & efficiency

- Minimizes latency by enabling you to select controllers located in the same geographical region as the tenant WAN edge devices.
- Improves performance and efficiency by letting you choose controllers based on available CPU, DRAM, hard disk resources, and their utilization.

Scalability

Provides scalability by allowing you to migrate tenants to different controllers when the tenant device forecast changes.

Restrictions for automatic tenant placement on multitenant SD-WAN Controllers

If you need to migrate a tenant to a different pair of SD-WAN Controllers, change the SD-WAN Controllers one at a time. This restriction ensures that one controller remains available to the tenant WAN edge devices and prevents traffic disruption. SD-WAN Controllers CLI templates must not contain tenant configuration. This configuration is added dynamically and managed internally by the device. If tenant configuration is present in any SD-WAN Controller CLI template, it must be removed to prevent issues during tenant migration or placement operations.

Prerequisites for automatic tenant placement on multitenant SD-WAN Controllers

Before adding new tenants, ensure that SD-WAN Controller, capacity limits, and account configurations meet the foundational requirements.

SD-WAN Controller requirements

- Ensure at least two Cisco SD-WAN Controllers are operational and visible in SD-WAN Manager before adding new tenants.
- Push a template from SD-WAN Manager to a controller to place it in Manager mode; a controller in CLI mode cannot serve multiple tenants.
- Verify that each SD-WAN Controller pair can support a maximum of 24 tenants and 1000 tenant devices. Ensure at least two controllers have capacity for a new tenant. If no pair can support a new tenant, add two controllers and switch them to Manager mode.

Tenant provisioning rules

- Add up to 16 tenants in a single operation. SD-WAN Manager provisions tenants sequentially, not in parallel.
- Do not start a second **Add Tenant** task while one is already in progress; otherwise, the second task fails.

Accounts and profiles

Each tenant requires a unique Virtual Account (VA) on Plug and Play Connect in Cisco Software Central. The tenant VA must belong to the same Smart Account (SA) as the provider VA. Depending on the deployment type, one of the following must be completed:

- On-premises deployments: Create a SD-WAN Validator controller profile for the tenant on Plug and Play Connect with these mandatory fields:

Table 325: Mandatory fields for on-premises validator controller profile

Field	Description
Profile name	Enter a name for the controller profile.
Multitenancy	From the drop-down list, select **Yes**.
SP organization name	Enter the provider organization name.
Organization name	Enter the tenant organization name in the format <SP Org Name>-<Tenant Org Name>. The organization name can be up to 64 characters.
Primary controller	Enter the host details for the primary SD-WAN Validator

- For cloud deployments: SD-WAN Manager automatically creates the Validator Controller profile during tenant creation.

Assign SD-WAN Controllers to tenants during onboarding

Before you begin

Each tenant requires a unique Virtual Account (VA) on Plug and Play Connect in Cisco Software Central. The tenant VA must belong to the same Smart Account (SA) as the provider VA. Depending on the deployment type, one of these must be completed:

- On-premises deployments: Create a Cisco SD-WAN Validator controller profile for the tenant on Plug and Play Connect with these mandatory fields:

Table 326: Mandatory fields for on-premises validator controller profile

Field	Description
Profile name	Enter a name for the controller profile.
Multitenancy	From the drop-down list, select **Yes**.
SP organization name	Enter the provider organization name.
Organization name	Enter the tenant organization name in the format <SP Org Name>-<Tenant Org Name>. The organization name can be up to 64 characters.
Primary controller	Enter the host details for the primary SD-WAN Validator.

- For cloud deployments: SD-WAN Manager automatically creates the Validator Controller profile during tenant creation.

To provision and activate the tenant in SD-WAN Manager with the configured settings, follow these steps.

Procedure

Step 1 Log in to SD-WAN Manager as the provider admin user.

Step 2 From the menu, choose **Administration** > **Tenant Management**.

Step 3 Click **Add Tenant**.

Step 4 In the **Add Tenant** slide-in pane, click **New Tenant**.

Step 5 Configure tenant details:

Table 327: Tenant Configuration Fields

Field	Details
Name	Enter a name for the tenant. For cloud deployments, the tenant name must match the tenant VA name in Plug and Play Connect.
Description	Enter a description (up to 256 alphanumeric characters).

Field	Details
Organization name	Enter the tenant's organization name (case-sensitive, up to 64 characters). Use the format <SP Org Name>-<Tenant Org Name> Example: managed-sp-customer1
URL subdomain	Enter the tenant's fully qualified subdomain name. It must include the provider's domain name. Example: customer1.managed-sp.com. See DNS configuration table for deployment-specific steps.
Forecasted devices	Enter the maximum number of WAN edge devices the tenant can add. If this limit is exceeded, SD-WAN Manager blocks device addition.
Select two controllers	• Automatic placement (default): Ensure the field is set to Autoplacement. • Manual placement: **a.** Click the **Select two Controllers** drop-down list. SD-WAN Manager lists the hostnames of the available SD-WAN Controllers. For each SD-WAN Controller, SD-WAN Manager shows whether the controller is reachable and reports the utilization details. See utilizations details table for more information. **b.** Select two SD-WAN Controllers to assign to the tenant based on the utilization details.

Table 328: Utilization details

Field	Description
Tenant hosting capacity	Each SD-WAN Controller can serve a maximum of 24 tenants. Tenant hosting capacity represents the number of tenants to which the Cisco SD-WAN Controller is assigned in the form of a percentage. This value indicates whether you can assign another tenant to this controller.
Used device capacity	Each SD-WAN Controller can support a maximum of 1000 tenant WAN edge devices. Used device capacity represents the number of tenant WAN edge devices connected to the SD-WAN Controller in the form of a percentage of the maximum capacity (1000 WAN edge devices). This value indicates whether the SD-WAN Controller can support the number of devices forecast for the tenant that you are onboarding.
Memory utilized	This value represents memory consumption as a percentage.
CPU utilized	This value represents CPU usage as a percentage.

Table 329: DNS configuration

Deployment type	DNS configuration steps
On-premises	• Add the tenant subdomain to DNS and map it to the IPs of the three SD-WAN Manager instances in the cluster. • Create a provider DNS A record from the provider's domain name and cluster ID. Example: `vmanage123.sdwan.cisco.com`. Validate: `nslookup vmanage123.sdwan.cisco.com`. • Create tenant DNS CNAME records mapping the tenant FQDN to the provider FQDN. Example: `customer1.sdwan.cisco.com`. Validate: `nslookup customer1.sdwan.cisco.com`. • If DNS is misconfigured, an authentication error occurs.
Cloud	• The tenant subdomain is automatically added to DNS. • DNS resolution can take up to one hour after creation.

Step 6 Save the tenant configuration.

Step 7 To add another tenant, repeat steps 4 to 6.

When the task completes successfully, you can view the tenant information, including the assigned SD-WAN Controllers and Validators, on **Administration** > **Tenant Management**.

After completing the tenant addition steps, SD-WAN Manager performs the Create Tenant Bulk task, which:

- Creates the tenant.
- Assigns two SD-WAN Controllers and pushes CLI templates with the tenant information.
- Sends the tenant and controller details to SD-WAN Validator.

Update SD-WAN Controller placement for a tenant

You can migrate a tenant to a different pair of SD-WAN Controller if the currently assigned controllers cannot support the tenant's revised WAN edge device forecast.

During migration, change one controller at a time to ensure continuous availability and prevent traffic disruption.

Procedure

Step 1 Log in to SD-WAN Manager as the provider admin user.

Step 2 From the menu, choose **Administration** > **Tenant Management**.

Step 3 Locate the tenant to migrate and click **…** next to the tenant organization name.

Step 4 Click **Update Controller Placement.**

Step 5 In the **Update Controller Placement** slide-in pane, configure these:

a) Source Controller (currently applied)

1. Click the drop-down list to view the tenant's currently assigned controllers.
2. SD-WAN Manager shows reachability and utilization details for each controller:
   - Tenant hosting capacity (max 24 tenants)
   - Used device capacity (max 1000 devices)
   - Memory utilization (%)
   - CPU utilization (%)
3. Select the check box next to one of the currently assigned controllers.

b) Destination controller

1. Click the drop-down list to view available controllers not currently assigned to the tenant.
2. SD-WAN Manager shows reachability and utilization details for each controller.
   - Tenant hosting capacity (max 24 tenants)
   - Used device capacity (max 1000 devices)
   - Memory utilization (%)
   - CPU utilization (%)
3. Select the checkbox next to the controller you want to assign.

Note
If the selected controller cannot support the tenant's devices, the update operation fails.

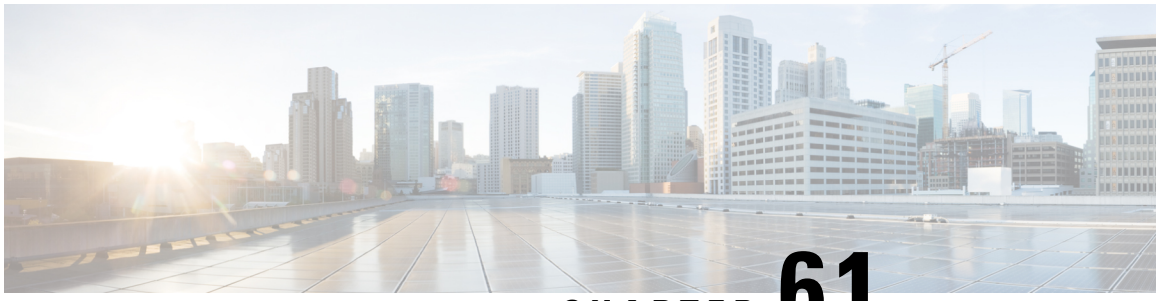
Step 6 Click **Update**.

Step 7 To change the second controller assigned to the tenant, repeat steps 5–6.

SD-WAN Manager starts the Tenant Controller Update task, migrating the tenant details from the previous controller to the new controller.

What to do next

After the task completes successfully, view the updated tenant information, including the assigned SD-WAN Controllers, on **Administration** > **Tenant Management**.



CHAPTER 61

Dynamic On-Demand Tunnels

- Feature history for dynamic on-demand tunnels, on page 915
- Dynamic on-demand tunnels, on page 916
- How on-demand tunnels work, on page 916
- How on-demand tunnels work with a transport gateway, on page 918
- Prerequisites for on-demand tunnels, on page 918
- Restrictions for on-demand tunnels, on page 922
- Configure on-demand tunnels, on page 922
- Monitor the status of on-demand tunnels, on page 927
- View OMP routes, on page 929

Feature history for dynamic on-demand tunnels

Table 330: Feature History Table

Feature Name	Release Number	Description
Dynamic On-Demand Tunnels	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco SD-WAN Release 20.3.1	This feature enables you to configure an inactive state for tunnels between edge devices. This configuration reduces performance demands on devices and decreases network traffic.
Dynamic On-Demand Tunnels with Transport Gateways	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	A transport gateway can serve as the hub between two spoke devices. It provides the backup route that is necessary for spoke-to-spoke on-demand tunnels to operate. Using a transport gateway as the hub simplifies the process of enabling on-demand tunnels. This method does not require any changes to control policy on Cisco SD-WAN Controllers.

Dynamic on-demand tunnels

A Cisco Catalyst SD-WAN on-demand tunnel is a network feature that:

- automatically establishes secure tunnels between spoke devices when traffic starts,
- uses a configurable inactivity timer to remove tunnels after traffic stops, and
- conserves bandwidth and device performance when inactive.

On-demand tunnels enable efficient, temporary connections that optimize network resource usage.

Cisco Catalyst SD-WAN on-demand tunnels are triggered by device traffic and are removed after a set period of inactivity, ensuring inactive links do not consume bandwidth or affect performance.

How on-demand tunnels work

Summary

When you configure a site to use dynamic tunnels, the on-demand functionality is enabled. In this mode of operation, Cisco Catalyst SD-WAN edge routers do not bring up direct tunnels to other sites that are also enabled with on-demand functionality.

Cisco Catalyst SD-WAN selects one or more edge routers (typically centrally located routers) to act as backup forwarding node(s), providing a secondary path for traffic between two nodes. The backup node(s) are not enabled for on-demand. All on-demand sites form static tunnels with the backup node(s). The backup node(s) provide a static backup route for traffic between two nodes that have on-demand enabled.

The first packet of traffic between two nodes is routed through the static backup path, and triggers the on-demand tunnel to become active between the sites. The backup path continues to forward traffic until the direct path becomes active.

All on-demand sites learn the TLOCs and prefixes of all other on-demand remote sites. The prefixes also have a backup path set up through Cisco Catalyst SD-WAN Controller control policy. So in the control plane, the on-demand tunnel network has the same state as a full-mesh tunnel network, including a backup path.

The control plane downloads to the data plane, routes, with the backup path and remote TLOCs that represent a potential direct path between any two sites, but it does not set up a direct path tunnel to remote TLOCs.

All prefixes learned from remote sites must have a backup path. A less-specific aggregate route from a hub site is not a valid backup path. The specific prefix advertised from the remote branch must also be advertised as a backup from the hub.

If this specific prefix is missing as a backup, the on-demand tunnel setup will fail.

Therefore, the backup path must be a static tunnel that is always UP. This static tunnel should include both the specific prefixes from the remote branch and any necessary aggregate routes to ensure proper tunnel establishment and maintenance.

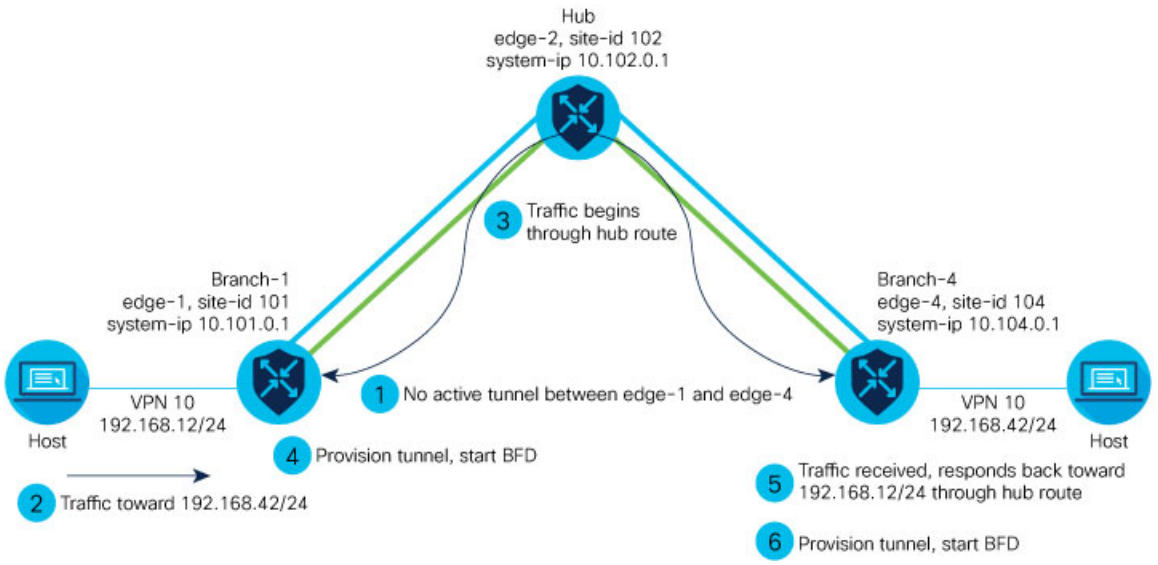
Traffic from either end of the on-demand tunnel triggers setting up the tunnel. This enables on-demand tunnels to accommodate network address translation (NAT) traversal.

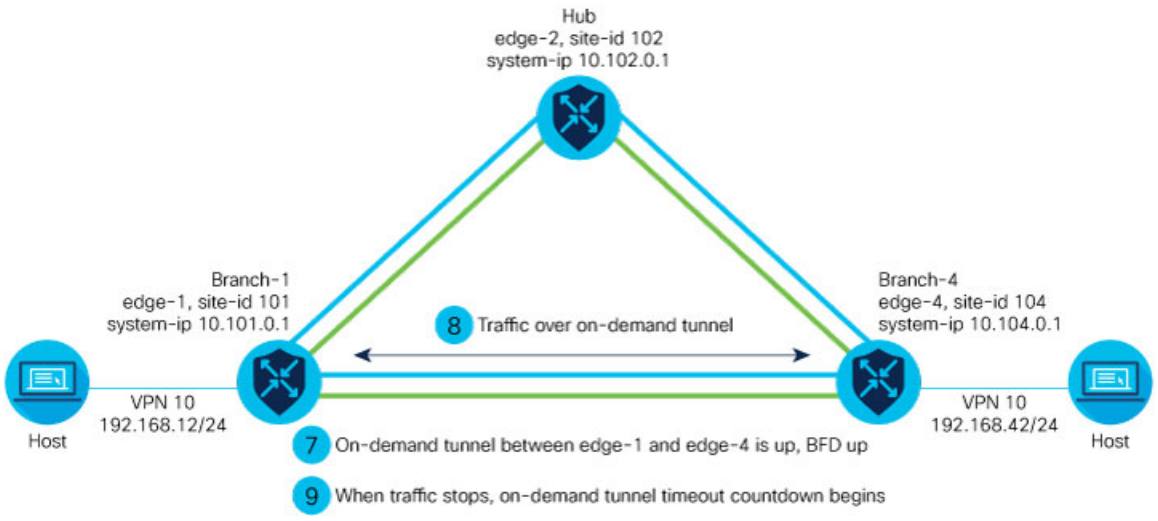
The on-demand tunnel feature introduces two states for the on-demand branch site:

- Inactive: The on-demand tunnel is not set up with the remote site. There is no active traffic to or from the remote site. Remote site TLOCs are inactive—no bidirectional forwarding detection (BFD) is set up, the prefix is installed with the inactive paths, and the backup path is set as the path to forward any traffic.
- Active: The on-demand direct site-to-site tunnel is set up to the remote site. There is active traffic to or from the remote site. This state is identical to the case of a typical tunnel, where the remote TLOCs have BFD set up, and the prefix is installed with the direct path tunnel. In this state, tunnel activity is tracked. If there is no traffic for the "idle time" duration (default 10 minutes), the direct site-to-site tunnel is removed and the state changes to Inactive.

Workflow

Figure 9: Process of On-Demand Tunnel Establishment Between Two Edge Routers





The steps below demonstrate what occurs between two edge routers with an on-demand tunnel configured.

1. There is no active tunnel between the two edge routers. edge-1 and edge-4 are in their inactive states.

2. The host behind edge-1 initiates traffic toward the host behind edge-4.
3. edge-1 forwards the traffic through the backup path using the hub or backup node to edge-4.
4. edge-1 provisions the on-demand tunnel and begins bidirectional forwarding detection (BFD). edge-4 is now in its active state on edge-1.
5. When edge-4 receives the return traffic for the host behind edge-1, it forwards the traffic through the backup path using the hub or backup node to edge-1.
6. edge-4 provisions the on-demand tunnel and begins BFD. edge-1 is now in active state on edge-4.
7. At this point, the on-demand tunnel between edge-1 and edge-4 is up, and BFD is up.
8. Traffic between the two edge devices takes the direct route through the on-demand tunnel.
9. Both edge-1 and edge-4 track the traffic activity on the on-demand tunnel in both directions.

   If there is no traffic for the idle timeout duration, the on-demand tunnel is deleted, and the edge-1 and edge-4 devices go back to the inactive state.

How on-demand tunnels work with a transport gateway

Summary

A transport gateway can serve as the hub between two spoke devices, providing the backup route that is necessary for spoke-to-spoke on-demand tunnels to operate. Using a transport gateway as the hub simplifies the process of enabling on-demand tunnels. This method does not require configuring control policy on Cisco SD-WAN Controllers.

Workflow

For information about configuration, see *Configure On-Demand Tunnels Using a Transport Gateway*.

Prerequisites for on-demand tunnels

There are several prerequisites for using on-demand tunnels:

- Configure a Centralized Control Policy for On-Demand Tunnels
- Prerequisites: OMP Settings
- Prerequisites: Hub Device Traffic Engineering Service
- Prerequisites: Spoke Device ECMP Limit
- Prerequisites: OMP Settings
- Prerequisites: Hub Device Traffic Engineering Service
- Prerequisites: Spoke Device ECMP Limit

Prerequisites: OMP settings

When on-demand tunnels are enabled, spokes use backup paths through the hub, so a higher path limit is necessary. The direct paths as well as the backup paths need to be advertised. To accommodate this, increase the Cisco Catalyst SD-WAN Controller send-path-limit to advertise all available paths. We recommend to use the maximum possible value.

Note If there are too many Hub TLOCs configured in the on-demand tunnel control policy, the recommended value for send-path-limit is not enough always. In such cases, the on-demand tunnel feature will not work at all.

Starting from Cisco vManage Release 20.8.1 and Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, the maximum send-path-limit is 32. In Cisco vManage Release 20.7.x and earlier releases, the maximum send-path-limit is 16.

For information about configuring Cisco SD-WAN Controller send-path-limit, see the routing configuration guides on the Cisco Catalyst SD-WAN Configuration Guides page.

Before you begin

The Cisco Catalyst SD-WAN Controller send-path-limit must be more than the default 4.

Procedure

Step 1 Configure the OMP send path limit using a feature template

For a Cisco Catalyst SD-WAN Controller in Managed mode, use this procedure to configure the OMP send path limit.

To confirm that it is in Managed mode, from the Cisco SD-WAN Manager menu, choose **Configuration** > **Control Components**. For a **Controller** row, the **Managed By** column shows a template name.

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
b) Click **Feature Templates.** In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.
c) Edit or create an OMP template for device type Controller. In some earlier releases, the device type is called vSmart. Any functioning Cisco Catalyst SD-WAN deployment has at least one vSmart OMP template configured.
d) In **Basic Configuration**, set the **Number of Paths Advertised per Prefix** to 16 (recommended). From Cisco SD-WAN Release 20.8.1, the maximum is 32.

Step 2 Configure the OMP send path limit for an edge device using CLI commands

Use a CLI add-on profile, CLI add-on feature template, or CLI template to execute these CLI commands. By default, CLI templates and the CLI add-on profile execute commands in global configuration mode. For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

For an edge device, use these commands to configure an OMP send path limit.

a) Enter OMP configuration mode.
b) Set the send path limit. We recommend 16.

From Cisco SD-WAN Release 20.8.1, the maximum is 32.

Example:

```
sdwan
omp
 send-path-limit 16
```

Prerequisites: Hub device traffic engineering service

Before you begin

On the hub device, the Traffic Engineering service (service TE) must be enabled.

This ensures that the Cisco Catalyst SD-WAN Overlay Management Protocol (OMP) on the spoke devices accepts the backup path through the hub, which is being added as an intermediate path between the two spoke devices. Without this, the backup path through the hub would be considered invalid and unresolved by the spoke devices.

Procedure

Step 1 Enable the Traffic Engineering Service Using Cisco SD-WAN Manager

a) In Cisco SD-WAN Manager, open **Configuration** > **Templates**
b) Click **Feature Templates**.

In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

c) Click **Add Template**.
d) Select a platform.
e) From **VPN**, select **VPN**.
f) Ensure that in **Basic Configuration**, the **VPN** field is set to 0.
g) From **Service**, click **New Service** and select **TE**.
h) Click **Add**, and then click **Update**. The TE service appears in the table of services.
i) Apply the VPN-0 template to the hub

Step 2 Enable the Traffic Engineering Service, Using CLI Commands (Cisco IOS XE Catalyst SD-WAN Devices)

Use a CLI add-on profile, CLI add-on feature template, or CLI template to execute these CLI commands. By default, CLI templates and the CLI add-on profile execute commands in global configuration mode. For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

Example:

```
sdwan
 service TE vrf global
exit
```

Step 3 Enable the Traffic Engineering Service, Using CLI Commands (Cisco vEdge Devices)

Example:

```
vpn 0
 service TE
 exit
```

Prerequisites: Spoke Device ECMP Limit

Before you begin

On spoke devices, the ECMP limit must be more than the default 4. Recommended: 16

When on-demand tunnels are enabled, spoke devices create both direct and backup paths. To accommodate the need for more paths, increase the ECMP limit.

Procedure

Step 1 Configure the ECMP Limit Using a Configuration Group

On the **Configuration** > **Configuration Groups** page, choose the SD-WAN solution type.

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
b) Do one of these:

- Edit a profile directly:

  In the System Profile tab, create (**Add New)** or edit a System profile.

- Edit a profile in a configuration group:

  Open a configuration group and edit the System profile.

c) In the system profile, create or edit an OMP feature.
d) In the **Basic Configuration** section, use the **ECMP Limit** field to configure the equal-cost multi-path (ECMP) limit as 16 (recommended).

Step 2 Configure the ECMP Limit Using a Feature Template

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
b) Click **Feature Templates**.

In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

c) Click **Add Template**.
d) Select a device and click **Cisco OMP**.
e) In **Basic Configuration**, set the **ECMP Limit** field to 16 (recommended).

Step 3 Configure the ECMP Limit Using CLI Commands

Use a CLI add-on profile, CLI add-on feature template, or CLI template to execute these CLI commands. By default, CLI templates and the CLI add-on profile execute commands in global configuration mode. For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

Example:

```
sdwan
omp
 no shutdown
 ecmp-limit       16
```

You can view the current ecmp-limit using the `show running-config omp` command.

Restrictions for on-demand tunnels

- PfR statistics collection starts fresh for each on-demand tunnel setup and does not cache statistics for deleted tunnels after idle timeout.
- Out-of-order (OOO) packets may occur when the router switches traffic from the backup path to the on-demand tunnel; the router forwards packets as received.
- Unidirectional and multicast flows do not trigger on-demand tunnel setup and continue to use the backup path.
- Do not configure a data policy that applies a **set tloc-list** action to an on-demand site TLOC; doing so will result in dropped traffic.
- If the Pair Wise Key (PWK) IPSEc feature is enabled, on-demand tunnels are not supported.
- All TLOCs in the system are reset (disabled and then enabled) when you execute **on-demand enable** or **no on-demand enable**.
- When provisioning on-demand tunnels, the edge device provisions tunnels to all TLOCs on the remote edge device; for multi-home sites, you must enable on-demand mode on all systems.
- The system keeps all edge devices using on-demand tunnels active if service or user traffic exists on any on-demand tunnel in either direction; tunnels can be enabled between two sites only if both are in on-demand mode.
- You must configure a backup path for all prefixes from on-demand remote sites; the backup path must always be UP. The setup or removal of on-demand tunnels does not affect overlay route (OMP) updates or service/LAN-side route updates (such as OSPF or BGP). If either site is not in on-demand mode, the system sets up static tunnels between the sites.

Configure on-demand tunnels

The following procedures describe how to configure on-demand tunnels using different methods, including using control policy, or a simpler method using a transport gateway as a hub.

- Configure On-Demand Tunnels Using Control Policy
- Configure On-Demand Tunnels Using a Transport Gateway
- Enable On-Demand Tunnels on a Spoke Device Using a Configuration Group
- Enable On-Demand Tunnels on a Spoke Device Using a Template
- Enable On-Demand Tunnels Using a CLI Template

Configure on-demand tunnels using control policy

To configure on-demand tunnels using the control policy method, do the following:

Procedure

Step 1 Configure a control policy, as described in Configure a centralized control policy for on-demand tunnels.

Step 2 Enable on-demand tunnels n spoke devices, as described in Enable on-demand tunnels on a spoke device using a template and Enable on-demand tunnels using a CLI template.

Configure a centralized control policy for on-demand tunnels

Before you begin

This procedure configures a centralized control policy on a Cisco Catalyst SD-WAN Controller to enable on-demand tunnels.

- The Cisco Catalyst SD-WAN Controller centralized control policy must include the `tloc-action backup` action.

  This ensures that the backup path through the hub for communication between all of the spoke devices.

- The Cisco Catalyst SD-WAN Controllerr centralized control policy must accept all spoke prefix routes.
- The Cisco Catalyst SD-WAN Controller centralized control policy must accept TLOCs of all spokes.

  For information about configuring a Cisco Catalyst SD-WAN Controller **centralized control policy,** see the policies configuration guides on the Cisco Catalyst SD-WAN Configuration Guides page.

- When configuring on-demand tunnels using a transport gateway, do not use the control policy procedure described here. For information, see Configure On-Demand Tunnels Using a Transport Gateway.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.

a) Select **Centralized Policy**.
b) Click **Add Policy**.
c) In the left pane, click **Site**.
d) Click **Next**.
e) Click **Add Topology** and select **Custom Control (Route & TLOC)**.
f) Enter a name and description for the topology.
g) Click **Sequence Type**.
h) In the **Add Control Policy** pop-up window, choose **Route**.
i) Click **Sequence Rule** to create a sequence.

Step 2 Click **Match**.

a) Among the match conditions, click **Site**.
b) In the **Match Conditions** area, click the **Site List** menu and choose a site list.
c) Click **Actions**, and then **Accept**.

Step 3 Among the actions, click **TLOC Action**.

a) In the **Actions** area, click the **TLOC Action** menu and choose **Backup**.
b) Among the actions, click **TLOC**.
c) In the **Actions** area, click the **TLOC List** menu and choose or create a TLOC list.
d) Click **Save Match and Actions**.

Step 4 Click **Default Action**.

a) In the **Default Action** area, click the pencil icon to edit.
b) Near the **Actions** label, click **Accept**.
c) Click **Save Control Policy**.
d) Click **Next** twice.
e) In the Topology tab, click **New Site/WAN Region List**.
f) Click **Outbound Site List** and choose a site list that defines the sites at which you are enabling on-demand tunnels.
g) Adjacent to the site list, click **Add**.
h) Enter a name and description for the policy.
i) Click **Save Policy**.

Configure centralized control policy for on-demand tunnels using a CLI policy

Before you begin

The Cisco Catalyst SD-WAN Controller must be managed by Cisco SD-WAN Manager.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Classic** > **Policies**.

Step 2 Open **Centralized Policy**.

Step 3 From **Custom Options**, choose **Centralized Policy** > **CLI Policy**.

Step 4 Click **Add Policy**.

Step 5 Enter the CLI commands for the policy.

Example:

```
control-policy Dynamic-Tunnel-Control-Policy
    sequence 100
     match route
      site-list Branches
     !
     action accept
      set
       tloc-action backup
       tloc-list Hub-TLOCs
      !
     !
     sequence 200
      match tloc
     !
     action accept
    !
  default-action accept
 !
 lists
```

```
  site-list Branches
   site-id 200
   site-id 300
  !
  tloc-list Hub-TLOCs
   tloc 10.0.0.1 color mpls encap ipsec
   tloc 10.0.0.1 color public-internet encap ipsec
!
!
apply-policy
 site-list Branches
  control-policy Dynamic-Tunnel-Control-Policy out
 !
!
```

Configure on-demand tunnels using a transport gateway

Before you begin

- On Cisco SD-WAN Controllers, configure the send path limit, as described in Prerequisites: OMP settings.
- On spoke devices, configure the ECMP limit, as described in Prerequisites: Spoke Device ECMP Limit.
- When using a transport gateway as a hub to support on-demand tunnels, there is no need to create or modify a control policy.

  Do not use the procedure described in Configure a Centralized Control Policy for On-Demand Tunnels.

Procedure

Step 1 Enable transport gateway functionality on a router serving as the hub, providing a backup route between spokes, as described in the Transport Gateway section of the *Cisco Catalyst SD-WAN Routing Configuration Guide*.

Step 2 Enable on-demand tunnels and configure the idle timeout on spoke devices as described in Enable on-demand tunnels on a spoke device using a template.

Enable on-demand tunnels on a spoke device using a configuration group

Before you begin

On the **Configuration** > **Configuration Groups** page, choose the **SD-WAN** solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Do one of these:

- Edit a profile directly:

  In the System Profile tab, create (**Add New**) or edit a System profile.

- Edit a profile in a configuration group:

  Open a configuration group and edit the System profile.

Step 3 In the System profile, create (**Add New**) or edit a Basic feature.

Step 4 In the **Advanced** section, use the **On Demand Tunnel** control to enable on-demand tunnels.

Enable on-demand tunnels on a spoke device using a template

Before you begin

- See the Prerequisites for On-Demand Tunnels.
- Do not enable on-demand on the hub device.
- On the spoke devices, enable on-demand at the system level. In the case of multi-homed sites, enable on-demand on all systems at the site.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**

Step 2 Click **Feature Templates**.

Note
In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

Step 3 Click **Add Template**.

Step 4 Select a device.

Step 5 From **Basic Information**, select **Cisco System**.

Step 6 Click **Advanced**.

Step 7 Enable **On-demand Tunnel.**

Step 8 (optional) Configure the **On-demand Tunnel Idle Timeout** time. The default idle timeout value is 10 minutes. Range: 1 to 65535 minutes

Step 9 Attach the System feature template to the device template for the spoke device.

Enable on-demand tunnels using a CLI template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

By default, CLI templates execute commands in global configuration mode.

Before you begin

- See Prerequisites for On-Demand Tunnels.
- Do not enable on-demand on the hub device

Procedure

On the spoke devices, enable on-demand tunnels at the system level. In the case of multi-homed sites, enable on-demand on all systems in the site.

The default idle timeout value is 10 minutes. Range: 1 to 65535 minutes

Example:

```
system
     on-demand enable
     on-demand idle-timeout 10
```

Monitor the status of on-demand tunnels

The following sections describe procedures for monitoring the status of on-demand tunnels.

- View the Current Status of On-Demand Tunnels Using Cisco SD-WAN Manager
- View a Chart of the On-Demand Tunnel Status Over Time in Cisco SD-WAN Manager
- View the Route to a Destination Device

View the current status of on-demand tunnels using Cisco SD-WAN Manager

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

For Cisco Catalyst SD-WAN Control Components Release 20.6.x and earlier:

From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

Step 2 Select a device.

Step 3 Select **Real Time**.

Step 4 For **Device Options**, select one of the following:

- **On Demand Local**: Displays the status of on-demand tunnels on the specified device.
- **On Demand Remote**: Displays the status of on-demand tunnels on the specified device, and on all connected devices.

The output is equivalent to executing the `show [sdwan] system on-demand [remote-system] [system-ip ip-address] CLI` command. It displays the status of on-demand tunnels.

View a chart of the on-demand tunnel status over time in Cisco SD-WAN Manager

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

Cisco Cisco Catalyst SD-WAN Control Components Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network** > > **.**

Step 2 Select a device.

Step 3 From WAN, choose Tunnel.

Step 4 From the **Chart Options** drop-down list, select **On-Demand Tunnel Status.** The chart shows the status of tunnels as `ACTIVE` or `INACTIVE`. `INACTIVE` indicates that an on-demand tunnel is in its inactive mode.

View the route to a destination device

Viewing the route between routers A and B can show whether the route is using an on-demand tunnel. On router A, use the `traceroute` command and enter router B as the destination. The command output shows whether the current route includes a hop at a hub device or whether the route is directly to the destination.

In the following examples, the router IP addresses are as follows:

- Router A: 10.1.1.1
- Router B: 10.1.1.2
- Hub device: 10.100.1.100

No Active On-Demand Tunnel

In the following example, there is no active on-demand tunnel between routers A and B, so the route includes the hub device. Note that it takes two hops to reach router B.

```
RouterA#traceroute vrf 1 10.1.1.2 numeric
Type escape sequence to abort.
Tracing the route to 10.1.1.2
VRF info: (vrf in name/id, vrf out name/id)
1 10.100.1.100 10 msec 8 msec 0 msec
2 10.1.1.2 2 msec * 1 msec
```

Active On-Demand Tunnel

```
RouterA#traceroute vrf 1 10.1.1.2 numeric
Type escape sequence to abort.
Tracing the route to 10.1.1.2
VRF info: (vrf in name/id, vrf out name/id)
1 10.1.1.2 1 msec
```

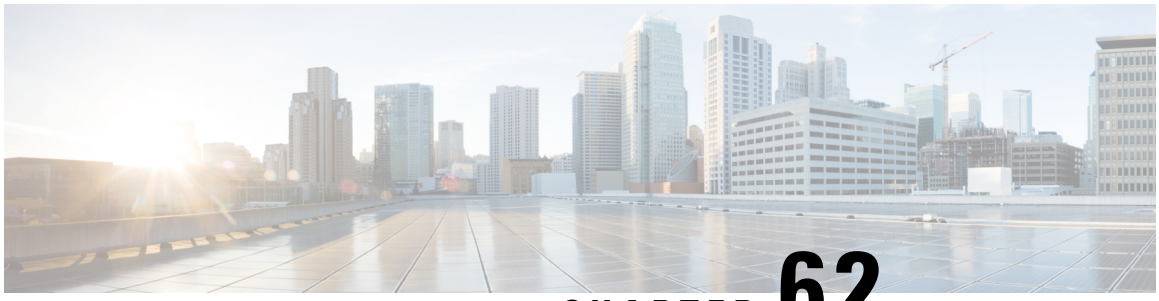
In the following example, there is an active on-demand tunnel between routers A and B, so the route from router A and to router B is direct.

View OMP routes

Viewing OMP routes can show the status of on-demand tunnels between two routers. Use the show `sdwan omp routes` command and view the **STATUS** column. The following table shows the possible values for this column, depending on whether an on-demand tunnel is active or not between two routers:

Table 331: Status of Routes, with or without an Active On-Demand Tunnel Between Two Routers

On-Demand Tunnel Between Routers A and B	STATUS for OMP Routes Between Routers A and B	STATUS for Backup Routes (through the Hub)
Not active	I, U, IA (installed, unresolved, and inactive)	C, I, R (chosen, installed, and resolved)
Active	C, I, R (chosen, installed, and resolved)	R (resolved)



CHAPTER 62

IPv6 Functionality

• Configure IPv6 functionality, on page 931

Configure IPv6 functionality

Configure IPv6 functionality for an Interface or Subinterface using templates

Before you begin

Perform these steps to configure IPv6 functionality for an interface or subinterface template.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**, and click **Add Template** to select an appropriate device model.

Step 3 Select **Cisco VPN Interface Ethernet** from the list of templates.

Step 4 From **Basic Configuration**, click **IPv6** and configure these parameters.

Field	Description
Static	Selected by default because IPv6 addresses are static.
IPv6 Address	IPv6 address of the interface or subinterface.

Configure IPv6 functionality for an interface or subinterface using CLI commands

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Configure according to this example.

```
interface GigabitEthernet1
  no shutdown
  ipv6 address 2001:DB8:1::1/64
  ipv6 enable
```

Configure IPv6 functionality for OMP using templates

Before you begin

Perform these steps to configure IPv6 functionality for OMP.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**, and click **Add Template** to select an appropriate device model.

Step 3 Select **Cisco OMP** from the list of templates.

Step 4 In the **Advertise** section, select **IPv6** and configure these parameters.

Field	Description
Connected	Click **Off** to disable advertising connected routes to OMP. By default, connected routes are advertised to OMP.
Static	Click **Off** to disable advertising static routes to OMP. By default static routes are advertised to OMP.
BGP	Click **Off** to advertise BGP routes to OMP. By default, BGP routes are not advertised to OMP.

Configure IPv6 functionality for OMP using CLI commands

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Enable service VRF for IPv6, according to this example.

```
config-transaction
vrf definition 1
  rd 1:1
  address-family ipv6
```

Step 3 Enable OMP, according to this example.

OMP supports global IPv6 configuration. In addition, per VRF level configuration is allowed. Per VRF level configuration overrides global configuration.

```
config-transaction
sdwan
  omp
  !
  address-family ipv6
   advertise bgp
   advertise connected

   address-family ipv6 vrf 1
    advertise static
```

Step 4 Global configuration is the default configuration, so IPv6 is enabled by default for OMP. To disable IPv6 OMP route redistribution for a particular VRF, configure the redistribution protocol to **no**.

```
config-transaction
sdwan
  omp
  !
  address-family ipv6
   advertise bgp
   advertise connected

   address-family ipv6 vrf 1
    no advertise connected
    no advertise static
    no advertise bgp
```

Configure IPv6 functionality for BGP using templates

Before you begin

Perform these steps to configure IPv6 functionality for BGP.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**, and click **Add Template** to select an appropriate device model.

Step 3 Select **Cisco BGP** from the list of templates.

Step 4 In the **Unicast Address Family** section, select **IPv6** and configure these parameters.

Tab	Field	Description
	Maximum Paths	Maximum number of parallel IBGP paths that can be installed into a route table to enable IBGP multipath load sharing. Range: 0 to 32
	Address Family	BGP IPv6 unicast address family.
RE-DISTRIBUTE		Click the **Redistribute** tab, and then click **Add New Redistribute**.
	Protocol	Select the protocols from which to redistribute routes into BGP, for all BGP sessions. Options are Connected, NAT, OMP, OSPF, and Static. At a minimum, select these: • For service-side BGP routing, select OMP. By default, OMP routes are not redistributed into BGP. • For transport-side BGP routing, select Connected, and then under Route Policy, specify a route policy that has BGP advertise the loopback interface address to its neighbors.
	Route Policy	Name of the route policy to apply to redistributed routes.
		Click **Add** to save the redistribution information.
NETWORK		Click the **Network** tab, and then click **Add New Network**.
	Network Prefix	Network prefix in the format of prefix/length, for BGP to advertise.
		Click **Add** to save the network prefix.
AGGREGATE ADDRESS		Click the **Aggregate Address** tab, and then click **Add New Aggregate Address**.
	Aggregate Prefix	Prefix of the addresses to aggregate for all BGP sessions, in the format prefix/length.
	AS Set Path	Click **On** to generate set path information for the aggregated prefixes.
	Summary Only	Click **On** to filter out more specific routes from BGP updates.
		Click **Add** to save the aggregate address.

Step 5 In the **Neighbor** section, select **IPv6**, create a new neighbor or edit an existing one, and then configure these parameters.

Field	Description
IPv6 Address*	IPv6 address of the BGP neighbor.
Description	Description of the BGP neighbor.
Remote AS*	AS number of the remote BGP peer.
Address Family	Select **Global** from the drop-down list, click **On** and select the address family. Enter the address family information.
Shutdown	To shut down a BGP neighbor when you push the template, select **Global** from the drop-down list and then click **Yes**. Default: Off

Configure IPv6 functionality for BGP using CLI commands

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Configure according to this example.

```
config-transaction
router bgp 1
 bgp log-neighbor-changes
  address-family ipv6 unicast vrf 1
  neighbor 2001:DB8:19::1 remote-as 2
  neighbor 2001:DB8:19::1 activate
  neighbor 2001:DB8:19::1 advertisement-interval 1
  neighbor 2001:DB8:19::1 password cisco
  redistribute omp
  redistribute static
  exit-address-family
```

Configure IPv6 functionality for VRRP using templates

Before you begin

Perform these steps to configure IPv6 functionality for Virtual Router Redundancy Protocol (VRRP).

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**, and click **Add Template** to select an appropriate device model.

Step 3 Select **Cisco VPN Interface Ethernet** from the list of templates.

Step 4 In the **VRRP** section, select **IPv6**.

Step 5 Click **New VRRP** and configure these parameters.

Field	Description
Group ID	Virtual router ID, which represents a group of routers. Range: 1 to 255
Priority	Priority level of the router within a VRRP group. Range: 1 to 254 Default: 100
Timer	Not used.
Track OMP	Select **On** to track the Overlay Management Protocol (OMP) session running on the WAN connection when determining the primary VRRP virtual router. Default: Off
Track Prefix List	Value to track a list of IPv6 remote prefixes. This value is an alphanumeric string that is configured under Policy.
Link Local IPv6 Address	Virtual link local IPv6 address, which represents the link local address of the group. The address should be in standard link local address format. For example, FE80::AB8.
Global IPv6 Address	Virtual global unicast IPv6 address, which represents the global address of the group. The address should be an IPv6 global prefix address that has the same mask as the interface forwarding address on which the VRRP group is configured. Example: 2001::2/124 Maximum: 3 global IPv6 addresses

Configure IPv6 functionality for VRRP using CLI commands

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Configure VRRP, according to this example.

```
config-transaction
interface GigabitEthernet1

 vrrp 10 address-family ipv6
   priority 20
   track omp shutdown
   address FE80::10:100:1 primary
   address 2001:10:100::1/64
```

```
Prefix-list tracking
track 1 ipv6 route 1:1::1/128
 reachability
 ipv6 vrf 1

 track 2 ipv6 route 2:2::2/128
 reachability
 ipv6 vrf 2

 track 20 list boolean or
  object 1
  object 2

vrrp 10 address-family ipv6
  track 20 shutdown
```

Configure IPv6 functionality for SNMP using templates

Before you begin

Configure the SNMP community and trap target group.

Perform these steps to configure IPv6 functionality for SNMP.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**, and click **Add Template** to select an appropriate device model.

Step 3 Select **Cisco SNMP** from the list of templates.

Step 4 In the **Trap** section, create or edit an SNMP trap target.

Note the prerequisites for this procedure.

Step 5 Configure these parameters.

Field	Description
VPN ID	Number of the VPN to use to reach the trap server. Range: 0 to 65530
IP Address	IP address of the SNMP server.
UDP Port	UDP port number for connecting to the SNMP server. Range: 1 to 65535
Trap Group Name	Name of a trap group configured in the **Group** tab.
User Name	Name of a community configured in the **Community** tab.

Field	Description
Source Interface	Interface to use to send traps to the SNMP server that is receiving the trap information.

Configure IPv6 functionality for SNMP using CLI commands

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Configure SNMP, according to these examples.

This example permits any SNMP to access all objects with read-only permission using the community string named public. The device also sends Border Gateway Protocol (BGP) traps IPv6 host 3ffe:b00:c18:1::3/127 using SNMP v1.The community string named public is sent with the traps.

```
Device# config-transaction
Device(config)# snmp-server community public
Device(config)# snmp-server enable traps bgp
Device(config)# snmp-server host 3ffe:b00:c18:1::3/127 public
```

In this example, the SNMP context A is associated with the views in SNMPv2c group GROUP1 and the IPv6 named access list public2.

```
Device# config-transaction
Device(config)# snmp-server context A
Device(config)# snmp mib community-map commA context A target-list comm AVpn
Device(config)# snmp mib target list commAVpn vrf CustomerA
Device(config)# snmp-server view viewA ciscoPingMIB included
Device(config)# snmp-server view viewA ipForward included
Device(config)# snmp-server group GROUP1 v2c contextA read viewA write viewA notify access ipv6
public2
```

This example configures the IPv6 host as the notification server.

```
Device> enable
Device# config-transaction
Device(config)# snmp-server community mgr view restricted rw ipv6 mgr2
Device(config)# snmp-server engineID remote 3ffe:b00:c18:1::3/127 remotev6
Device(config)# snmp-server group publicv2c access ipv6 public2
Device(config)# snmp-server hosthost1.com2c vrf trap-vrf mgr
Device(config)# snmp-server user user1 bldg1 remote3ffe:b00:c18:1::3/127 v2c access ipv6 public2
Device(config)# snmp-server enable traps bgp
Device(config)# exit
```

Configure IPv6 functionality for a DHCP relay agent using templates

Before you begin

Perform these steps to configure IPv6 functionality for a DHCP relay agent.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**, and click **Add Template** to select an appropriate device model.

Step 3 Select **Cisco VPN Interface Ethernet** from the list of templates.

Step 4 In the **Basic Configuration** section, select **IPv6**.

Step 5 In the **DHCP Helper** area, click **Add** and configure these parameters.

Field	Description
DHCPv6 Helper #	IP address of the DHCP helper
DHCPv6 Helper VPN	VPN ID of the VPN source interface for the DHCP helper.

Configure IPv6 functionality for a DHCP relay agent using CLI commands

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Configure a DHCP relay agent, according to this example.

```
device-configuration
interface GigabitEthernet8
 vrf forwarding 2
 no ip address
 ipv6 address 2001:A14:99::F/64
 ipv6 dhcp relay destination vrf 1 2001:A14:19::12 GigabitEthernet2
```

Configure IPv6 functionality for ACL and QoS using templates

Before you begin

Perform these steps to configure IPv6 functionality for access control lists (ACL) and quality of service (QoS).

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**, and click **Add Template** to select an appropriate device model.

Step 3 Select **Cisco VPN Interface Ethernet** from the list of templates.

Step 4 In the **ACL/QoS** section, configure these parameters.

Parameter Name	Description
Ingress ACL – IPv6	Click **On** to enable the IPv6 ingress access list.
IPv6 Ingress Access List	Enter the name of the IPv6 ingress access list.
Egress ACL – IPv6	Click **On** to enable the IPv6 egress access list.
IPv6 Egress Access List	Enter the name of the IPv6 egress access list.

Configure IPv6 functionality for ACL and QoS using CLI commands

Before you begin

Perform these steps to configure IPv6 functionality for access control lists (ACL) and quality of service (QoS).

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Configure ACL according to this example.

```
Device(config)# policy
Device(config-policy)# ipv6
Device(config-ipv6)# access-list ipv6_acl
Device(config-access-list-ipv6_acl)#    sequence 11
Device(config-sequence-11)#     match
Device(config-match)#       source-ip 2001:380:1::64/128
Device(config-match)#      destination-ip 2001:3c0:1::64/128
Device(config-match)#      source-port      4000
Device(config-match)#      destination-port 3000
Device(config-match)#      traffic-class    6
Device(config-match)#      next-header      6
Device(config-match)#      packet-length    1000
Device(config-match)#     action accept
Device(config-action)#

Device(config)# sdwan interface GigabitEthernet6 ipv6 access-list ipv6_acl in
Device(config-interface-GigabitEthernet6)#
Device(config-interface-GigabitEthernet6)#

Device(config)# policy lists data-ipv6-prefix-list source_ipv6_list
Device(config-data-ipv6-prefix-list-source_ipv6_list)# ipv6-prefix 2001:380:1::/64

Device(config)# policy
Device(config-policy)# ipv6
Device(config-ipv6)# access-list ipv_ipv6_prefix
Device(config-access-list-ipv_ipv6_prefix)# sequence 11
Device(config-sequence-11)#     match
Device(config-match)#       source-data-prefix-list data-ipv6-prefix-list
Device(config-match)#       destination-data-prefix-list source_ipv6_list
```

```
Device(config-match)#      destination-ip 2001:3c0:1::64/128
Device(config-match)#      source-port      4000
Device(config-match)#      destination-port 3000
Device(config-match)#      traffic-class    6
Device(config-match)#      next-header      6
Device(config-match)#      packet-length    1000
Device(config-match)#     !
Device(config-match)#     action accept
```

Step 3 Configure QoS according to this example.

```
class-map match-any class0
match qos-group 0
class-map match-any class1
match qos-group 1
!
policy-map qos_map_for_data_policy
class class0
  bandwidth percent 10
  random-detect
class class1
  bandwidth percent 10
  random-detect

policy
no app-visibility
class-map
  class class0 queue 0
  class class1 queue 1
!
ipv6
  access-list fwd_class_data_policy
   sequence 5
    match
     traffic-class 0
    !
    action accept
     count fwd_class_data_policycnt_5
     class class0
    !
   sequence 6
    match
     traffic-class 1
    !
    action accept
     count fwd_class_data_policycnt_6
     class class1
!
default-action drop
```

Configure IPv6 functionality for a logging host using templates

Before you begin

Perform these steps to configure IPv6 functionality for a logging host.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**, and click **Add Template** to select an appropriate device model.

Step 3 Select **Cisco Logging** from the list of templates.

Step 4 From **Server**, click **IPv6** and configure these parameters.

Field	Description
IPv6 Hostname/IPv6 Address	Host name or IP address of the server to direct the logging information.
VPN ID	VPN ID of the VPN source interface.
Source Interface	Name of the source interface.
Priority	Maximum severity of messages that are logged.

Configure IPv6 functionality for a logging host using CLI commands

Before you begin

Perform these steps to configure IPv6 functionality for a logging host.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Configure a logging host, according to this example.

```
config-transaction
Device(config)# logging host ipv6
AAAA:BBBB:CCCC:DDDD::FFFF
```

Note
Creating and deleting the logging host configurations in same transaction causes unexpected behavior. For example, deleting **logging host** *ipv6-address* and creating **logging host** *ipv6-address* **vrf** *vrf-name* configuration in same transaction causes both configurations to disappear from the device. Send the two requests in separate transactions.

Configure IPv6 functionality for a prefix list using templates

Before you begin

Perform these steps to configure IPv6 functionality for a prefix list.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.

Step 2 From the **Custom Options** drop-down list, select **Lists**. You can make this selection for a centralized policy or a localized policy.

Step 3 Select **Prefix** from the list on the left and then select **New Prefix List**.

Step 4 Click **IPv6** and enter the IPv6 address in **Add Prefix**.

Configure IPv6 functionality for a prefix list using CLI commands

Before you begin

Perform these steps to configure IPv6 functionality for a prefix list.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Configure a prefix list, according to this example.

```
config-transaction
Device(config)# policy
Device(config-policy)# ipv6
Device(config-ipv6)# access-list ipv6_acl
Device(config-access-list-ipv6_acl)#  sequence 11
Device(config-sequence-11)#  match
Device(config-match)# source-ip 2001:DB8:1::64/128
Device(config-match)# destination-ip 2001:DB8:1::64/128
```

Configure IPv6 functionality for a data prefix using templates

Before you begin

Perform these steps to configure IPv6 functionality for a data prefix.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.

Step 2 From the **Custom Options** drop-down list, select **Lists**. You can make this selection for a centralized policy or a localized policy.

Step 3 Select **Data Prefix** from the list on the left and then select **New Data Prefix List**.

Step 4 From **Internet Protocol**, click **IPv6** and enter the IPv6 address in **Add Prefix**.

Configure IPv6 functionality for a data prefix using CLI commands

Before you begin

Perform these steps to configure IPv6 functionality for a data prefix.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Configure a data prefix, according to this example.

```
Device(config)# policy lists data-ipv6-prefix-list source_ipv6_list
Device(config-data-ipv6-prefix-list-source_ipv6_list)# ipv6-prefix 2001:DB8:1::/64
```

Configure IPv6 functionality for a centralized policy using templates

Before you begin

Perform these steps to configure IPv6 functionality for a centralized policy.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.

Step 2 From the **Custom Options** drop-down list, select **Traffic Policy** under **Centralized Policy**.

Step 3 Select **Traffic Data**.

Step 4 Select **Add Policy** and click **Create New**.

Step 5 Click **Sequence Type** and then select **Traffic Engineering**.

Step 6 Click **Sequence Rule**.

Step 7 From the **Protocol** drop-down list, select **IPv6** to apply the policy only to IPv6 address families, or select **Both** to apply the policy IPv4 and IPv6 address families.

Step 8 Click **Sequence Type** and then select **QoS**.

Step 9 Click **Sequence Rule**.

Step 10 From the **Protocol** drop-down list, click **IPv6** to apply the policy only to IPv6 address families, or select **Both** to apply the policy IPv4 and IPv6 address families.

Configure IPv6 functionality for a centralized policy using CLI commands

Before you begin

Perform these steps to configure IPv6 functionality for a centralized policy.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Configure a IPv6 in a centralized policy, according to this example.

```
config-transaction
(config)# policy
(config-policy)# lists ipv6-prefix-list foo ipv6-prefix 1::1/64
                 ipv6-prefix-list ipv6-1
                 ipv6-prefix 1::1/128
```

Configure IPv6 functionality for a localized policy using templates

Before you begin

Perform these steps to configure IPv6 functionality for a localized policy.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.

Step 2 From the **Custom Options** drop-down list, select **Access Control Lists** under **Localized Policy**.

Step 3 Click **Add Access Control List Policy** and choose **Add IPv6 ACL Policy**. The policy you create applies only to IPv6 address families.

Configure IPv6 functionality for a localized policy using CLI commands

Before you begin

Perform these steps to configure IPv6 functionality for a localized policy.

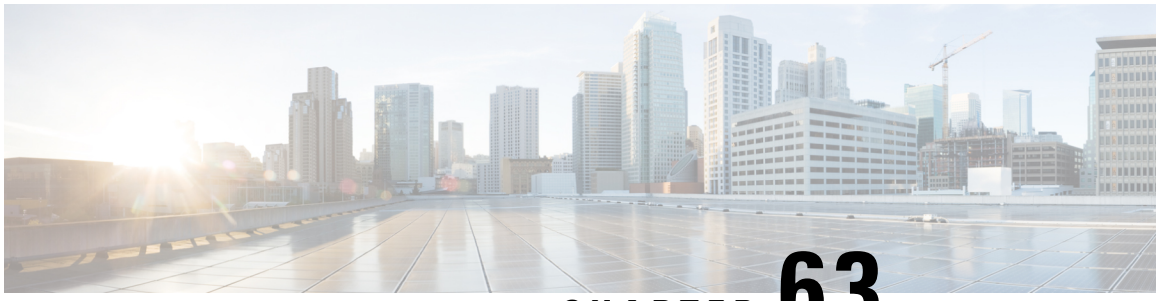
Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Configure a IPv6 in a localized policy, according to this example.

The example matches IPv6 routes that have addresses specified by the prefix list called marketing.

```
config-transaction
Device(config)# route-map name
Device(config-route-map)# match ipv6 address prefix-list marketing
```



CHAPTER 63

IPv6 in a Dual Stack Environment

- Dual stack environment with IPv6 as the preferred address family, on page 947
- Dual stack environment with IPv6 as the preferred address family, on page 948
- Methods for configuring a dual stack environment with IPv6 as the preferred address family, on page 949
- Monitor the use of IPv6 as the preferred address family in a dual stack environment, in SD-WAN Manager, on page 953
- Monitoring IPv6 as the preferred address family in a dual stack environment, on page 953

Dual stack environment with IPv6 as the preferred address family

Table 332: Feature History

Feature Name	Release Information	Description
IPv6 as Preferred Address Family in a Dual Stack Environment	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco Catalyst SD-WAN Control Components Release 20.10.1	You can select IPv6 as the preferred address family for control and data connections in a dual stack network environment. For Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller, configure IPv6 as the preferred address family by using the feature template or the CLI template. For Cisco IOS XE Catalyst SD-WAN devices, configure IPv6 as the preferred address family using the configuration groups, the Quick Connect workflow, or by CLI commands executed through a CLI add-on profile or template.

Dual stack environment with IPv6 as the preferred address family

A dual stack environment is a network that supports both IPv4 and IPv6 addressing, and where both can be used simultaneously. In a dual stack Cisco Catalyst SD-WAN environment, you can select a preferred address family, either IPv4 or IPv6, for establishing control and data connections.

Control connections

You can select a preferred address family, IPv4 or IPv6, to establish control and data connections in a dual stack network environment. Use the **Dual Stack IPv6 Default** drop-down list in Cisco SD-WAN Manager to set IPv6 or IPv4.

- **Dual Stack IPv6 Default**: **True**:

  The device establishes IPv6 control connections with SD-WAN Manager and the SD-WAN Controller that the device is connected to.

- **Dual Stack IPv6 Default**: **False**:

  The device establishes IPv4 control connections with SD-WAN Manager and the SD-WAN Controller that the device is connected to.

Data connections

Data connections or Bidirectional Forwarding Detection (BFD) sessions are established based on the IPv6 option set in local, remote devices. In a dual stack network environment, if you choose **True** for a local or remote device, the BFD session is an IPv6 connection. Otherwise, it is IPv4.

- **Dual Stack IPv6 Default**: **True**:

  Establishes IPv6 BFD sessions.

- **Dual Stack IPv6 Default**: **False**:

  Establishes IPv4 BFD sessions.

SD-WAN Validator

The **Dual Stack IPv6 Default** drop-down list options applies to devices, SD-WAN Manager, and SD-WAN Controller, but not to SD-WAN Validator.

The connections from SD-WAN Manager, SD-WAN Controller, and devices to the SD-WAN Validator are always dual (IPv4 and IPv6) in a dual stack network environment, regardless of the **Dual Stack IPv6 Default** setting.

NAT44 and NAT66

You can configure an IPv6 connection on devices that are at sites behind NAT44 and NAT66.

Benefits of setting IPv6 as the preferred address family

You have the option to migrate from IPv4 to IPv6, which allows you to have more IP addresses compared to IPv4. With IPv6, there can be no depletion of IP addresses.

Methods for configuring a dual stack environment with IPv6 as the preferred address family

These are methods of configuring devices and SD-WAN Control Components for IPv6 connections.

Configuring devices for IPv6 connectivity

- Configure IPv6 as the preferred address family for devices, using a configuration group, on page 949
- Configure IPv6 as the preferred address family for devices, using the Quick Connect workflow, on page 950
- Configure IPv6 as the preferred address family for devices, using CLI commands, on page 951

Configuring SD-WAN Control Components for IPv6 connectivity

- Configure IPv6 as the preferred address family for SD-WAN Manager and SD-WAN Controller, using CLI commands, on page 951
- Configure IPv6 as the preferred address family for SD-WAN Manager and SD-WAN Controller, using templates, on page 952

Configure IPv6 as the preferred address family for devices, using a configuration group

Before you begin

Follow these steps to configure IPv6 as the preferred address family for Cisco IOS XE Catalyst SD-WAN devices in a dual stack environment, using a configuration group.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Click **Configuration Groups**.

Step 3 Create a new configuration group or open an existing one to display the full details of the configuration group.

Step 4 In the **Deployment** area, view the devices associated with the configuration group. You can add devices if desired.

Step 5 Click **Deploy** to deploy the configuration to the associated devices.

Step 6 In **Process Overview**, click **Next**.

Step 7 On the **Selected Devices to Deploy** page, select or deselect devices and click **Next**.

Step 8 For **Dual Stack IPv6 Default**, select **True** to set IPv6 as the default connection type, and click **Next**.

Here's how **Dual Stack IPv6 Default** affects control connections and BFD sessions:

- **True**: Devices establish an IPv6 control connection with SD-WAN Manager and the SD-WAN Controller they are connected to. BFD sessions use IPv6.
- **False**: Devices establish an IPv4 control connection with SD-WAN Manager and the SD-WAN Controller they are connected to. BFD sessions use IPv4.

The connections from devices to SD-WAN Validator are always dual (IPv4 and IPv6) in a dual IP stack environment, regardless of how**Dual Stack IPv6 Default** is configured.

Step 9 On the summary page, click **Deploy**.

What to do next

For more information on using configuration groups, see Configuration Groups and Feature Profiles.

Configure IPv6 as the preferred address family for devices, using the Quick Connect workflow

For information about the workflow, see Quick Connect Workflow.

Before you begin

Follow these steps to configure IPv6 as the preferred address family for Cisco IOS XE Catalyst SD-WAN devices in a dual stack environment, using the Quick Connect workflow.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Workflows** > **Quick Connect**.

Step 2 On the **Process Overview** page, click **Next**.

Step 3 Select an option to sync your devices, and click **Next**.

Step 4 On the **Selected devices to bring up** page, select devices, and click **Next**.

Step 5 In the **Dual Stack IPv6 Default** drop-down list, select **True** to set IPv6 as a default connection. Click **Apply**, and then click **Next**.

Here's how **Dual Stack IPv6 Default** affects control connections and BFD sessions:

- **True**: Devices establish an IPv6 control connection with SD-WAN Manager and the SD-WAN Controller they are connected to. BFD sessions use IPv6.
- **False**: Devices establish an IPv4 control connection with SD-WAN Manager and the SD-WAN Controller they are connected to. BFD sessions use IPv4.

The connections from devices to SD-WAN Validator are always dual (IPv4 and IPv6) in a dual IP stack environment, regardless of how**Dual Stack IPv6 Default** is configured.

Step 6 On the **Summary** page, click **Deploy**.

Configure IPv6 as the preferred address family for devices, using CLI commands

Before you begin

Follow these steps to configure IPv6 as the preferred address family for Cisco IOS XE Catalyst SD-WAN devices in a dual stack environment, using CLI commands.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Enable IPv6 on the tunnel interface.

```
interface tunnel1
no shutdown
ipv6 enable
```

Step 3 Enable IPv6.

```
system
ipv6-strict-control true
```

This example configures IPv6 as the preferred address family for devices.

```
interface Tunnel1
 no shutdown
 ip unnumbered GigabitEthernet1
 tunnel source GigabitEthernet1
 tunnel mode sdwan
 ipv6 enable
exit

system
gps-location latitude 32.0
gps-location longitude -100.0
system-ip 10.16.255.14
domain-id 1
site-id 400
ipv6-strict-control true
admin-tech-on-failure
organization-name "Cisco"
vbond vbond
```

Configure IPv6 as the preferred address family for SD-WAN Manager and SD-WAN Controller, using CLI commands

Before you begin

Follow these steps to configure IPv6 as the preferred address family for SD-WAN Manager and SD-WAN Controller in a dual stack environment, using CLI commands.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Enable IPv6.

```
system
ipv6-strict-control true
```

This example configures IPv6 as the preferred address family for SD-WAN Manager and SD-WAN Controllers.

```
system
host-name vm9
system-ip 10.16.255.19
site-id 400
ipv6-strict-control true
port-offset 9
no daemon-restart
admin-tech-on-failure
no vrrp-advt-with-phymac
organization-name "Cisco"
vbond vbond
```

Configure IPv6 as the preferred address family for SD-WAN Manager and SD-WAN Controller, using templates

Before you begin

Follow these steps to configure IPv6 as the preferred address family for SD-WAN Manager and SD-WAN Controller in a dual stack environment, using templates.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**, and click **Add Template**.

Step 3 In the list of devices, select **Controller**.

Step 4 Select **System** from the list of templates.

Step 5 In the **Basic Information** section, for the **Dual Stack IPv6 Default** field, click **On** to enable.

This sets IPv6 as a default connection.

Here's how **Dual Stack IPv6 Default** affects connections:

- **On**: SD-WAN Manager and SD-WAN Controllers establish an IPv6 control connection with other SD-WAN Manager and SD-WAN Controller instances.
- **Off**: SD-WAN Manager and SD-WAN Controllers establish IPv4 control connections.

The connections from SD-WAN Manager and SD-WAN Controller instances to SD-WAN Validator are always dual (IPv4 and IPv6) in a dual IP stack environment, regardless of how**Dual Stack IPv6 Default** is configured.

Step 6 Click **Save**.

Monitor the use of IPv6 as the preferred address family in a dual stack environment, in SD-WAN Manager

After you configure IPv6 as the preferred address family for connections, the BFD connections will be up and running in SD-WAN Manager.

Before you begin

Follow these steps to view the BFD connections in SD-WAN Manager.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

Step 2 Verify the status of the connection in the **BFD** column.

Monitoring IPv6 as the preferred address family in a dual stack environment

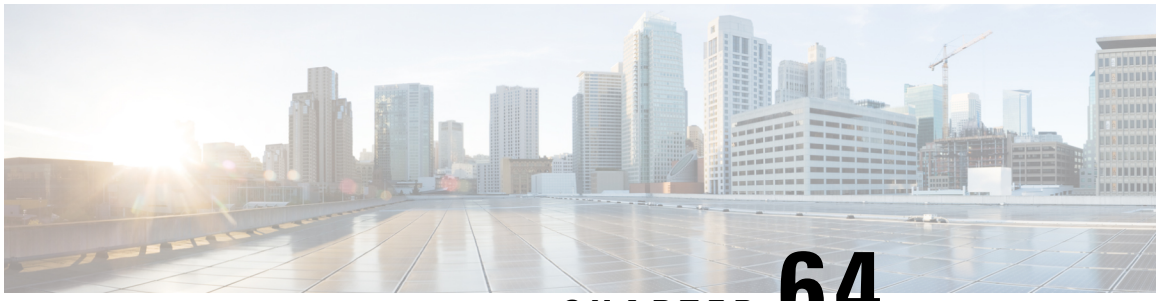
These commands are useful for monitoring the use of IPv6 addressing in a dual stack environment.

Cisco IOS XE Catalyst SD-WAN devices

- **show sdwan control connections**
- **show sdwan control local-properties**
- **show sdwan bfd sessions**
- **show sdwan omp tlocs**
- **show sdwan bfd tloc-summary-list**

SD-WAN Manager and SD-WAN Controller

- **show control connections**
- **show control local-properties**



CHAPTER 64

CLI Templates for Cisco IOS XE Catalyst SD-WAN Devices

- Feature history: CLI templates, on page 955
- CLI templates for Cisco IOS XE Catalyst SD-WAN devices, on page 956
- Using CLI templates in Cisco SD-WAN Manager, on page 957
- Sample configurations for CLI templates, on page 960

Feature history: CLI templates

Developments of CLI templates, release by release.

Table 333: Feature history

Feature Name	Release Information	Description
Device Configuration CLI Templates	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r Cisco vManage 20.1.1	The CLI Templates feature has been updated to support device configuration-based CLIs. You can use these templates to push the device configuration (yang-cli) to devices directly.
CLI Template for Cisco XE SD-WAN Routers	Cisco IOS XE Release 16.11.1a Cisco SD-WAN release 19.1	The CLI Templates for Cisco IOS XE Catalyst SD-WAN device features allow to you configure intent-based CLI templates for Cisco XE SD-WAN routers using Cisco SD-WAN Manager.
VRF Configuration	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Support for VRF configuration increased from a total of 100 to a total of 300 VRFs. Supported on: Cisco ASR 1001-HX and Cisco ASR 1002-HX

CLI templates for Cisco IOS XE Catalyst SD-WAN devices

Describes CLI templates, one method of configuring Cisco IOS XE Catalyst SD-WAN devices.

You can configure CLI templates for Cisco IOS XE Catalyst SD-WAN devices in the following ways:

- Device configuration-based CLI templates for Cisco IOS XE Catalyst SD-WAN devices, on page 957
- Intent-based CLI templates for Cisco IOS XE Catalyst SD-WAN devices, on page 958

Note If you generate a CLI template in a higher version of Cisco SD-WAN Manager and then try to apply it in a lower version, it may not be supported depending on the configuration. In this case, Cisco SD-WAN Manager might also deny access and generate an error message. It is recommended that you use a CLI template generated in an earlier version of Cisco SD-WAN Manager. For example, if you are using Cisco vManage Release 20.7.x, you can use a CLI template generated in Cisco vManage Release 20.6.x and earlier releases.

Benefits of CLI templates

- You can reuse any Cisco vEdge-specific Cisco SD-WAN Manager feature templates for Cisco IOS XE Routers. When you create a device template using Cisco XE SDWAN Feature Templates, Cisco SD-WAN Manager displays the intent-based configuration (vEdge CLI syntax) and the corresponding device-based (Cisco XE SDWAN Routers) configuration. You can examine the intent-based configuration and repurpose that to create a separate CLI template for XE SDWAN routers.
- You can make multiple changes to a CLI template in a single edit.
- You can use a single configuration across multiple devices of the same device models. Variables can be used for rapid bulk configuration rollout with unique per-device settings. Common configurations like system-IP, site-id, hostname, IP addresses, and so on, can be defined as editable variables in the template and the same template can be attached to multiple devices.
- You can define custom length for variables in CLI Templates.
- You can use any existing IOS-XE device intent configuration as input for CLI template.
- Content of a CLI template can be used across multiple IOS-XE device types (common CLIs like VPN, VPN interface, BGP, OSPF and so on).

Restrictions of CLI templates

Auxiliary ports: When using a CLI template for Cisco Integrated Services Routers that have an auxiliary port, do not include commands for auxiliary ports, such as `line aux 0`. Doing so results in an error. These commands may be executed directly on the device.

When you import the CLI template configuration using the command, `show sdwan running-config`, you need to add quotes manually for the CLI template on the Cisco SD-WAN Manager.

From Cisco IOS XE Catalyst SD-WAN Release 17.12.x, policies configured using a Cisco Catalyst SD-WAN Controller template are ignored. To configure policies, navigate to **Configuration** > **Policies** > **Custom Options** > **CLI Policy**, add the policy and activate it for Cisco Catalyst SD-WAN Controller.

Using CLI templates in Cisco SD-WAN Manager

You can configure CLI templates in Cisco SD-WAN Manager using these two methods:

- Device configuration-based CLI templates for Cisco IOS XE Catalyst SD-WAN devices
- Intent-based CLI templates for Cisco IOS XE Catalyst SD-WAN devices

Device configuration-based CLI templates for Cisco IOS XE Catalyst SD-WAN devices

A device configuration-based CLI Template for Cisco IOS XE Catalyst SD-WAN devices is a configuration management tool that:

- enables Cisco SD-WAN Manager (vManage 20.1.1 and later) to specify CLI templates using yang-cli,
- pushes only the difference between device and template configurations to Cisco IOS XE Catalyst SD-WAN devices, and
- provides a preview of configuration changes before deployment.

These templates are used alongside feature templates and policies, including localized and security policies, in Cisco SD-WAN Manager.

Note To configure features not accessible using Cisco SD-WAN Manager, we recommend doing the following:

1. Use the relevant feature template in addition to a CLI add-on feature template.
2. For situations where the previous option is not sufficient, use the device configuration-based CLI templates as described in this section.

Create a CLI template using the device configuration option

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Device Templates**.

Note
In Cisco SD-WAN Release 20.7.x and earlier releases, **Device Templates** is titled as **Device**.

Step 2 From the **Create Template** drop-down list, select **CLI Template**.

Step 3 From the **Device Model** drop-down list, select the type of device for which you are creating the template.

Step 4 In the **Template Name** and **Template Description**, enter a name upto 128 alphanumeric characters and a description upto 2048 alphanumeric characters.

Step 5 Choose **Device configuration**. Using this option, you can provide Cisco IOS XE configuration commands that appear in the output of the `show sdwan running-config` command.

(Optional) To load the running config of a connected device, select it from the Load Running config from reachable device list and click **Search**.

Step 6 In **CLI Configuration**, enter the configuration either by typing it, cutting and pasting it, or uploading a file.

Step 7 To convert an actual configuration value to a variable, select the value and click **Create Variable**. Enter the variable name, and click **Create Variable**.

You can also type the variable name directly, in the format {{*variable-name*}}; for example, {{*hostname*}}.

These variables can be filled in device variables page per device after attaching the template. Values can be entered manually or can be uploaded via a csv file.

Step 8 Click **Add** to save the feature template.

The new device template is displayed in the Device Template table.

Intent-based CLI templates for Cisco IOS XE Catalyst SD-WAN devices

An intent-based CLI template for Cisco IOS XE Catalyst SD-WAN devices is a configuration management tool that:

- allows Cisco SD-WAN Manager to configure CLI templates using intent-based commands,
- supports vEdge device syntax for command input, and
- pushes vEdge syntax-based commands to Cisco IOS XE Catalyst SD-WAN devices in IOS XE syntax.

Intent-based CLI templates enable configuration of Cisco IOS XE Catalyst SD-WAN devices using vEdge syntax via Cisco SD-WAN Manager.

With the support of device configuration-based CLI templates, the intent-based CLI templates will be deprecated. We recommend using the device configuration-based CLI templates as described in Device Configuration-Based CLI Templates for Cisco IOS XE Catalyst SD-WAN Devices.

Using Cisco SD-WAN Manager CLI templates significantly reduces the effort to configure feature templates.

Create a CLI template using the intent option

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Device Templates**.

Note
In Cisco SD-WAN Release 20.7.x and earlier releases, **Device Templates** is titled as **Device**.

Step 2 From the **Create Template** drop-down list, select **CLI Template**.

Step 3 From the **Device Model** drop-down list, select the type of device for which you are creating the template.

Step 4 In the **Template Name** and **Template Description**, enter a name upto 128 alphanumeric characters and a description upto 2048 alphanumeric characters.

Step 5 The configuration of the CLI template can either be intent-based or based on the device configuration:

- **Intent**: If you specify **Intent**, you specify commands in the Cisco vEdge format. If the device you've selected is a Cisco IOS XE Catalyst SD-WAN device, Cisco SD-WAN Manager converts the configuration for the device.
- **Device configuration**: This option is available from Cisco IOS XE Catalyst SD-WAN Release 17.2.1r and onwards and only for Cisco IOS XE Catalyst SD-WAN devices. For this option, you must specify the entire device configuration as it appears in `show sd-wan running config`.

Note
You can only use this feature with the qualified CLIs described in the *Cisco IOS XE Catalyst SD-WAN Qualified Command Reference Guide*.

Example:

You can upload a configuration file using **Select a File** or copy and paste the CLI configuration. Following is an example of an intent-based CLI with variables.

```
system

   host-name {{hostname}}
   system-ip {{system_ip}}
   domain-id 1

   site-id {{site_id}}
   port-offset           1
   admin-tech-on-failure
   organization-name "XYZ"
   logging
    disk
     enable
! !
```

These variables can be filled in device variables page per device after attaching the template. Values can be entered manually or can be uploaded via a csv file.

Step 6 To save the feature template, click **Add**.

What to do next

Sample configurations for CLI templates

System level configuration

Table 334: System level parameters

CLI Template Configuration	Configuration on the Device
system host-name pm4 system-ip 172.16.255.14 overlay-id 1 site-id 400 control-session-pps 300 admin-tech-on-failure sp-organization-name "XYZ Inc Regression" organization-name "XYZ Regression" console-baud-rate 115200 vbond 10.0.12.26 port 12346	system host-name pm4 system-ip 172.16.255.14 overlay-id 1 site-id 400 control-session-pps 300 admin-tech-on-failure sp-organization-name “XYZ Inc Regression” organization-name “XYZ Inc Regression” console-baud-rate 11520 vbond 10.0.12.26 port 12346

AAA Configuration - authentication, authorization, and accounting (AAA) with RADIUS and TACACS+

Table 335: AAA configuration

CLI Template Configuration	Configuration on the Device
aaa auth- order local radius tacacs usergroup basic task system read write task interface read write ! usergroup netadmin ! usergroup operator task system read task interface read task policy read task routing read task security read ! user admin password 6nbbLkA==$ae/DO78l/wluPUohhBU2L6h/ Q.PLkurGvxjRlS9OWB9iTtFwSGNQcABV6F MW57vuEHvo3zp3qdYVinLmMIu/p/ secret $9$3/IL3/UF2F2F3E$J9NKBeKlWrq9ExmHk6F5VAiDMOFQfD.QPAmMxDdxz.c ! ! radius server 10.99.144.200 source-interface GigabitEthernet0/0/1 exit server 10.99.144.201 source-interface GigabitEthernet0/1/0 exit ! tacacs server 10.0.1.1 auth-port 50 vpn 0 source-interface GigabitEthernet0/0/1 key 1 secret-key 8Kcuva0CM871E8czESwV5g/YX4Q8pY1LSNk/+PIDrpCg= exit ! !	aaa group server tacacs+ server-10.0.1.1 server-private 10.0.1.1 timeout 5 key 8vs5hzVg/Z6EeuUdNHTzOwWPsUv9V/50xmcRfShWp3YI= ip tacacs source-interface GigabitEthernet0/0/1 ! aaa group server radius server-10.99.144.200 server-private 10.99.144.200 auth-port 1812 timeout 5 retransmit 3 ip radius source-interface GigabitEthernet0/0/1 ! aaa group server radius server-10.99.144.201 server-private 10.99.144.201 auth-port 1812 timeout 5 retransmit 3 ip radius source-interface GigabitEthernet0/1/0 ! aaa authentication login default local group radius group tacacs+ aaa authorization exec default local group radius group tacacs+ a aa session-id common --- added by default username admin privilege 15 secret 9 $9$3/IL3/UF2F2F3E$J9NKBeKlWrq9ExmHk6F5VAiDMOFQfD.QPAmMxDdxz.c

Logging configuration - configures logging to either the local hard drive or a remote host

Table 336: Logging configuration

CLI Template Configuration	Configuration on the Device
logging disk enable file size 12 file rotate 6 ! server 192.168.13.1 vpn 0 source-interface Loopback1 priority alert exit !	logging disk enable ! ! logging persistent size 75497472 filesize 12582912 logging buffered 512000 --- added by default logging host 192.168.13.1 no logging rate-limit logging source-interface Loopback1 logging persistent

Switch port and VLAN configuration

Table 337: Switch port configuration

CLI Template Configuration	Configuration on the Device
interface GigabitEthernet0/1/4 switchport mode trunk access vlan vlan 10 access vlan name "DHCP Vlan" trunk allowed vlan 10 ! no shutdown vpn 10 name "DHCP VPN" interface Vlan10 description "Vlan 10 Mgmt interface" ip address 10.29.35.1/24 no shutdown ! !	interface GigabitEthernet0/1/4 switchport ios-sw:mode trunk switchport ios-sw:trunk allowed vlan 10 no shutdown no ip address exit interface Vlan10 description Vlan 10 Mgmt interface no shutdown arp timeout 1200 vrf forwarding 10 ip address 10.29.35.1 255.255.255.0 ip mtu 1500 exit

Cellular configuration

Table 338: Cellular configuration - configures cellular controllers and cellular interfaces

CLI Template Configuration	Configuration on the Device
vpn 0 interface Cellular0/2/0 description "Cellular interface" no shutdown ! controller cellular 0/2/0 lte sim max-retry 1 lte failovertimer 7 profile id 1 apn Broadband !	interface Cellular0/2/0 description Cellular interface no shutdown ip address negotiated ip mtu 1428 mtu 1500 exit controller Cellular 0/2/0 lte sim max-retry 1 lte failovertimer 7 profile id 1 apn Broadband authentication none pdn-type ipv4

BGP, OSPF, and EIGRP - configures BGP, OSPF, and EIGRP routing protocols under transport or service VPN

Table 339: BGP, OSPF, and EIGRP configuration

CLI Template Configuration	Configuration on the Device

CLI Template Configuration	Configuration on the Device
vpn1 bgp 2 shutdown distance external 30 distance internal 250 distance local 10 address-family ipv4-unicast network 10.0.100.0/24 redistribute static route-policy route_map redistribute connected route-policy route_map ! neighbor 10.0.100.1 no shutdown remote-as 3 timers keepalive 12 holdtime 20 connect-retry 300 advertisement-interval 123 ! update-source GigabitEthernet0/0/1 ebgp-multihop 1 password $8$9pou4PH9b60B072hcw3MmSSdLCfJk8bVys12lLVb+08= address-family ipv4-unicast vpn 1 router ospf router-id 172.16.255.15 compatible rfc1583 timers spf 200 1000 10000 redistribute connected route-policy route_map max-metric router-lsa administrative area 23 stub interface GigabitEthernet0/0/1 cost 23 authentication type message-digest authentication authentication-key key1 exit exit ! vpn 1 router eigrp 1 af-interface GigabitEthernet0/0/2 no split-horizon exit-af-interface ! address-family ipv4 network 10.1.10.1/32 address-family ipv4 topology base redistribute omp exit-af-topology	

CLI Template Configuration	Configuration on the Device
	router bgp 2 bgp log-neighbor-changes distance bgp 30 250 10 address-family ipv4 unicast vrf 1 neighbor 10.0.100.1 remote-as 3 neighbor 10.0.100.1 activate neighbor 10.0.100.1 ebgp-multihop 1 neighbor 10.0.100.1 maximum-prefix 2147483647 100 neighbor 10.0.100.1 password 0 password neighbor 10.0.100.1 send-community both neighbor 10.0.100.1 timers 12 20 neighbor 10.0.100.1 update-source GigabitEthernet0/0/1 network 10.0.100.0 mask 255.255.255.0 redistribute connected redistribute static route-map route_map exit-address-family ! timers bgp 60 180 router ospf 1 vrf 1 auto-cost reference-bandwidth 100 max-metric router-lsa timers throttle spf 200 1000 10000 router-id 172.16.255.15 default-information originate distance ospf external 110 distance ospf inter-area 110 distance ospf intra-area 110 redistribute connected subnets route-map route_map ! interface GigabitEthernet0/0/1 no shutdown arp timeout 1200 vrf forwarding 1 ip address 10.1.100.14 255.255.255.0 ip redirects ip mtu 1500 ip ospf 1 area 23 ip ospf network broadcast mtu 1500 negotiation auto exit ! router eigrp eigrp-name address-family ipv4 vrf 1 autonomous-system 1 af-interface GigabitEthernet0/0/2 hello-interval 5 hold-time 15 no split-horizon exit-af-interface ! network 10.1.10.1 0.0.0.0 topology base redistribute omp exit-af-topology ! exit-address-family

CLI Template Configuration	Configuration on the Device
	! !

VPN, Interface, and tunnel configuration for WAN and LAN interfaces

Table 340: VPN, Interface, and Tunnel configuration

CLI Template Configuration	Configuration on the Device
vpn 0 interface GigabitEthernet0/2/0 ip address 10.1.14.14/24 tunnel-interface encapsulation ipsec color lte no allow-service bgp allow-service dhcp allow-service dns allow-service icmp no allow-service sshd no allow-service netconf no allow-service ntp no allow-service ospf no allow-service stun allow-service https ! autonegotiate no shutdown ! ip route 0.0.0.0/0 10.1.14.13 vpn 512 interface GigabitEthernet0 ip dhcp-client ipv6 dhcp-client autonegotiate no shutdown ! !	ip route 0.0.0.0 0.0.0.0 10.1.14.13 1 interface GigabitEthernet0/2/0 no shutdown arp timeout 1200 – added by default ip address 10.1.14.14 255.255.255.0 ip redirects --> added by default ip mtu 1500 mtu 1500 negotiation auto --> added by default exit interface Tunnel20 ---> based on the interface 0/2/0 no shutdown ip unnumbered GigabitEthernet0/2/0 no ip redirects ipv6 unnumbered GigabitEthernet0/2/0 no ipv6 redirects tunnel source GigabitEthernet0/2/0 tunnel mode sdwan sdwan interface GigabitEthernet0/2/0 tunnel-interface encapsulation ipsec weight 1 color lte no last-resort-circuit vmanage-connection-preference 5 no allow-service all no allow-service bgp allow-service dhcp allow-service dns allow-service icmp no allow-service sshd no allow-service netconf no allow-service ntp no allow-service ospf no allow-service stun interface GigabitEthernet0 no shutdown arp timeout 1200 vrf forwarding Mgmt-intf ip address dhcp client-id GigabitEthernet0 ip redirects ip dhcp client default-router distance 1 ip mtu 1500 mtu 1500 negotiation auto

Network Address Translation (NAT) over Direct Internet Access (DIA)

Table 341: NAT over DIA

CLI Template Configuration	Configuration on the Device
vpn 201 interface GigabitEthernet0/0/2.2901 description gigi21 ip address 10.201.201.1/24 mtu 1496 no shutdown vrrp 100 track-omp ipv4 10.201.201.3 ! ! ! dhcp-server address-pool 10.201.201.0/24 exclude 10.201.201.1-10.201.201.10 10.201.201.20-10.201.201.22 offer-time 600 lease-time 86400 admin-state up options default-gateway 10.201.201.1 dns-servers 10.99.139.201 tftp-servers 10.99.139.201 ! ! ! ip route 0.0.0.0/0 vpn 0 ! vpn 0 interface GigabitEthernet0/0/0 ip address 172.16.10.1/24 nat udp-timeout 3 tcp-timeout 40 respond-to-ping ! !	interface GigabitEthernet0/0/2.2901 no shutdown encapsulation dot1Q 2901 vrf forwarding 201 ip address 10.201.201.1 255.255.255.0 ip mtu 1496 vrrp 100 address-family ipv4 vrrpv2 address 10.201.201.3 priority 100 track omp shutdown exit exit ip dhcp excluded-address vrf 201 10.201.201.1 10.201.201.10 ip dhcp excluded-address vrf 201 10.201.201.20 10.201.201.22 ip dhcp pool vrf-201-GigabitEthernet0/0/2.2901 option 150 ip 10.99.139.201 vrf 201 lease 1 0 0 default-router 10.201.201.1 dns-server 10.99.139.201 network 10.201.201.0 255.255.255.0 exit ip dhcp use hardware-address client-id no ip dhcp use class ip dhcp use vrf remote ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet0/0/0 overload ip nat translation tcp-timeout 40 ip nat translation udp-timeout 3 ip nat route vrf 201 0.0.0.0 0.0.0.0 global interface GigabitEthernet1/0/2 no shutdown arp timeout 1200 ip address 10.1.15.15 255.255.255.0 ip nat outside ip redirects ip mtu 1500 mtu 1500 negotiation auto

NAT64 configuration

Table 342: NAT64 configuration

CLI Template Configuration	Configuration on the Device
vpn 1 nat64 v4 pool pool1 start-address 10.1.1.10 v4 pool pool1 end-address 10.1.1.100 ! interface GigabitEthernet3 ip address 10.1.19.15/24 nat64 ! autonegotiate no shutdown !	interface GigabitEthernet3 no shutdown arp timeout 1200 vrf forwarding 1 ip address 10.1.19.15 255.255.255.0 negotiation auto nat64 enable nat64 prefix stateful 2001::F/64 vrf 1 nat64 v4 pool pool1 10.1.1.10 10.1.1.100 nat64 v6v4 list global-list pool pool1 vrf 1 nat64 translation timeout tcp 60 nat64 translation timeout udp 1

Multilink and T1/E1 - configures T1/E1 controller and serial, multilink interfaces

Table 343: Configuring Multilink

CLI Template Configuration	Configuration on the Device
card type t1 0 2 controller T1 0/2/0 framing esf clock source internal linecode b8zs cablelength long 0db channel-group 1 timeslots 15 channel-group 2 timeslots 12 channel-group 3 timeslots 10 channel-group 4 timeslots 10 ! interface Multilink1 no shutdown encapsulation ppp ip address 10.1.10.30 255.255.255.0 ppp pap sent-username admin password admin ppp authentication pap ppp multilink ppp multilink links minimum 1 ppp multilink fragment disable ppp multilink group 1 exit interface Serial0/2/0:1 no shutdown encapsulation ppp bandwidth 1536 no ip address load-interval 30 ppp pap sent-username admin password admin ppp authentication pap ppp multilink ppp multilink group 1 exit	interface Multilink1 ip address 10.1.10.30/24 shutdown controller T1 0/2/0 linecode b8zs channel-group 1 channel-group 3 ! ppp pap sent-username admin password admin ppp authentication pap ppp multilink ppp multilink group 1

Local QoS policy

Table 344: Local QoS policy

CLI Template Configuration	Configuration on the Device

CLI Template Configuration	Configuration on the Device
vpn 1 interface GigabitEthernet0/0/1 ip address 10.2.54.15/24 no shutdown access-list MyACL in ! policy class-map class best-effort queue 3 class bulk-data queue 2 class critical-data queue 1 class voice queue 0 ! access-list MyACL sequence 10 match dscp 46 ! action accept class voice ! ! sequence 20 match source-ip 10.1.1.0/24 destination-ip 192.168.10.0/24 ! action accept class bulk-data set dscp 32 ! ! ! sequence 30 match destination-ip 192.168.20.0/24 ! action accept class critical-data set dscp 22 ! ! ! sequence 40 action accept class best-effort set dscp 0 ! ! ! default-action accept ! qos-scheduler be-scheduler class best-effort bandwidth-percent 20 buffer-percent 20 drops red-drop ! qos-scheduler bulk-scheduler	interface GigabitEthernet0/0/1 access-list MyACL in exit class-map match-any best-effort match qos-group 3 ! class-map match-any bulk-data match qos-group 2 ! class-map match-any critical-data match qos-group 1 ! class-map match-any voice match qos-group 0 ! policy-map MyQoSMap class best-effort random-detect bandwidth percent 20 ! class bulk-data random-detect bandwidth percent 20 ! class critical-data random-detect bandwidth percent 40 ! class voice priority percent 20 ! ! policy no app-visibility no flow-visibility no implicit-acl-logging log-frequency 1000 class-map class best-effort queue 3 class bulk-data queue 2 class critical-data queue 1 class voice queue 0 ! access-list MyACL sequence 10 match dscp 46 ! action accept class voice ! ! sequence 20 match source-ip 10.1.1.0/24 destination-ip 192.168.10.0/24 ! action accept class bulk-data set dscp 32 !

CLI Template Configuration	Configuration on the Device
class bulk-data bandwidth-percent 20 buffer-percent 20 drops red-drop ! qos-scheduler critical-scheduler class critical-data bandwidth-percent 40 buffer-percent 40 drops red-drop ! qos-scheduler voice-scheduler class voice bandwidth-percent 20 buffer-percent 20 scheduling llq ! qos-map MyQoSMap qos-scheduler be-scheduler qos-scheduler bulk-scheduler qos-scheduler critical-scheduler qos-scheduler voice-scheduler ! ! ! !	! ! sequence 30 match destination-ip 192.168.20.0/24 ! action accept class critical-data set dscp 22 ! ! ! sequence 40 action accept class best-effort set dscp 0 ! ! ! default-action accept ! ! ! !

Security policy (ZBFW, IPS/IDS, URL-Filtering) configuration

Table 345: Security policy (ZBFW, IPS/IDS, URL-Filtering)

CLI Template Configuration	Configuration on the Device
policy zone internet vpn 0 ! zone zone1 vpn 1 ! zone zone2 vpn 2 ! zone-pair ZP_zone1_internet_fw_policy source-zone zone1 destination-zone internet zone-policy fw_policy ! zone-pair ZP_zone1_zone2_fw_policy source-zone zone1 destination-zone zone2 zone-policy fw_policy ! zone-based-policy fw_policy sequence 1 match source-data-prefix-list subnet1 ! action inspect ! ! default-action pass ! zone-to-nozone-internet deny lists data-prefix-list subnet1 ip-prefix 10.0.10.0/24 ! ! url-filtering url_filter web-category-action block web-categories games block-threshold moderate-risk block text "<![CDATA[<h3>Access" to the requested page has been denied]]>" target-vpns 1 ! intrusion-prevention intrusion_policy security-level connectivity inspection-mode protection log-level err target-vpns 1 ! failure-mode open ! ! !	

CLI Template Configuration	Configuration on the Device
	ip access-list extended fw_policy-seq-1-acl_ 11 permit object-group fw-policy-seq-1-service-og_ object-group subnet1 any ! ip access-list extended utd-nat-acl 10 permit ip any any ! class-map type inspect match-all fw_policy-seq-1-cm_ match access-group name fw_policy-seq-1-acl_ ! policy-map type inspect fw_policy class fw_policy-seq-1-cm_ inspect ! class class-default pass ! ! object-group service fw_policy-seq-1-service-og_ ip ! parameter-map type inspect-global alert on log dropped-packets multi-tenancy vpn zone security ! parameter-map type umbrella global token A5EA676087BF66A42DC4F722C2AFD10D00256274 dnscrypt vrf 1 dns-resolver umbrella match-local-domain-to-bypass ! ! zone security internet vpn 0 ! zone security zone1 vpn 1 ! zone security zone2 vpn 2 ! zone-pair security ZP_zone1_internet_fw_policy source zone1 destination internet service-policy type inspect fw_policy ! zone-pair security ZP_zone1_zone2_fw_policy source zone1 destination zone2 service-policy type inspect fw_policy ! app-hosting appid utd app-resource package-profile cloud-low app-vnic gateway0 virtualportgroup 0 guest-interface 0

CLI Template Configuration	Configuration on the Device
	guest-ipaddress 192.168.1.2 netmask 255.255.255.252 ! app-vnic gateway1 virtualportgroup 1 guest-interface 1 guest-ipaddress 192.0.2.2 netmask 255.255.255.252 ! start ! utd multi-tenancy utd engine standard multi-tenancy web-filter block page profile block-url_filter text <\![CDATA[Access to the requested page has been denied Please contact your Network Administrator]]> ! web-filter url profile url_filter categories block games ! block page-profile block-url_filter log level error reputation block-threshold moderate-risk ! ! threat-inspection profile intrusion_policy threat protection policy connectivity logging level err ! utd global ! policy utd-policy-vrf-1 all-interfaces vrf 1 threat-inspection profile intrusion_policy web-filter url profile url_filter exit !

Configuring NTP

Table 346: Configuring NTP

CLI Template Configuration	Configuration on the Device
ntp server 10.29.43.1 source-interface GigabitEthernet1 version 4 exit ! !	ntp server 198.51.241.229 source GigabitEthernet1 version 4

IPv6 configuration

Table 347: IPv6 configuration

CLI Template Configuration	Configuration on the Device
vpn 1 interface GigabitEthernet3 ipv6 address 2671:123A::1/128 shutdown ! !	interface GigabitEthernet3 shutdown arp timeout 1200 vrf forwarding 1 no ip address ip redirects ip mtu 1500 ipv6 address 2671:123A::1/128 ipv6 redirects mtu 1500 negotiation auto exit vrf definition 1 rd 1:1 address-family ipv4 exit-address-family ! address-family ipv6 exit-address-family ! !

Service configuration

In Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and earlier, only the following configurations under **service** can be configured via CLI templates:

```
service pad
service config
service tcp-keepalives-in
service tcp-keepalives-out
service tcp-small-servers
service udp-small-servers
```

VRF configuration

Configure up to 300 VRFs, with a corresponding subinterface for each VRF. The example configures two VRFs.

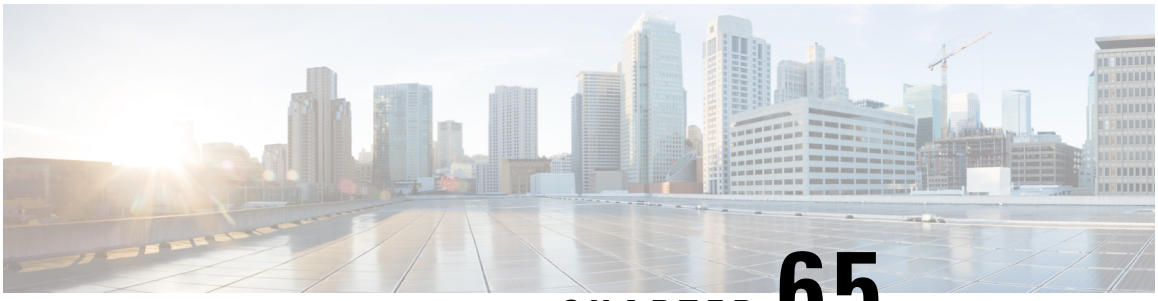
Warning Do not configure VLAN 1. It is reserved for the native VLAN.

Table 348: VRF configuration

CLI Template Configuration	Configuration on the Device
! vpn 2 router bgp 1000 address-family ipv4-unicast redistribute omp address-family ipv6-unicast redistribute omp ! neighbor 192.0.2.2 no shutdown remote-as 2 ! ipv6-neighbor 2001:DB8:2::2 remote-as 2 ! ! interface GigabitEthernet0/0/0.2 ip address 192.0.2.1/24 ipv6 address 2001: DB8:2::1/64 mtu 1496 no shutdown ! ! vpn 3 router bgp 1000 address-family ipv4-unicast redistribute omp address-family ipv6-unicast redistribute omp ! neighbor 192.0.3.2 no shutdown remote-as 3 ! ipv6-neighbor 2001: DB8:3::2 remote-as 3 ! ! interface GigabitEthernet0/0/0.3 ip address 192.0.3.1/24 ipv6 address 2001: DB8:3::1/64 mtu 1496 no shutdown !	

CLI Template Configuration	Configuration on the Device
	vrf definition 2 rd 1:2 address-family ipv4 route-target export 1000:2 route-target import 1000:2 exit-address-family ! address-family ipv6 exit-address-family ! ! router bgp 1000 bgp log-neighbor-changes distance bgp 20 200 20 ! address-family ipv4 vrf 2 redistribute omp neighbor 192.0.2.2 remote-as 2 neighbor 192.0.2.2 activate neighbor 192.0.2.2 send-community both exit-address-family ! address-family ipv6 vrf 2 redistribute omp neighbor 2001:DB8:2::2 remote-as 2 neighbor 2001: DB8:2::2 activate neighbor 2001: DB8:2::2 send-community both exit-address-family ! interface GigabitEthernet0/0/0.2 encapsulation dot1Q 2 vrf forwarding 2 ip address 192.0.2.1 255.255.255.0 ip mtu 1496 ipv6 address 2001:DB8:2::1/64 end vrf definition 3 rd 1:3 address-family ipv4 route-target export 1000:3 route-target import 1000:3 exit-address-family ! address-family ipv6 exit-address-family ! ! router bgp 1000 bgp log-neighbor-changes distance bgp 20 200 20 ! address-family ipv4 vrf 3 redistribute omp neighbor 192.0.3.2 remote-as 3 neighbor 192.0.3.2 activate neighbor 192.0.3.2 send-community both exit-address-family ! address-family ipv6 vrf 3 redistribute omp neighbor 2001:DB8:3::2 remote-as 3

CLI Template Configuration	Configuration on the Device
	neighbor 2001: DB8:3::2 activate neighbor 2001: DB8:3::2 send-community both exit-address-family ! interface GigabitEthernet0/0/0.3 encapsulation dot1Q 3 vrf forwarding 3 ip address 192.0.3.1 255.255.255.0 ip mtu 1496 ipv6 address 2001:DB8:3::1/64 end



CHAPTER 65

CLI Add-On Feature Templates

- Feature history for CLI add-on feature templates, on page 981
- CLI add-on feature templates, on page 982
- Create a CLI add-on feature template, on page 983
- Qualified CLI commands for CLI add-on feature templates, on page 984

Feature history for CLI add-on feature templates

Developments in the CLI add-on feature template, release by release.

Table 349: Feature history

Feature Name	Release Information	Description
CLI Add-On Feature Templates	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r Cisco vManage 20.1.1	This feature adds a new feature template called the CLI add-on feature template. You can use this feature template to attach specific CLI configurations to a device. If a configuration cannot be specified using Cisco SD-WAN Manager but can be configured using the CLI on the device, then you can use this feature template to specify such configurations. You can also use CLI add-on feature templates to add small pieces of CLI configuration, instead of an entire running configuration. This feature is not intended to replace existing feature templates but instead to enhance their functionality. Note that not all CLIs are qualified. For more information, see Qualified CLIs for Cisco IOS XE Release 17.2.1r.
Additional Commands Qualified for CLI Add-On Feature Templates	Cisco IOS XE Catalyst SD-WAN Release Amsterdam 17.2.x Cisco SD-WAN Release 20.1.12	With each release, we qualify commands for use with the CLI add-on feature templates feature. In this release, we qualified additional commands. See the Appendix in the Cisco IOS XE SD-WAN Qualified Command Reference Guide.

CLI add-on feature templates

The CLI add-on feature template is a template that:

- Allows you to add custom device commands not available in standard feature templates.
- Gives the commands in it priority over those present in the feature templates during merges.

When you specify commands using the template, always use the commands as per the syntax displayed in the **show sdwan running-config** output.

For example, for Cisco AAA, the `attempts login` command is not available in Cisco SD-WAN Manager.

By using a CLI add-on feature template, you can specify the `aaa authentication attempts login number` command for a device.

After you create the feature template, ensure that you add it to the device template.

You must define the CLI add-on feature template before you use it in a device template.

Restrictions for CLI add-on feature templates

The CLI add-on feature templates:

- Are supported only on devices running Cisco IOS XE Catalyst SD-WAN Release 17.2.1r or later.
- Allow only one CLI add-on template per device template.
- Require verification of each command by logging in and running it on the intended device before adding it to the CLI add-on feature template.
- Include only supported commands. Using unsupported commands cause errors and configuration failures.

  For example, "`login local`" is not supported.

Create a CLI add-on feature template

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Feature Templates** > **Add Template** to select an appropriate device model.

Note
In Cisco SD-WAN Release 20.7.x and earlier releases, **Feature Templates** is titled as **Feature**.

Step 2 From **Select Devices**, select the devices for which you are creating the template.

Step 3 From **Select Template**, scroll down to the **OTHER TEMPLATES** section.

Step 4 Click **CLI Add-On Template**.

Step 5 In the mandatory **Template Name** field, enter a name for the feature template; In the mandatory **Description** field, enter a description for the device template.

This **Template Name** field can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It does not support spaces or any other characters. The **Description** field can only contain any characters and spaces.

Step 6 In **CLI Configuration**, enter the configuration either by typing it, cutting and pasting it, or uploading a file.

Step 7 To convert an actual configuration value to a variable, select the value and click **Create Variable**. Enter the variable name, and click **Create Variable.** You can also type the variable name directly, in the format `{{variable-name}}`.

Step 8 Click **Save**. The new feature template is displayed in the **Feature Template** table.

Step 9 To use the CLI add-on feature template, edit the device template as follows:

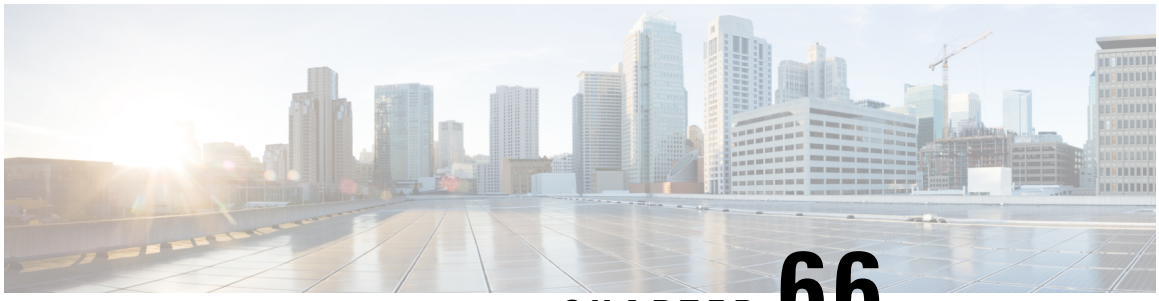
a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

b) Click **Device Templates**.

In Cisco SD-WAN Release 20.7.x and earlier releases, **Device Templates** is titled as **Device**.

Qualified CLI commands for CLI add-on feature templates

For a release-wise list of CLI commands that are qualified for use in SD-WAN Manager CLI templates, see the *Cisco IOS XE Catalyst SD-WAN Qualified Command Reference Guide*.



CHAPTER 66

Configuring and Monitoring P-LTE-450 MHz Modules

Table 350: Feature History

Feature Name	Release Information	Description
Configuring and Monitoring P-LTE-450 modules using Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a and Cisco Catalyst SD-WAN Manager Release 20.18.1	You can configure category P Long-Term Evolution (LTE) 450MHz Pluggable Interface Module (PIM), referred to as P-LTE-450, on rugged series routers using the Ethernet interface in Cisco SD-WAN Manager. Additionally, Cisco SD-WAN Manager enables you to monitor the module's performance through the monitoring dashboard. Cisco IR1101 Rugged Series Router and Cisco IR1800 Rugged Series Router support P-LTE-450 modules.

- Configuring and monitoring P-LTE-450 modules, on page 985
- Prerequisite for configuring P-LTE-450 MHz modules, on page 986
- Restrictions for configuring P-LTE-450 modules, on page 986
- Configure a P-LTE-450 module using Configuration Group and CLI Add-on Profile, on page 987
- Monitor the P-LTE-450 module using Cisco Catalyst SD-WAN Manager, on page 988
- Monitor a P-LTE-450 module using CLI , on page 989

Configuring and monitoring P-LTE-450 modules

A P-LTE-450 module configuration and monitoring is a network management solution that:

- Enables configuration of P-LTE-450 modules through the Ethernet Interface option in Cisco SD-WAN Manager.
- Support real-time monitoring of the P-LTE-450 module's performance on Cisco SD-WAN Manager monitoring dashboard, and
- Simplifies usage of LTE 450 MHz for industrial applications.

P-LTE-450 Pluggable Interface Module

P-LTE-450 PIM enables reliable Long-Term Evolution (LTE) connectivity, specifically tailored for the 450 MHz frequency band, which is widely used in critical communication scenarios such as utility networks, public safety, and rural broadband.

P-LTE-450 module is similar to a Catalyst Cellular Gateway with the following features:

- The modem is an IP passthrough for both IPv4 and IPv6 traffic.
- The management interface, GigabitEthernet 0/1/0 (Base chassis), or GigabitEthernet 0/4/0 (Expansion module), is configured under Cisco IOS XE.

Key difference with LTE modules

P-LTE-450 MHz modules is different from regular LTE modules on the IOS XE platform with a few notable differences. Some of the key differences are:

- IP passthrough is configured on the Gigabit Ethernet interface instead of the cellular interface.
- Allows minimum P-LTE-450 cellular configuration through Cisco IOS XE config mode under Gigabit Ethernet 0/x/0 interface through lte 450 xxx commands.
- Supports GPS connectivity through SMA(f) connector.

  There is no Cisco IOS XE support equivalent to Cellular PIM for GPS features.

Note For more information about , see P-LTE 450 Support and 450MHz Category-4 LTE PIM.

Prerequisite for configuring P-LTE-450 MHz modules

Minimum supported release for configuring P-LTE-450 MHz modules using Cisco SD-WAN Manager is Cisco Catalyst SD-WAN Manager Release 20.18.1 and Cisco IOS XE Catalyst SD-WAN Release 17.18.1a.

- The P-LTE-450 requires Network Advantage license to be recognized under Cisco IOS XE. For more information about licensing policy, see Smart Licensing Using Policy (SLP).
- Thermal Considerations: The host router and the P-LTE-450 module is able to boot up and operate at a lower temperature than the radio module on the P-LTE-450. The radio module will not operate at a temperature below -30° C (-22° F).

Restrictions for configuring P-LTE-450 modules

Avoid Using P-LTE-450 as a Primary Link for PNP

Do not configure the P-LTE-450 module as a primary link for Plug and Play (PNP) deployments.

Platform supports only one P-LTE-450 module

Configure only a single P-LTE-450 module on each platform.

Place P-LTE-450 Only in Supported Slots

Configure the P-LTE-450 module only in slot 0/1 or slot 0/4 due to hardware limitations.

Configure a P-LTE-450 module using Configuration Group and CLI Add-on Profile

To configure a P-LTE-450 module with the **Ethernet Interface** option in Configuration Group and CLI Add-on Profile, follow these steps:

Before you begin

- You must note the username and password that can be found on the sticker label that comes with the P-LTE-450 module. Before performing any P-LTE-450 parameter configuration, set the username and password using CLI.

Procedure

Step 1 Add the following commands in the add-on CLI profile:

```
lte450 band 31
lte450 profile id 2 apn <apn_name> authentication none pdn-type ipv4 vlan <vlan_number>
```

In the preceding command, do the following:

- Configure the username and password of the P-LTE-450 module using the Add-on Profile.
- Provide an appropriate apn_name such as ‘internet’. It should be communicated by your service provider.
- Provide an appropriate vlan_number such as ‘2’.
- Use band ‘`31’ or ‘72’`.

Example:

```
Device:interface GigabitEthernet0/4/0
 no shutdown
 ip address dhcp
 negotiation auto
lte450 credential username admin password VzbhPxZJ42WUhPHB
lte450 band 31
lte450 profile id 2 apn internet authentication none pdn-type ipv4 vlan 2
exit
```

Note
Commands in the CLI add-on Profile override configurations specified by corresponding configuration group features.

Step 2 Configure **Ethernet Interface** in Configuration Group using the **Transport VPN** profile.

Example:

```
Device:interface GigabitEthernet0/4/0.2
 description LTE450 Interface
 no shutdown
 encapsulation dot1Q 2
 ip address dhcp
exit
```

For more information about configuring Ethernet interface in Configuration Group, see Ethernet Interface.

Note
For the the P-LTE-450 module, in the **Interface Name*** field, enter either GigabitEthernet0/4/0.2 or GigabitEthernet0/1/0.2.

What to do next

After configuring the **Ethernet Interface** option, associate the Configuration Group containing the Transport profile to the **Ethernet Interface** option and attach it to the device. For more information, see Deploy a Configuration Group.

Monitor the P-LTE-450 module using Cisco Catalyst SD-WAN Manager

You can monitor the detailed hardware, radio-related, and network-specific information about the P-LTE-450 module using Cisco SD-WAN Manager.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
Step 2 Choose a device from the list of devices that appear on the dashboard.
Step 3 Click **Real Time** in the left pane.
Step 4 Click **Device Options**, and choose a command.

Table 351: Device Options

Device Option	Command	Description
Cellular LTE450 Hardware	`show lte450 0/1/0 hardware`	Displays the details of modem and PIM information
Cellular LTE450 Radio	`show lte450 0/1/0 radio`	Displays the signal quality
Cellular LTE450 Network	`show lte450 0/1/0 network`	Displays the mobile network status

Monitor a P-LTE-450 module using CLI

You can monitor the hardware, radio, and network-specific details of the P-LTE-450 module using the following CLI commands.

show lte450 0/1/0 radio

The following is a sample output from the show lte450 0/1/0 radio command using the keyword lte450. The example shows

Example

```
Device# show lte450 0/1/0 radio
Signal quality
==============
RSSI = -77 dBm
RSRP = -99 dBm
RSRQ = -8 dB
SINR = 5 dB

Antenna signal quality
======================
Main RSSI = -78 dBm
Main RSRP = -101 dBm
Aux RSSI = -77 dB
Aux RSRP = -99 dB
```

show lte450 0/1/0 hardware

The following is a sample output from the show lte450 0/1/0 hardware hardware command using the keyword lte450. The example shows

Example

```
Device# show lte450 0/1/0 <hardware>

 System Status
=============
System time = Wed May 21 05:31:08 2025
Uptime = 2h 33m 48s
Load Average = 2.67 2.56 2.55
Free Disk space = 89204 KB
Free RAM = 54944 KB

Modem information
=================
Modem MAC = 88:5D:90:EF:FF:FF
Modem hardware version = ML620EU
Modem firmware version = 0.3.4.1/ML620EUV13_RELEASE_20240305
Modem temperature = 48.0 deg C

PIM information
===============
PIM MAC = FC:C2:3D:30:E3:F2
PIM hardware version = IPS-701-V3
PIM firmware version = IPS701-v1.3.0-Secured
PIM serial number = 50030301564
Management IPv4 Address = 192.168.200.1
Management IPv6 Address = fd00:ffff:c0:a8c8::1/64
PIM temperature = 49.5 deg C
```

```
GNSS Location Data
==================
Latitude =
Longitude =
Altitude =
Time =

Watchdog Statistics
===================
Hardware watchdog counter = 0
Modem watchdog counter = 0
```

show lte450 0/1/0 network

The following is a sample output from the show lte450 0/1/0 network command using the keyword lte450. The example shows

Example

```
Device# show lte450 0/1/0 network

Mobile network status
=====================
Connection Status = Online
Connection time = 2h 31m 21s
IMSI = 001010123456058
ICCID = 89860001010123456789
MSISDN =
APN-1 IPv4 address = 192.168.4.38
APN-1 IPv6 address = 2001:0468:3000:0008:2001:0468:3000:0008
APN-2 IPv4 address =
APN-2 IPv6 address =
APN-3 IPv4 address =
APN-3 IPv6 address =

Mobile connection information
=============================
IMEI = 862128050313077
System mode = LTE
EPS State = ATTACHED
RRC State = RRC IDLE
CEREG = 1
APN-1 APN name = ims.mnc001.mcc001.gprs
APN-2 APN name =
APN-3 APN name =
Band = 31
PLMN = 00101
Cell ID = 27447298
TAC = 0(1)
PCI = 2
TX power = 0
Bandwidth = 5MHz
LTE RX channel = 9895
LTE TX channel = 27785
Current upload = 0.0 Kbps
Current download = 0.0 Kbps
```

show lte450 0/1/0 all

The following is a sample output from the show lte450 0/1/0 all command using the keyword lte450 The example shows

Example

```
Device# show lte450 0/1/0 all
System Status
=============
System time = Wed May 21 05:31:44 2025
Uptime = 2h 34m 24s
Load Average = 2.47 2.53 2.54
Free Disk space = 89204 KB
Free RAM = 54944 KB

Modem information
=================
Modem MAC = 88:5D:90:EF:FF:FF
Modem hardware version = ML620EU
Modem firmware version = 0.3.4.1/ML620EUV13_RELEASE_20240305
Modem temperature = 48.0 deg C

PIM information
===============
PIM MAC = FC:C2:3D:30:E3:F2
PIM hardware version = IPS-701-V3
PIM firmware version = IPS701-v1.3.0-Secured
PIM serial number = 50030301564
Management IPv4 Address = 192.168.200.1
Management IPv6 Address = fd00:ffff:c0:a8c8::1/64
PIM temperature = 50.0 deg C

GNSS Location Data
==================
Latitude =
Longitude =
Altitude =
Time =

Watchdog Statistics
===================
Hardware watchdog counter = 0
Modem watchdog counter = 0

Mobile network status
=====================
Connection Status = Online
Connection time = 2h 31m 54s
IMSI = 001010123456058
ICCID = 89860001010123456789
MSISDN =
APN-1 IPv4 address = 192.168.4.38
APN-1 IPv6 address = 2001:0468:3000:0008:2001:0468:3000:0008
APN-2 IPv4 address =
APN-2 IPv6 address =
APN-3 IPv4 address =
APN-3 IPv6 address =

Mobile connection information
=============================
IMEI = 862128050313077
System mode = LTE
EPS State = ATTACHED
RRC State = RRC IDLE
CEREG = 1
APN-1 APN name = ims.mnc001.mcc001.gprs
APN-2 APN name =
APN-3 APN name =
```

```
Band = 31
PLMN = 00101
Cell ID = 27447298
TAC = 0(1)
PCI = 2
TX power = 0
Bandwidth = 5MHz
LTE RX channel = 9895
LTE TX channel = 27785
Current upload = 0.0 Kbps
Current download = 0.0 Kbps

Signal quality
==============
RSSI = -77 dBm
RSRP = -99 dBm
RSRQ = -8 dB
SINR = 5 dB

Antenna signal quality
======================
Main RSSI = -78 dBm
Main RSRP = -101 dBm
Aux RSSI = -77 dB
Aux RSRP = -99 dB
```