

Cisco Catalyst SD-WAN NAT Configuration Guide, Release 26.x and Later

First Published: 2026-09-28

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 **Read Me First** 1

CHAPTER 2 **NAT fundamentals and DIA** 3

- Configure NAT 3
- NAT Direct Internet Access 4
  - Information About NAT DIA 6
    - Multiple NAT DIA Methods on an Interface 7
    - Benefits of NAT DIA 7
  - Restrictions for NAT DIA 8
  - Configure NAT DIA 9
    - Configure a NAT Pool and a Loopback Interface 9
    - Configure a NAT DIA Route 16
  - Configure a NAT DIA Route Using the CLI 16
  - Verify NAT DIA Route Configuration 17
  - Advertise NAT Routes Through OMP 17
    - Information About Advertising NAT Routes Through OMP 17
    - Enable NAT Route Advertisements Through OMP Using the CLI 18
    - Verify NAT Route Advertisements Through OMP Using the CLI 19
  - NAT DIA IPv4 over an IPv6 Tunnel 20
    - Information About NAT DIA IPv4 over an IPv6 Tunnel 20
    - Restrictions for NAT DIA IPv4 over an IPv6 Tunnel 21
    - Use Case for NAT DIA IPv4 over an IPv6 Tunnel 21
    - Workflow for Configuring NAT DIA IPv4 over an IPv6 Tunnel 22
    - Configure NAT DIA IPv4 over an IPv6 Tunnel Using the CLI 22

Configure NAT DIA IPv4 over an IPv6 Tunnel Using CLI (Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and later releases) 23
Configure NAT DIA IPv4 over an IPv6 Tunnel Using a CLI Add-On Template 24
Verify NAT DIA IPv4 over an IPv6 Tunnel Configuration 25
Configuration Examples for NAT DIA IPv4 over an IPv6 Tunnel 27
Dialer Interfaces with NAT DIA 27
Information About Using a Dialer Interface with NAT DIA 27
Workflow for a NAT DIA Dialer Interface 28
Restrictions for Using a Dialer Interface with NAT DIA 29
Configure a Dialer Interface with NAT DIA Using a CLI Template 29
Verify a Dialer Interface Configuration 31
Configuration Example for Using a Dialer Interface with NAT DIA 32
NAT DIA Static NAT Mapping with HSRP 33
Information About Static NAT Mapping with HSRP 33
Restrictions for Static NAT Mapping with HSRP 34
Configure Static NAT Mapping with HSRP Using a CLI Template 34
Verify Static NAT Mapping with HSRP 36
Application-Level Gateways with NAT DIA 38
Information About Using ALGs with NAT DIA 38
Restrictions for Using ALGs with NAT DIA 39
Configure ALGs with NAT DIA Using a CLI Template 39
Verify ALG Configuration 40
Port Forwarding with NAT DIA 41
Information About Port Forwarding with NAT DIA 41
Restrictions for Port Forwarding with NAT DIA 43
Configure Port Forwarding with NAT DIA 44
Configure Port Forwarding with NAT DIA Using a CLI Template 46
Verify Configuration of Port Forwarding with NAT DIA 47
NAT High-Speed Logging 48
Information About NAT HSL 48
Restrictions for NAT HSL 48
Prerequisites for NAT HSL 49
Best Practices for NAT HSL 49
Configure NAT HSL Using a CLI Template 49

Verify NAT HSL Configuration 49
Source Port Preservation for Known Cisco Catalyst SD-WAN Ports 50
Information About Source Port Preservation for the Well-Known Cisco Catalyst SD-WAN Ports 50
Features of Source Port Preservation 51
Prerequisites for Source Port Preservation 52
Restrictions for Source Port Preservation 52
Configure Source Port Preservation for DIA Interface Overload Using a CLI Template 52
Configure Source Port Preservation for DIA Pool Overload Using a CLI Template 53
Configure Source Port Preservation for DIA Loopback Overload Using a CLI Template 54
Verify Source Port Preservation 54
Destination NAT 55
Information about Destination NAT 55
Restrictions for Destination NAT 56
Use Case for Destination NAT 56
Configure Destination NAT Using a CLI Template 57
Verify Destination NAT 57
Troubleshoot Destination NAT 58

CHAPTER 3 **NAT DIA Tracker** 59
Information About NAT DIA Tracking 60
ICMP Endpoint Tracker for NAT DIA 61
Supported Devices for ICMP Trackers 62
Restrictions for ICMP Trackers 62
Supported Interfaces for NAT DIA Tracker 63
Restrictions for NAT DIA Tracker 63
Workflow for NAT DIA Tracker on IPv4 Interfaces 64
Configure NAT DIA Tracker on IPv4 Interfaces in Cisco SD-WAN Manager 64
Configure NAT DIA Tracker 66
Configure NAT DIA Tracker on IPv4 Interfaces using Configuration Groups in Cisco SD-WAN Manager 66
Configure NAT DIA Tracker on IPv4 Interfaces Using the CLI 68
Configure an ICMP Tracker for NAT DIA Using the CLI 69
Configuration Examples for NAT DIA Tracking on IPv4 Interfaces Using the CLI 70

Stabilize NAT DIA Tracker Status 71
Monitor NAT DIA Tracker Configuration on IPv4 Interfaces 72
Verify the Configurations for NAT DIA Tracker on IPv4 Interfaces 73
Workflow for NAT DIA Tracker on IPv6 Interfaces 75
Configure NAT DIA Tracker on IPv6 Interfaces using Configuration Groups in Cisco SD-WAN Manager 75
Configure NAT DIA Tracker on IPv6 Interfaces using a CLI Template 78
Verify the Configurations for NAT DIA Tracker on IPv6 Interfaces 82

CHAPTER 4 **Service-Side NAT** 85
Information About Service-Side NAT 86
Benefits of Service-Side NAT 88
Traffic Flows for Service-Side NAT 88
Restrictions for Service-Side NAT 88
Configure Service-Side NAT 89
Create and Apply a Centralized Data Policy for Service-Side NAT 89
Configure Service-Side Dynamic NAT 90
Configure Service-Side Static NAT 91
Configure Service-Side Port Forwarding for NAT 93
Configure Service-Side NAT Using the CLI 94
Verify Configuration of Service-Side NAT 97
Configuration Examples for Service-Side NAT 99
Intra-VPN Service-Side NAT 99
Information About Intra-VPN Service-Side NAT 99
Benefits of Intra-VPN Service-Side NAT 100
Restrictions for Intra-VPN Service-Side NAT 100
Configure Intra-VPN Service-Side NAT 100
Configure Intra-VPN Service-Side NAT Using a CLI Add-On Template 101
Configuration Examples for Intra-VPN Service-Side NAT 101
Service-Side Conditional Static NAT 103
Information About Service-Side Conditional Static NAT 103
Benefits of Service-Side Conditional Static NAT 103
Restrictions for Service-Side Conditional Static NAT 103
Workflow for Configuring Service-Side Conditional Static NAT 103

Configure Service-Side Conditional Static NAT Using the CLI 103
Verify Service-Side Conditional Static NAT Configuration 104
Service-Side Static Network NAT 105
Information About Service-Side Static Network NAT 105
Benefits of Service-Side Static Network NAT 105
Restrictions for Service-Side Static Network NAT 105
Configure Service-Side Static Network NAT 105
Configure Service-Side Static Network NAT Using the CLI 106
Verify Service-Side Static Network NAT Configuration 107
Application-Level Gateways with Service-Side NAT 107
Information About Using ALGs with Service-Side NAT 108
Benefits of Using ALGs with Service-Side NAT 108
Restrictions for Using ALGs with Service-Side NAT 108
Configure ALGs with Service-Side NAT Using a CLI Template 108
Verify ALG Configuration 110

CHAPTER 5 **Service-side NAT Object Tracker 113**
Feature history of service-side NAT object tracker 113
Service-side NAT object tracker 113
Restrictions for service-side NAT object tracker 114
Use case for service-side NAT object tracker 114
How to configure the service-side NAT with an object tracker 114
Configure service-side NAT object tracker using templates 115
Configure service-side NAT object tracker using CLI commands 116
Configure service-side NAT object tracker using a CLI add-on template 118
Associate the service-side NAT object tracker with a NAT pool using a Cisco VPN template 118
Verify the service-side NAT object tracker configuration 119
Monitor service-side NAT object tracker 120

CHAPTER 6 **Configure NAT64 121**
Configure NAT64 121
NAT64 direct internet access 121
Information about NAT64 DIA 122
How NAT64 DIA works 122

Benefits of NAT64 DIA 122
Restrictions for NAT64 DIA 123
Configure NAT64 DIA and a DIA route 123
Configure NAT64 DIA 124
Configure a NAT64 DIA route 125
Configure a NAT64 DIA route using the CLI 126
Verify NAT64 DIA route configuration 127
Configuration example for NAT64 DIA 127
Service-side NAT64 128
Information about service-side NAT64 128
How service-side NAT64 works 129
Benefits of service-side NAT64 129
Use cases for service-side NAT64 129
Prerequisites for service-side NAT64 130
Restrictions for service-side NAT64 130
Configure service-side NAT64 130
Enable service-side NAT64 using a feature template 130
Configure a service-side NAT64 pool using a configuration group 131
Configure a service-side NAT64 pool 132
Configure service-side NAT64 using the CLI 133
Verify configuration of service-side NAT64 134
Configuration examples for service-side NAT64 135
Mapping of address and port using encapsulation with NAT64 136
Information about MAP-E with NAT64 137
Components of a MAP-E configuration with NAT64 137
Benefits of MAP-E with NAT64 138
Restrictions for MAP-E with NAT64 139
Workflow for MAP-E with NAT64 139
Configure MAP-E with NAT64 using a CLI template 140
Verify MAP-E with NAT64 configuration 142

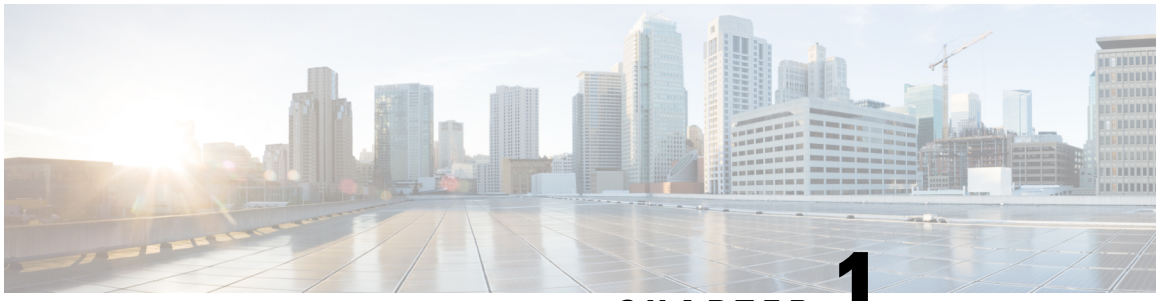
CHAPTER 7 **Configure NAT66** 145
Feature history: Configure NAT66 145
Information about NAT66 DIA 147

How NAT66 DIA works 148
NAT66 DIA With centralized data policy 149
Benefits of NAT66 DIA 151
Restrictions for NAT66 DIA 152
Configure NAT66 DIA and a DIA route 153
Configure NAT66 DIA 153
Enable DHCPv6 prefix delegation using a CLI add-on template 154
Configure a NAT66 DIA route 155
Configure NAT66 DIA using stateless DHCP through Cisco Catalyst SD-WAN Manager 156
Configure NAT66 DIA using stateless DHCP through a feature template 157
Configure NAT66 DIA using the CLI 157
Verify NAT66 DIA and DIA route configuration 159
Configuration example for NAT66 DIA 161
NAT66 DIA Route redistribution 162
Information about NAT66 route redistribution 162
Configure NAT66 DIA route redistribution using a feature template 163
Configure NAT66 DIA route redistribution into BGP using a feature template 163
Configure NAT66 DIA route redistribution into OSPFv3 using a feature template 163
Configure NAT66 DIA route redistribution using CLI based configuration group 164
Configure NAT66 DIA route redistribution into BGP using CLI based configuration group 164
Configure NAT66 DIA route redistribution into OSPFv3 using CLI based configuration group 166
Dialer interfaces with NAT66 DIA 167
Information about dialer interface with NAT66 DIA 167
Benefits of using a dialer interface with NAT66 DIA 168
Workflow for IPv6 traffic through a NAT DIA dialer interface 168
Restrictions for using a dialer interface with NAT66 DIA 169
Configure a dialer interface with NAT66 DIA 169
Configure a dialer interface with NAT66 DIA using configuration groups 170
Configure a dialer interface with NAT66 DIA using a CLI template 170
Verify a dialer interface configuration for NAT66 DIA 172
Configuration example for using a dialer interface with NAT66 DIA 174

CHAPTER 8 **Feature history: Site-local failover for NAT DIA** 175
Information About Site-Local Failover for NAT DIA 175

Benefits of Site-Local Failover for NAT DIA 177
Restrictions for Site-Local Failover for NAT DIA 177
Configure Site-local failover for NAT DIA 177
Verify Site Local Failover For NAT DIA 179

CHAPTER 9 **Support document links** 183
Support articles 183
Submit feedback for a support document 184
Disclaimer and caution 184



CHAPTER 1

Read Me First

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Related References

- Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations
- Cisco Catalyst SD-WAN Device Compatibility

User Documentation

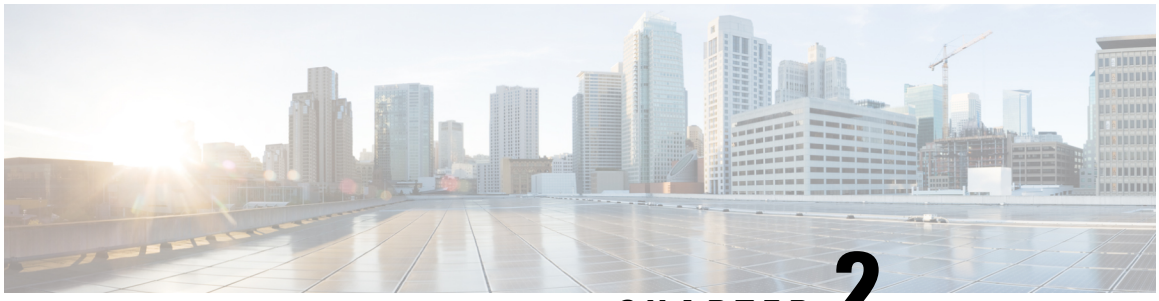
- User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17

Communications, Services, and Additional Information

- Sign up for Cisco email newsletters and other communications at: Cisco Profile Manager.
- For information on the latest technical, advanced, and remote services to increase the operational reliability of your network visit Cisco Services.
- To browse and discover secure, validated enterprise-class apps, products, solutions, and services, visit Cisco Devnet.
- To obtain general networking, training, and certification titles from Cisco Press Publishers, visit Cisco Press.
- To find warranty information for a specific product or product family, visit Cisco Warranty Finder.
- To view open and resolved bugs for a release, access the Cisco Bug Search Tool.
- To submit a service request, visit Cisco Support.

Documentation Feedback

To provide feedback about Cisco technical documentation use the feedback form available in the right pane of every online document.



CHAPTER 2

NAT fundamentals and DIA

- Configure NAT, on page 3
- NAT Direct Internet Access, on page 4

Configure NAT

Cisco IOS XE Catalyst SD-WAN includes the following types of Network Address Translation (NAT) configuration:

- NAT Direct Internet Access (DIA): Allows remote sites to route traffic directly to the internet rather than routing the traffic to a central site or data center.
- NAT service-side: Allows you to configure inside and outside NAT on data traffic traveling to and from the service hosts of the network overlay. Service-side NAT translates data traffic, of inside and outside host addresses, that match a configured centralized data policy.

NAT is designed for IP address conservation. NAT enables private IP networks that use nonregistered IP addresses to connect to the internet. NAT operates on a device, usually connecting two networks. Before packets are forwarded onto another network, NAT translates the private (not globally unique) addresses in the internal network into legal addresses.

NAT allows a single device to act as an agent between the internet (or public network) and a local network (or private network), which means that only a single unique IP address is required to represent an entire group of computers to anything outside their network.

Note When NAT performs maintenance operations, it needs to lock the NAT database. When the NAT database is locked, NAT does not process any packets for translations. Typically, NAT maintenance operations are less than a second to a few seconds. Usually, NAT sending out untranslated packets is not an issue because these packets are dropped by an ISP.

Configure the following command to ensure that NAT drops packets when performing NAT database updates:

```
ip nat service modify-in-progress drop
```

NAT Direct Internet Access

Table 1: Feature History

Feature Name	Release Information	Description
Support for NAT Pool, Static NAT, and NAT as a Loopback Interface	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r Cisco vManage 20.1.1	This feature supports NAT configuration for loopback interface addresses, NAT pool support for Direct Internet Access (DIA), and static NAT.
Advertise NAT Routes Through OMP	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This feature allows you to advertise NAT routes through the Cisco Catalyst SD-WAN Overlay Management Protocol (OMP) to the branch routers. You can configure this feature only through a Cisco SD-WAN Manager device CLI template.
Support for NAT DIA IPv4 over an IPv6 Tunnel	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	This feature provides support for an IPv4 client to access IPv4 servers when using an IPv6 network. IPv4 traffic is routed to the internet over an IPv6 tunnel. You can configure NAT DIA IPv4 over an IPv6 tunnel using the CLI or a CLI add-on template.
Support for PPP Dialer Interfaces with NAT DIA	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	This feature adds support for the following Point-to-Point Protocol (PPP) dialer interfaces: PPP over Ethernet (PPPoE), PPP over Asynchronous Transfer Mode (PPPoA), and PPP over Ethernet Asynchronous Transfer Mode (PPPoEoA). You can use the PPP dialer interfaces to access IPv4 services and sites.

Feature Name	Release Information	Description
ALG Support for NAT DIA and Zone-Based Firewalls	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	This feature provides support for an application-level gateway (ALG) that translates the IP address inside the payload of an application packet. Specific protocols such as Domain Name System (DNS), FTP, and Session Initiation Protocol (SIP) require a NAT ALG for translation of the IP addresses and port numbers in the packet payload.
Support for Port Forwarding with NAT DIA	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	With this feature, you can define one or more port-forwarding rules to send packets received on a particular port from an external network to reach devices on an internal network. Before Cisco IOS XE Catalyst SD-WAN Release 17.9.1a and Cisco vManage Release 20.9.1, port forwarding was available for service-side NAT only.
Support for NAT High-Speed Logging	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1 — Also Cisco IOS XE Release 17.6.4 and later 17.6.x releases Cisco vManage Release 20.6.4 and later 20.6.x releases	This feature provides the ability to enable or disable high-speed logging (HSL) of all translations by NAT. You can configure NAT HSL using a device CLI template or CLI add-on feature template.
Support for Source Port Preservation for well-known Cisco Catalyst SD-WAN Ports	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco vManage Release 20.10.1	This feature allows preservation of well-known Cisco Catalyst SD-WAN ports during NAT.
Destination NAT Support	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature changes the destination address of packets passing through WAN edge devices. Destination NAT is used to redirect traffic destined to a private address to the translated destination public IP address.

Feature Name	Release Information	Description
Port Forwarding with NAT DIA Using a Loopback Interface	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature supports port forwarding with NAT DIA by using a loopback interface. You can configure a loopback interface by using either device CLI templates or CLI add-on feature templates.
ALG Support Enhancement for NAT DIA and Zone-Based Firewalls	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	The ALG support for NAT DIA is extended for the following protocols: • Trivial File Transfer Protocol (TFTP) • Point-to-Point Tunneling Protocol (PPTP) • Sun Remote Procedure Call (SUNRPC) • Skinny Client Control Protocol (SCCP) • H.323
Support for Configuring Multiple NAT Types	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	This feature supports configuration of multiple NAT types—interface, loopback interface, or NAT pool for Direct Internet Access (DIA). Use the centralized data policy to assign rules for combining various NAT types for DIA traffic egressing the edge router. You can also bypass NAT altogether.

Information About NAT DIA

NAT DIA allows branch sites to route traffic directly to the internet rather than having to go through a central site to be inspected. This allows cloud-based applications to go directly to the internet and to cloud-service providers without having to use unnecessary bandwidth.

NAT DIA Flow-Stickiness

Minimum supported releases: Cisco IOS XE Release 17.6.1a, Cisco vManage Release 20.6.1

When NAT DIA is configured with centralized data policy with application match, the application flows subject to NAT DIA policy may get reset due to path change. For example, when you have a data policy matching an application list and the action is NAT DIA, the first few packets may not be identified by deep packet inspection (DPI). So, the packets not matching NAT DIA application policy follow routing to the Cisco

Catalyst SD-WAN overlay path. When the flow is identified, the later packets of the flow will take the NAT DIA path as defined by the data policy. This path change results in a flow reset as different paths means different client source or port combination towards the server and the server resets the unknown TCP flows.

The Flow-Stickiness feature is enabled to record the flow level state of the NAT path. If the first packet of the flow is non-NAT, it keeps the rest of the packets of this flow to non-NAT paths. If the first packet flow is via the NAT DIA path, it keeps the rest of the packets of this flow to the NAT DIA path. It is enabled by default with NAT DIA data policy.

To disable flow stickiness, use the command **flow-stickiness-disable** under the localized policy using CLI add-on template.

Multiple NAT DIA Methods on an Interface

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

A NAT configuration can include an interface overload, an interface DIA pool, or an interface loopback. Having the ability to allow multiple NAT pools for an interface while also having a default interface for any traffic that doesn't match a pool provides a robust option for configuring NAT DIA.You can configure Cisco IOS XE Catalyst SD-WAN devices so that the NAT DIA traffic from an internal subnet is assigned to one public IP address, while all other NAT DIA traffic falls back to a default interface.

For example, your organization might have a requirement to apply NAT to IPs of a certain subset of phones to a different public address than the majority of internet traffic. You might also want to use public cloud services for voice and require all traffic for a voice subnet to use specific IP addresses. These scenarios require you to have multiple NAT pools for specific DIA traffic while also having a default NAT interface for regular traffic.

You can configure multiple NAT DIA methods using CLI commands, feature templates, or configuration groups. After configuring the interface with multiple NAT types, configure the centralized traffic policy to create rules based on the match–action condition. Based on the configured policy match condition and the exit DIA interface that you specify, the policy chooses the appropriate NAT method for source address translation.

If multiple NAT DIA methods are present, traffic can exit on any DIA interface and the corresponding NAT type is chosen. To ensure traffic egresses through a particular NAT DIA interface, configure the centralized traffic policy to include Local TLOC option and assign a preferred TLOC color to the NAT DIA interface. Based on the match condition, the policy selects the DIA interface associated with preferred color for egress.



Note

- This feature supports only IPv4 addresses.
- For a given match condition (sequence in data policy), multiple source DIA interfaces or source DIA pools can’t correspond to the same match interface. However, they can be provided in different sequences. For example, if the default NAT type is interface overload then the second method (match-interface) for the same interface cannot be interface overload. However, the second method can be a NAT pool or a loopback interface.

Benefits of NAT DIA

- Enables good application performance

- Contributes to reduced bandwidth consumption and latency
- Contributes to lower bandwidth cost
- Enables improved branch office user experience by providing DIA at remote sites

Restrictions for NAT DIA

- NAT64:
  - NAT DIA pool is not supported for NAT64.
- Multiple NAT DIA:
  - Support for multiple NAT DIA pools per interface requires Cisco IOS XE Catalyst SD-WAN Release 17.14.1a or later.
- Multiple NAT mappings:
  - A NAT mapping can include an interface overload, an interface DIA pool, or an interface loopback. Multiple NAT mappings for the same interface require Cisco IOS XE Catalyst SD-WAN Release 17.14.1a or later.
  - The VPN redundancy mapping should match NAT DIA pool redundancy mapping model or provide an option on Cisco SD-WAN Manager to accept redundancy number as input field, so that the correct VPN mapping is used for NAT DIA.
- Shared IP address:
  - An IP address used in a NAT pool cannot be shared with an interface address or static address mappings.
- Requirement of at least one NAT on WAN interface:
  - Cisco SD-WAN Manager does not configure a NAT DIA route in a **Cisco VPN** template, which is the service-side VPN, if at least one form of NAT is not enabled on the WAN interface.
- Non-tunnel traffic
  - NAT DIA or non-tunnel traffic is not supported for L3 TLOC extension.
- Port allocation limit
  - When configuring NAT DIA for a single IP address, approximately 55,000 ports can be translated for TCP and UDP protocols each, providing up to 110,000 port translations in total.
  - When configuring NAT DIA for multiple IP addresses (NAT pool), approximately 64,000 ports can be translated for TCP and UDP protocols for each IP address in the pool. IP addresses from the NAT pool are chosen randomly and are not based on a round-robin method.
- NAT determines the exit interface for a packet based on the best path selection for each packet individually. After selecting the exit interface, NAT uses the NAT mapping linked to that interface to choose the source IP for translation and establishes a session for that flow. All subsequent packets in the same flow

exiting via the same interface use this NAT session for translation. If the interface undergoes UP or DOWN state changes, the best path selection changes, causing packets to exit through a different interface.

- NAT translation is created for DIA traffic even when a zone-based firewall (ZBFW) feature drops traffic.

Configure NAT DIA

Workflow for Enabling NAT DIA

1. Enable NAT by editing an existing **Cisco VPN Interface Ethernet** template. From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, you can configure multiple NAT types for an interface.
   a. Configure interface overload (default).



Note From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, the first NAT type that you configure becomes the default or the primary NAT method for the **Cisco VPN Interface Ethernet**. It can be either an interface overload, NAT pool, or a loopback interface.

Any additional NAT types that you configure for that interface become secondary NAT methods.

   b. Configure a NAT pool.
   c. Configure a loopback interface.
   d. (Optional) Configure static NAT.

2. Configure a NAT DIA route using a **Cisco VPN** template, which is a service-side VPN template used to direct user traffic from a service VPN directly into the internet transport.

Configure a NAT Pool and a Loopback Interface

A NAT pool is a range of IPv4 addresses that are allocated for NAT translation as needed.

You can specify a software-only interface called a loopback interface to emulate a physical interface. A loopback interface is a virtual interface on a device that remains up (active) until you disable it. From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, you can configure multiple NAT types for an interface.

Configure NAT DIA Using Configuration Groups

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click **…** adjacent to the configuration group name and choose **Edit**.
3. Click **Transport & Management Profile**.
4. Edit the **VPN0** feature by clicking **…** under **Actions**.
5. Click **Add Sub-Feature** and choose **Ethernet Interface**.
6. Click **NAT**.
7. Click **IPv4 Settings**.

8. In the **NAT** drop-down list, change the scope from **Default** to **Global**, and click **On** to enable NAT.
9. Configure the **NAT Type** by choosing from one of the following options:
   - interface
   - pool
   - loopback

   From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, click **Add Multiple NAT** to configure more NAT pools.

   The default is the **Interface** option.
10. In the **NAT Type** field, click the **Pool** option and enter the following NAT pool parameters:

Table 2: NAT Pool Parameters

Parameter Name	Description
Range Start	Enter a starting IP address for the NAT pool. **a.** Change the scope from **Default** to **Global** to enable the field. **b.** Enter the starting IP address for the NAT pool.
Range End	Enter a closing IP address for the NAT pool. **a.** Change the scope from **Default** to **Global** to enable the field. **b.** Enter the last IP address for the NAT pool.
Prefix Length	Enter the NAT pool prefix length.
UDP Timeout	Enter the time when NAT translations over UDP sessions time out. Range: 1 to 8947 minutes Default: 1 minute
TCP Timeout	Enter the time when NAT translations over TCP sessions time out. Range: 1 to 8947 minutes Default: 60 minutes (1 hour)

11. Configure a loopback interface. From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, click **Add Multiple NAT** to configure multiple loopback interfaces.

    In the **NAT Type** field, click the **Loopback** option and enter the name of the loopback interface.

Note For a given match condition (sequence in data-policy), multiple source DIA interfaces or source DIA pools can't correspond to the same match interface. However, they can be provided in different sequences. For example, if the default NAT type is interface overload then the second method (match-interface) for the same interface cannot be interface overload. However, the second method can be a NAT pool or a loopback interface.

12. Click **Save**.

Configure Match and Action Parameters Using a Policy Group

After you have configured the multiple NAT types using configuration groups, configure the **Application & Priority SLA** policy to apply match-action conditions. When the NAT DIA traffic matches the conditions in the match portion of a centralized data policy, the packet is accepted. Then, you can associate action parameters with accepted packets.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** > **Application & Priority SLA**.
2. Click **…** adjacent to the policy group name and choose **Edit**.
3. Click the **Advanced Layout** button on the top-right corner of the page to swtich to the advanced view.
4. Click **Add Traffic Policy**, provide the details for the new traffic policy, and choose **Accept**.
5. Click **Add**.
6. Click **Add Rules** and enter a name and sequence for the traffic.
7. Click **Add Match** to associate a match condition with the rule.
8. Click **Add Action** and choose **NAT VPN** to associate a NAT DIA action with the match condition specified in the previous step.
   - **DIA Pool**: Enter a comma-separated list of NAT DIA pools. You can enter up to 4095 NAT pools.
   - **DIA Interface**: Enter a comma-separated list of NAT DIA interfaces.
   - **ByPass**: Traffic exits the DIA interface associated with public internet without applying NAT to the source IP address.

Configure NAT DIA Using a Feature Template

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

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

3. To edit a **Cisco VPN Interface Ethernet** template, click **…** adjacent to the template name and choose **Edit**.
4. Click **NAT**.

5. Click **IPv4**.
6. In the **NAT** drop-down list, change the scope from **Default** to **Global**, and click **On** to enable NAT.
7. Configure interface overload.

   In the **NAT Type** field, ensure that **Interface** is enabled for interface overload mode.

   The default is the **Interface** option.
8. Configure a NAT pool. From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, click **Add Multiple NAT** to configure more NAT pools.

   In the **NAT Type** field, click the **Pool** option and enter the following NAT pool parameters:

   Table 3: NAT Pool Parameters

Parameter Name	Description
NAT Pool Range Start	Enter a starting IP address for the NAT pool. **a.** Change the scope from **Default** to **Global** to enable the field. **b.** Enter the starting IP address for the NAT pool.
NAT Pool Range End	Enter a closing IP address for the NAT pool. **a.** Change the scope from **Default** to **Global** to enable the field. **b.** Enter the last IP address for the NAT pool.
NAT Pool Prefix Length	Enter the NAT pool prefix length.
Overload	Click **On** to enable per-port translation. The default is **On**. **Note** If **Overload** is set to **Off**, only dynamic NAT is configured on the end device. Per-port NAT is not configured.
UDP Timeout	Enter the time when NAT translations over UDP sessions time out. Range: 1 to 8947 minutes Default: 1 minute
TCP Timeout	Enter the time when NAT translations over TCP sessions time out. Range: 1 to 8947 minutes Default: 60 minutes (1 hour)

9. Configure a loopback interface. From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, click **Add Multiple NAT** to configure multiple loopback interfaces.

   In the **NAT Type** field, click the **Loopback** option and enter the following values:

   Table 4: NAT Loopback Parameters

Parameter	Description
NAT Inside Source Loopback Interface	Specify the IP address of the loopback interface.
UDP Timeout	Enter the time when NAT translations over UDP sessions time out. Default: 1 minute. Range: 1-65536 minutes
TCP Timeout	Enter the time when NAT translations over TCP sessions time out. Default: 60 minutes (1 hour). Range: 1-65536 minutes



Note When a device from one template with a NAT configuration on one virtual interface is moved to another template without NAT configuration on another virtual interface, you must first disable the NAT configurations and then remove the virtual interface before enabling NAT configurations again. You disable NAT in the template to which the device was attached initially.

10. Click **Update**.

Configure Match and Action Parameters Using the Centralized Data Policy

After you have configured the multiple NAT types using a feature template, configure the traffic rules in the centralized data policy to apply match-action conditions. When the NAT DIA traffic matches the conditions in the match portion of a centralized data policy, the packet is accepted. Then, you can associate action parameters with accepted packets. For more information, about configuring the traffic policy, see Configure Traffic Rules in the *Cisco Catalyst SD-WAN Policies Configuration Guide* . After you have created a traffic policy, specify the match and action conditions:

1. Configure the traffic data policy.
2. After creating a custom sequence type in the traffic data policy, click **Sequence Rule** and configure the the details for the new traffic policy and choose **Accept**.
3. Configure the match condition. For more information, see Match Parameters - Data Policy in the *Cisco Catalyst SD-WAN Policies Configuration Guide*.
4. Click **Actions** > **Accept**.
5. Click **NAT VPN** and choose from the following NAT DIA actions to associate with the match condition that you specify in the previous step:
   - **ByPass**: Traffic exits the DIA interface associated with public internet without applying NAT to the source IP address.
   - **Pool**: Enter a comma-separated list of NAT DIA pools. You can enter up to 4095 NAT pools.

- **Interface**: Enter a comma-separated list of NAT DIA interfaces. You can enter up to four interfaces.

Configure Multiple NAT Types Using CLI

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

1. Configure a NAT DIA interface.

```
interface interface-name
 ip address ip-address prefix/length
 no ip redirects
 load-interval interval-number
 negotiation auto
 ip nat outside
 !
```

2. Configure multiple NAT DIA methods where the default NAT method is a NAT pool and the alternative or secondary NAT method is an interface overload.

```
ip nat inside source list list-name pool pool-name overload egress-interface
interface-name
```

3. Configure the alternative or secondary NAT method by using the **match-interface** keyword. Here, the alternative or secondary NAT method is the interface overload.

```
ip nat inside source list list-name interface interface-name overload match-interface
interface-name
```

   For more information about the match-interface keyword, see the ip nat inside source command in the *Cisco Catalyst SD-WAN Qualified Command Reference* guide.

The following is a sample configuration for configuring multiple NAT DIA where the default NAT method is using a NAT pool and the alternative or secondary NAT method is using interface overload with match-interface:

```
interface GigabitEthernet1
 ip address 10.1.1.1 255.255.255.0
 no ip redirects
 load-interval 30
 negotiation auto
 ip nat outside
 !
 ip nat inside source list dia-list pool natpool1 overload egress-interface GigabitEthernet1

 ip nat inside source list dia-list interface GigabitEthernet1 overload match-interface
GigabitEthernet1
```

The following is an example for configuring loopback interfaces as alternative or secondary NAT methods while the default method is a NAT pool or interface overload:

```
interface GigabitEthernet1
 ip address 10.1.1.1
 no ip redirects
 load-interval 30
 negotiation auto
 ip nat outside
 !
 ip nat inside source list dia-list interface Loopback10 overload match-interface
GigabitEthernet1
 ip nat inside source list dia-list interface Loopback11 overload match-interface
GigabitEthernet1
```

The following is an example for configuring NAT pools as alternative or secondary methods while the default method is an interface overload or a NAT pool:

```
interface GigabitEthernet1
 ip address 10.1.1.1
 no ip redirects
 load-interval 30
 negotiation auto
 ip nat outside
 !
 ip nat pool natpool10 10.10.10.10 10.10.10.10 prefix-length 24
 ip nat inside source list dia-list pool natpool1 overload match-interface GigabitEthernet1

 ip nat inside source list dia-list pool natpool2 overload match-interface GigabitEthernet1
```

Configure the Traffic Data Policy

After you have configured the multiple NAT types using a feature template, configure the traffic rules in the centralized data policy to apply match-action conditions. When the NAT DIA traffic matches the conditions in the match portion of a centralized data policy, the packet is accepted.

The following is a sample configuration for configuring the traffic data policy:

```
data-policy data-policy-name
  vpn-list list-name
   sequence sequence-number
    match source-data-prefix-list data-prefix list-name
    !
    action accept
     count vpn-list-name
     nat use-vpn 0
     nat source-dia-pool pool-id
     nat source-dia-interface interface-name
    !
   !
   default-action drop
  !
```

The following is an example for configuring the traffic data policy:

```
data-policy MULTIPLE-NAT-DIA-TRAFFIC
  vpn-list VPN1
   sequence 1
    match source-data-prefix-list NAT-DIA-PREFIX-LIST
    !
    action accept
     count VPN1-TRAFFIC
     nat use-vpn 0
     nat source-dia-pool 1
         !
   !
   default-action drop
  !
```

For more information about configuring the traffic data policy, see Configure Centralized Policies Using the CLI in *Cisco Catalyst SD-WAN Policies Configuration Guide*.

The following is an example configuration corresponding to the above traffic data policy, where the default NAT method is interface overload and the alternative or secondary NAT method is NAT pool:

```
interface GigabitEthernet1
 ip address 10.1.1.1 255.255.255.0
 no ip redirects
```

```
load-interval 30
negotiation auto
ip nat outside
!
ip nat inside source list dia-list pool natpool1 overload match-interface GigabitEthernet1

ip nat inside source list dia-list interface GigabitEthernet1 overload
```

Configure a NAT DIA Route

Every service VPN routes packets into the transport VPN for DIA traffic. Configure a NAT DIA route for the service-side VPN.

Note You configure an IPv4 DIA route in a **Cisco VPN** template, which is a service-side VPN.

Configure a NAT DIA Route Using a Cisco VPN Template

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

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

3. To edit a **Cisco VPN** template, click **. . .** adjacent to the template name and choose **Edit**.
4. Click **IPv4 Route**.
5. Click **New IPv4 Route**.
6. In the **Prefix** field, enter an IPv4 prefix for NAT.
7. In the **Gateway** field, click **VPN**.
8. In the **Enable VPN** drop-down list, change the scope from **Default** to **Global**, and click **On** to enable VPN.
9. Click **Update**.

Configure a NAT DIA Route Using the CLI

The following is a sample configuration for configuring a NAT DIA route.

```
Device(config)# interface GigabitEthernet3
ip address 192.0.2.1 255.255.255.0
ip nat outside
no shut

interface GigabitEthernet2
vrf forwarding 1
ip address 10.0.0.1 255.255.255.0
no shut
```

```
ip nat route vrf 1 0.0.0.0 0.0.0.0 global
ip route 0.0.0.0 0.0.0.0 192.0.2.2
```

Verify NAT DIA Route Configuration

The following is a sample output from the **show ip route** command:

```
Device# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected
```

The following is a sample output from the **show ip route vrf 1** command:

```
Device# show ip route vrf 1

Routing Table: 1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected
```

Advertise NAT Routes Through OMP

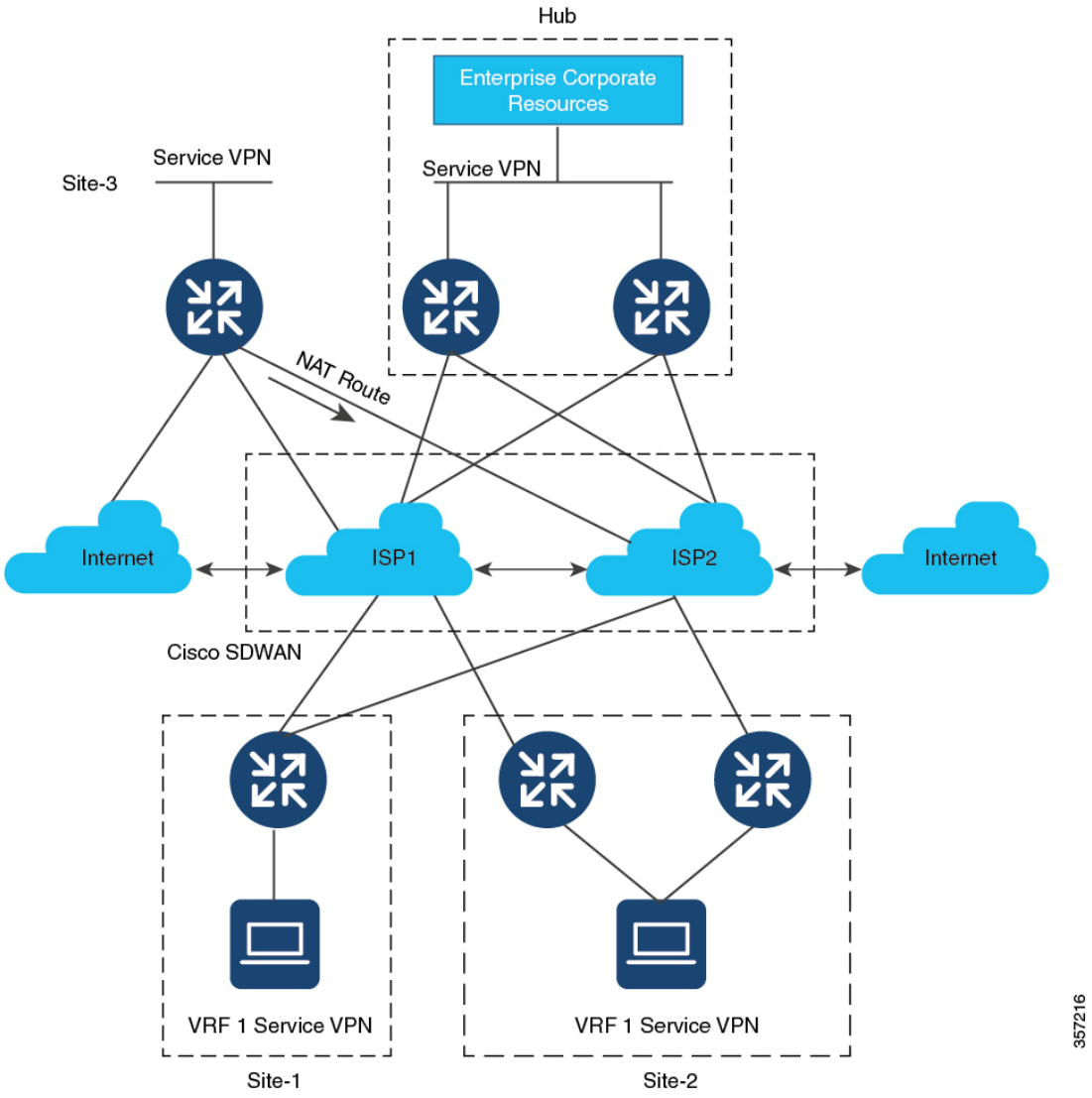
The following sections provide information about advertising NAT routes through OMP.

Information About Advertising NAT Routes Through OMP

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, you can configure NAT DIA default routes to be advertised through OMP. OMP is enabled by default on all Cisco IOS XE Catalyst SD-WAN devices, and so, there is no need to explicitly configure or enable OMP. OMP must be operational for the overlay network to function. If you disable OMP, you disable the overlay network.

When NAT DIA advertisement is configured on any designated Cisco IOS XE Catalyst SD-WAN device on the network, OMP advertises the NAT default route to the branches. The branches receive the default route and use it to reach the hub for all DIA traffic. The Cisco IOS XE Catalyst SD-WAN device acts as the internet gateway for all DIA traffic.

Figure 1: Advertising NAT Routes Using OMP



Enable NAT Route Advertisements Through OMP Using the CLI

To advertise the default route over OMP, use the **sdwan omp** command.

Use the following configuration to advertise NAT routes through OMP.

Note This command has been tested using only the device CLI template.

```
ip nat route vrf 1 0.0.0.0 0.0.0.0 global
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet3 overload
sdwan
 omp
  address-family vrf 1
```

```
   advertise network 0.0.0.0/0
interface GigabitEthernet3
 ip nat outside
```

Note Ensure that NAT routes are advertised only when NAT DIA is configured.

The **advertise network** keyword is mandatory while configuring the advertisement of NAT routes into OMP.

Verify NAT Route Advertisements Through OMP Using the CLI

To display the default route information, use the **show sdwan omp routes** command.

```
Device# show sdwan omp routes

Code:
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
                          PATH                ATTRIBUTE
VPN PREFIX      FROM PEER ID LABEL STATUS    TYPE       TLOC IP  COLOR        ENCAP
PREFERENCE
10 0.0.0.0/0           10.1.1.3 23 1002 C,I,R      installed 10.1.1.10 biz-internet ipsec
        -
                       10.1.1.3 24 1002 R          installed 10.1.1.30 biz-internet ipsec
        -
10 10.2.0.0/16         10.1.1.3 27 1002 C,I,R      installed 10.1.1.10 biz-internet ipsec
        -
                       10.1.1.3 28 1002 R          installed 10.1.1.30 biz-internet ipsec
        -
10 172.254.32.76/30    10.1.1.3 26 1002 C,I,R      installed 10.1.1.30 biz-internet ipsec
        -
10 172.254.51.124/30   10.1.1.3 25 1002 C,I,R      installed 10.1.1.30 biz-internet ipsec
        -
10 172.254.249.164/30  10.1.1.3 22 1002 C,I,R      installed 10.1.1.10 biz-internet ipsec
        -
10 172.254.252.12/30   10.1.1.3 21 1002 C,I,R      installed 10.1.1.10 biz-internet ipsec
        -
10 172.30.1.0/24       0.0.0.0 75 1002 C,Red,R          installed 10.1.1.26 gold
ipsec         -
                       0.0.0.0 76 1002 C,Red,R          installed 10.1.1.26 silver
ipsec         -
                       10.1.1.3 29 1002 Inv,U      installed 10.1.1.36 gold          ipsec
         -
                       10.1.1.3 30 1002 Inv,U      installed 10.1.1.36 silver        ipsec
         -
```

To display the information about a NAT DIA route created on the spoke, use the **show ip route vrf 1** command.

```
Device# show ip route vrf 10

Routing Table: 10
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
D - EIGRP, EX - EIGRP external, 0 - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type
 1, N2 - OSPF NSSA external type 2  E1 - OSPF external type 1, E2 - OSPF external type m -
 OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT IA i - IS-IS, su - IS-IS summary, Ll
- IS-IS level-1, L2 - IS-IS level-2 is - IS-IS inter area, * - candidate default, U -
per-user static route
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, 1 - LISP a - application route
+ - replicated route, % - next hop override, p - overrides from PfR & - replicated local
route overrides by connected

Gateway of last resort is 10.1.1.10 to network 0.0.0.0

m 0.0.0.0/0 [251/0] via 10.1.1.10,2d16h, Sdwan-system-intf
        10.0.0.0/16 is subnetted, 1 subnets
```

Use the **show sdwan omp routes** command to display the default routes on the spoke.

```
Device# show sdwan omp routes vpn 10

Code:
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
                          PATH            ATTRIBUTE
VPN PREFIX      FROM PEER ID LABEL STATUS TYPE    TLOC IP COLOR        ENCAP      PREFERENCE
10 0.0.0.0/0           10.1.1.3 23 1002 C,I,R installed 10.1.1.10 biz-internet ipsec
   -
                       10.1.1.3 24 1002 R     installed 10.1.1.30 biz-internet ipsec
   -
```

NAT DIA IPv4 over an IPv6 Tunnel

The following sections provide information about configuring NAT DIA IPv4 over an IPv6 tunnel.

Information About NAT DIA IPv4 over an IPv6 Tunnel

The NAT DIA IPv4 over an IPv6 tunnel enables IPv6-only devices to access IPv4 websites and services.

The traffic flow is from the service side (LAN) to the transport side (WAN) in the overlay network.

Service-side source IPv4 addresses are translated to public IPv4 addresses on the tunnel interface.

Configure NAT DIA IPv4 over an IPv6 tunnel using a device CLI or a CLI add-on template.

Benefits of NAT DIA IPv4 over an IPv6 Tunnel

- Provides IPv4 access from an IPv6-only device.
- Supports routing of IPv4 traffic over an IPv6 tunnel.
- Supports translation of service-side source IPv4 addresses to public IPv4 addresses on the tunnel interface.

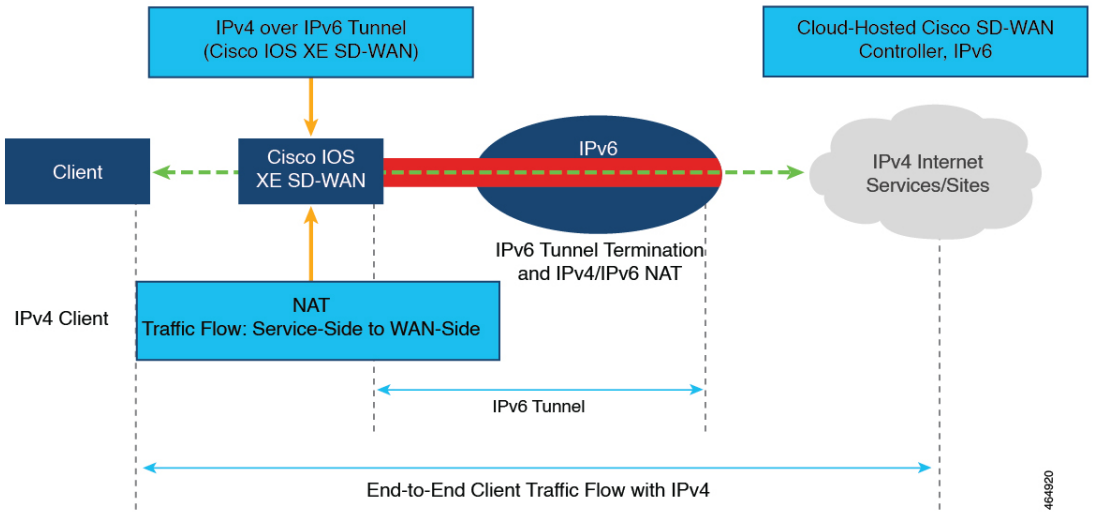
Restrictions for NAT DIA IPv4 over an IPv6 Tunnel

- NAT DIA tracker is not supported.
- Unified Threat Defense (UTD) is not supported.
- Keepalive traffic on a tunnel interface is not supported.

Use Case for NAT DIA IPv4 over an IPv6 Tunnel

A customer has an IPv6-only device, but requires access to IPv4 websites and services. To support this scenario, use an IPv6 tunnel for directing the IPv4 traffic to the internet.

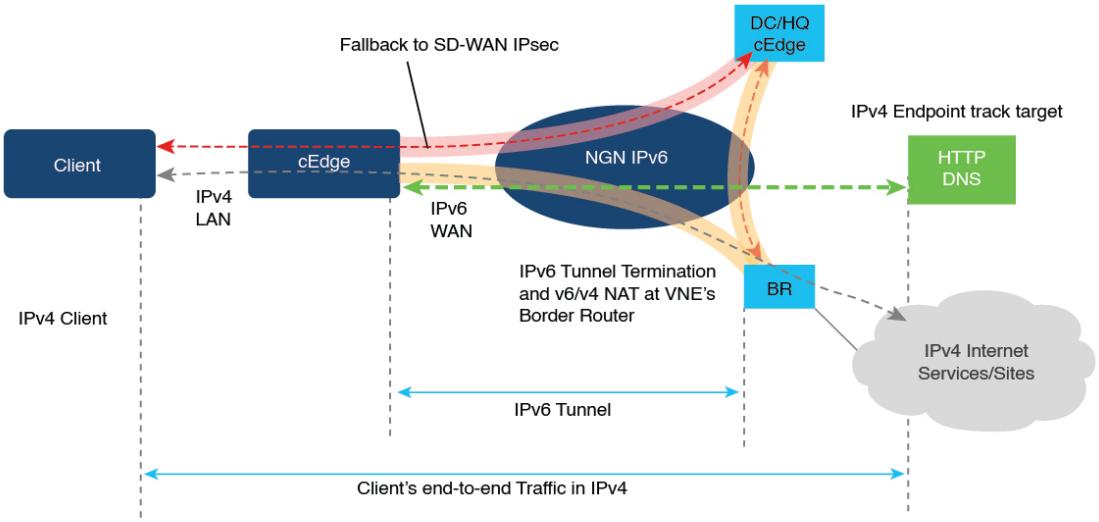
Figure 2: NAT DIA IPv4 over IPv6 Tunnel Support



Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1

The border router acts as a gateway between IPv6 and IPv4 traffic to send IPv4 bound traffic through static IPv6 tunnel. When the border router and the IPv6 tunnel is unreachable, the WAN edge device cannot determine if the IPv6 tunnel is inactive and therefore cannot re-route the traffic.

Associating IPv4 DIA tracker to an IPv6 tunnel and the border router, helps the WAN edge device to determine if the IPv6 tunnel is active based on the tracker status. When IPv4 tracker is inactive, the associated IPv6 tunnel is also inactive and the traffic is re-routed to an alternative path based on the routing table. When the IPv4 tracker is active, the associated IPv6 tunnel is also active and the traffic is resumed back to the IPv6 tunnel.



Workflow for Configuring NAT DIA IPv4 over an IPv6 Tunnel

Cisco SD-WAN Manager Configuration

1. Enable NAT by editing an existing **Cisco VPN Interface Ethernet** template.
   a. Configure interface overload (default).
   b. Configure a NAT pool.
2. Configure a NAT DIA route using a **Cisco VPN** template.

CLI Configuration

1. Configure an IPv4 over an IPv6 tunnel.
2. Configure the **ip nat outside** command on the tunnel interface.
3. Configure a NAT DIA route for routing IPv4 traffic over an IPv6 tunnel.

Configure NAT DIA IPv4 over an IPv6 Tunnel Using the CLI

1. Configure a global default route for the IPv6 tunnel:

```
Device(config)# interface Tunnel1000
Device(config-if)# ip address 10.1.15.15 255.255.255.0
Device(config-if)# ip mtu 1460
Device(config-if)# ip tcp adjust-mss 1420
Device(config-if)# load-interval 30
Device(config-if)# tunnel source GigabitEthernet3
Device(config-if)# tunnel mode ipv6
```

```
Device(config-if)# tunnel destination 2001:DB8:A1:10::10
Device(config-if)# tunnel route-via GigabitEthernet3 mandatory
Device(config-if)# tunnel path-mtu-discovery
!
Device(config)# ip route 0.0.0.0 0.0.0.0 Tunnel1000
```

2. Configure an IPv4 over an IPv6 tunnel using the **ip nat outside** command:

```
Device(config)# interface Tunnel1000
Device(config)# ip nat outside
```

3. Configure an IPv4 over an IPv6 tunnel with a NAT pool and interface overload mode:

```
Device(config)# interface Tunnel1000
Device(config)# ip nat inside source list nat-dia-vpn-hop-access-list interface Tunnel1000
 overload
```

or

```
Device(config)# ip nat pool natpool10 203.0.113.1 203.0.113.25 prefix-length 24
Device(config)# ip nat inside source list nat-dia-vpn-hop-access-list pool natpool10
overload egress-interface Tunnel1000
```

4. Configure a NAT DIA route within a service-side VPN:

```
Device(config)# ip nat route vrf 10 0.0.0.0 0.0.0.0 global
```

Note If you are configuring a NAT DIA route using a centralized data policy, use the **nat use-vpn 0** command.

Configure NAT DIA IPv4 over an IPv6 Tunnel Using CLI (Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and later releases)

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1

Note By default, CLI templates execute commands in global config mode.

You can configure NAT DIA IPv4 over an IPv6 tunnel using IPv4 NAT DIA tracker.

1. Configure the endpoint tracker for tracking the status of an endpoint:

   endpoint-tracker *tracker-name*

2. Configure the IP address of an endpoint:

   endpoint-ip *ip-address*

3. Configure the tracker type for the tracker:

   tracker-type *interface-name*

4. Configure NAT DIA IPv4 over an IPv6 tunnel.

Here is the complete configuration example to configure NAT DIA IPv4 over an IPv6 tunnel using IPv4 DIA tracker:

```
endpoint-tracker test1
 endpoint-ip 10.0.12.13
 tracker-type interface

   interface Tunnel5
   ip address 192.168.9.2 255.255.255.0
   ip nat outside
   endpoint-tracker test1
   tunnel source GigabitEthernet8
   tunnel mode ipv6
    tunnel destination 2A00:B00::1D1E:CA68
    tunnel path-mtu-discovery

    interface GigabitEthernet8
    no ip address
    negotiation auto
    ipv6 address 2A00:B00::1D1E:CA58/64
    no mop enabled
    no mop sysid

 ip nat inside source list nat-dia-vpn-hop-access-list interface Tunnel5 overload
 ip nat route vrf 1 0.0.0.0 0.0.0.0 global
 ip route 0.0.0.0 0.0.0.0 Tunnel5
```

Configure NAT DIA IPv4 over an IPv6 Tunnel Using a CLI Add-On Template

Before You Begin

Create a new CLI add-on template or edit an existing CLI add-on template.

Configure NAT DIA IPv4 over an IPv6 Tunnel Using a CLI Add-On Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Click **Add Template**.
4. Choose a device from the device list.
5. In the **OTHER TEMPLATES** area, click **CLI Add-On Template**.
6. In the **CLI Add-On Template** area, enter the configuration.
7. Configure IPv4 over an IPv6 tunnel as shown in the following example configuration:

```
interface Tunnel1000
 no shutdown
 ip address 203.0.113.1 255.255.255.0
 ip nat outside
 load-interval 30
 tunnel source GigabitEthernet1
 tunnel destination 2001:DB8:A1:10::10
 tunnel mode ipv6
 tunnel path-mtu-discovery
 tunnel route-via GigabitEthernet1 mandatory
!
ip nat inside source list nat-dia-vpn-hop-access-list interface Tunnel1000 overload
ip route 0.0.0.0 0.0.0.0 Tunnel1000 203.0.113.2
ip nat route vrf 10 0.0.0.0 0.0.0.0 global
```

8. Click **Save**.

   The CLI add-on template that you created is displayed in the **CLI Configuration** table.

9. Attach the CLI add-on template to your device.

Verify NAT DIA IPv4 over an IPv6 Tunnel Configuration

Verify NAT DIA Route Entries

The following is a sample output from the **show ip nat route-dia** command:

```
Device# show ip nat route-dia
route add [1] addr [0.0.0.0] vrfid [2] prefix len [0]
route add [1] addr [0.0.0.0] vrfid [4] prefix len [0]
```

In the sample output, two NAT route advertisements are enabled.

Verify NAT DIA Routing Table Entries

The following is a sample output from the **show ip route vrf 1 nat-route** command:

```
Device# show ip route vrf 1 nat-route
Routing Table: 1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

n*Nd  0.0.0.0/0 [6/0], 00:40:17, Null0
```

In this sample output, `n*Nd 0.0.0.0/0` is the configured NAT DIA route.

Display IP Translations

The following is a sample output from the **show ip nat translations** command:

```
Device# show ip nat translations
show ip nat translations
Pro  Inside global        Inside local          Outside local         Outside global
tcp  203.0.113.1:5201     10.20.24.150:5201     10.20.25.150:5201     10.20.25.150:5201
icmp 203.0.113.1:25440    10.20.24.150:25440    10.20.25.150:25440    10.20.25.150:25440
Total number of translations: 2
```

In the sample output, there are two translations.

Verify IP NAT Global Statistics

The following is a sample output from the **show ip nat statistics** command:

```
Device# show ip nat statistics
Total active translations: 2 (0 static, 2 dynamic; 2 extended)
```

```
Outside interfaces:
  Tunnel1000
Inside interfaces:
Hits: 1012528  Misses: 56
Expired translations: 3
Dynamic mappings:
-- Inside Source
[Id: 3] access-list nat-dia-vpn-hop-access-list interface Tunnel1000 refcount 2
nat-limit statistics:
 max entry: max allowed 0, used 0, missed 0
In-to-out drops: 0  Out-to-in drops: 0
Pool stats drop: 0  Mapping stats drop: 0
Port block alloc fail: 0
IP alias add fail: 0
Limit entry add fail: 0
```

In the sample output, there are two translations for tunnel 11000.

The output of the **show ip nat statistics** command displays information about all the IP address pools and NAT mappings that you have configured.

Clear NAT Global Statistics

Use the **clear ip nat statistics** command to clear NAT global statistics:

```
Device# clear ip nat global statistics
```

Display NAT Statistics

The following is a sample output from the **show platform hardware qfp active feature nat datapath stats** command:

```
Device# show platform hardware qfp active feature nat datapath stats
Total active translations: 2 (0 static, 2 dynamic; 2 extended)
Outside interfaces:
  Tunnel1000
Inside interfaces:
Hits: 1012528  Misses: 56
Expired translations: 3
Dynamic mappings:
-- Inside Source
[Id: 3] access-list nat-dia-vpn-hop-access-list interface Tunnel1000 refcount 2
nat-limit statistics:
 max entry: max allowed 0, used 0, missed 0
In-to-out drops: 0  Out-to-in drops: 0
Pool stats drop: 0  Mapping stats drop: 0
Port block alloc fail: 0
IP alias add fail: 0
Limit entry add fail: 0
```

Check NAT Global Counters: Datapath Map

The following is a sample output from the **show platform hardware qfp active feature nat datapath map** command:

```
Device# show platform hardware qfp active feature nat datapath map
I/f Map Table

if_handle 65529 next 0x0 hash_index 220
laddr 0.0.0.0 lport 0 map 0xdec942c0 refcnt 0
gaddr 203.60.10.1 gport 0 proto 0 vrfid 0x0
src_type 1 flags 0x80100 cpmapid 3
I/f Map Table End
```

```
edm maps 0
mapping id 1 pool_id 0 if_handle 0xfff9 match_type 0 source_type 1 domain 0 proto 0 Local
IP 0.0.0.0,
Local Port 0 Global IP 203.60.10.1 Global Port 0 Flags 0x80100 refcount 0 cp_mapping_id 3
next 0x0 hashidx 50 vrfid 0 vrf_tableid 0x0 rg 0 pap_enabled 0 egress_ifh 0x14
```

Check NAT Global Counters: Session Dump

The following is a sample output from the **show platform hardware qfp active feature nat datapath sess-dump** command:

```
Device# show platform hardware qfp active feature nat sess-dump
id 0xdd70c1d0 io 10.20.24.150 oo 10.20.25.150 io 5201 oo 5201 it 203.0.113.1 ot 10.20.25.150
 it 5201 ot 5201 pro 6 vrf 4 tableid 4 bck 65195 in_if 0 out_if 20 ext_flags 0x1 in_pkts
183466 in_bytes 264182128 out_pkts 91731 out_bytes 2987880flowdb in2out fh 0x0 flowdb out2in
 fh 0x0
id 0xdd70c090 io 10.20.24.150 oo 10.20.25.150 io 25965 oo 25965 it 203.0.113.1 ot 10.20.25.150
 it 25965 ot 25965 pro 1 vrf 4 tableid 4 bck 81393 in_if 0 out_if 20 ext_flags 0x1 in_pkts
 27 in_bytes 38610 out_pkts 27 out_bytes 38610flowdb in2out fh 0x0 flowdb out2in fh 0x0
```

Configuration Examples for NAT DIA IPv4 over an IPv6 Tunnel

```
Device# show sdwan running-config | section Tunnel1000|GigabitEthernet1
interface GigabitEthernet1
 ip address 10.1.15.15 255.255.255.0
 no ip redirects
 load-interval 30
 negotiation auto
 ipv6 address 2001:DB8:A1:F::F/64
 ipv6 enable
 ipv6 nd ra suppress all
 service-policy output shape_GigabitEthernet1
!
interface Tunnel1000
 no shutdown
 ip address 203.0.113.1 255.255.255.0
 ip nat outside
 load-interval 30
 tunnel source GigabitEthernet1
 tunnel destination 2001:DB8:a1:10::10
 tunnel mode ipv6
 tunnel path-mtu-discovery
 tunnel route-via GigabitEthernet1 mandatory
!
ip nat inside source list nat-dia-vpn-hop-access-list interface Tunnel1000 overload
ip route 0.0.0.0 0.0.0.0 Tunnel1000 203.0.113.2
ip nat route vrf 10 0.0.0.0 0.0.0.0 global
```

Dialer Interfaces with NAT DIA

The following sections provide information about configuring dialer interfaces with NAT DIA.

Information About Using a Dialer Interface with NAT DIA

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1

This feature provides support for Point-to-Point Protocol (PPP) dialer interfaces for the NAT DIA use case. Use dialer interfaces to access IPv4 internet services and sites.

A dialer interface specifies how to handle traffic from clients, including default routing information, the encapsulation protocol, and the dialer pool to use.

The following dialer interfaces are supported:

- Point-to-Point Protocol over Ethernet (PPPoE)
- Point-to-Point Protocol over Asynchronous Transfer Mode (PPPoA)
- Point-to-Point Protocol over Ethernet over Asynchronous Transfer Mode (PPPoEoA)

Adjust the TCP Maximum Segment Size for NAT DIA



Note Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.9.1a and Cisco vManage Release 20.9.1, you can adjust the TCP maximum segment size (MSS) value for preventing dropped TCP sessions.

Benefits of Using a Dialer Interface with NAT DIA

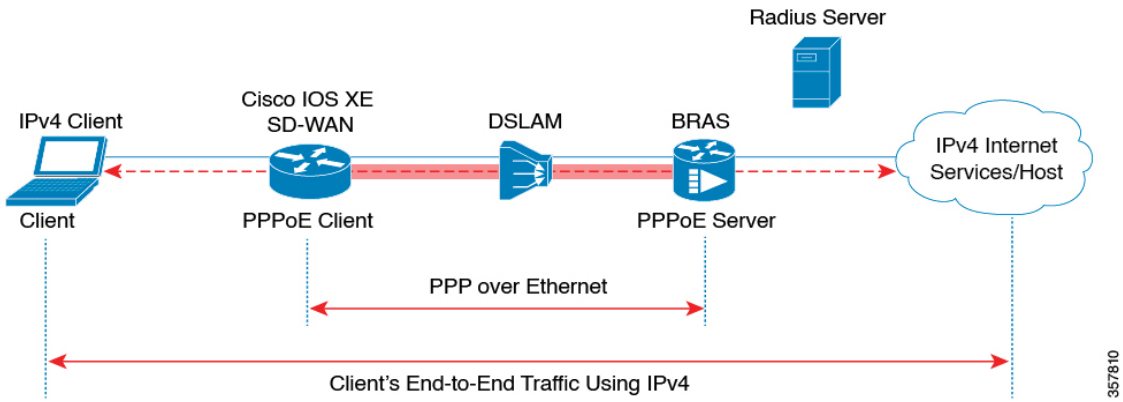
- Supports interface overload mode with NAT DIA
- Supports route-based as well as data-policy-based configuration with NAT DIA
- Provides support for NAT pools and loopback
- Provides support for static NAT configuration
- Provides support for static NAT port forwarding
- Allows physical interfaces to take on different characteristics based on incoming or outgoing call requirements
- Provides static or negotiated IP address support over a dialer interface with NAT DIA

Workflow for a NAT DIA Dialer Interface

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1

The following diagram describes how IPv4 client traffic gets routed over a dialer interface for reaching IPv4 internet sites and services.

Figure 3: Workflow for NAT DIA Dialer Interface Support



Restrictions for Using a Dialer Interface with NAT DIA

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1

- Only NAT DIA is supported with dialer interfaces.
- No support for service-side NAT with dialer interfaces.
- PPPoE jumbo frames are limited to 1800 bytes when using a device CLI or a CLI add-on template.
- There is no support for configuring the following PPPoA dialer interface encapsulations: AAL5MUX, AAL5SNAP, AAL5NLPID, or bridge-dot1q using Cisco SD-WAN Manager feature templates. If you want to configure these PPPoA encapsulations, you need to configure the encapsulations using a CLI template.
- NAT DIA tracker is not supported for a dialer interface with an **ip unnumbered** interface.
- NAT DIA path preference is not supported with loopback on a WAN interface.

Configure a Dialer Interface with NAT DIA Using a CLI Template

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1

1. Configure a PPPoE dialer interface with NAT DIA enabled.

   The **dialer down-with-vInterface** command, available from Cisco IOS XE Catalyst SD-WAN Release 17.9.1a and Cisco vManage Release 20.9.1, brings down the dialer interface when the PPP session goes down.

```
interface interface-type-number
 pppoe enable group global
 pppoe-client dial-pool-number dialer-pool-number
!
interface Dialer dialer-number
 description interface vers le BAS
 mtu bytes
 ip address negotiated
 ip mtu bytes
 ip nat outside
 encapsulation encapsulation-type
```

```
ip tcp adjust-mss bytes
dialer pool dialer-pool-number
dialer down-with-vInterface
ppp chap hostname hostname
ppp chap password password
ppp authentication chap callin
ppp ipcp route default
service-policy output shape_Dialer dialer-number
```

2. Enable **ip nat outside** over a dialer interface with interface overload mode.

```
interface Dialer dialer-number
ip nat outside
ip nat inside source list nat-dia-vpn-hop-access-list interface Dialer dialer-number
overload
```

3. Configure a NAT DIA route for a service-side VPN.

   or

   Configure a NAT DIA route for a service-side VPN using a centralized data policy.

```
ip nat route vrf vrf-id route-prefix prefix-mask global
```

Note When dialer interface is deleted in the same transaction as NAT Mapping with Pool-overload-config, an extra no NAT configuration is generated. Remove each NAT configurations separately using different transactions as shown:

```
Device(config)# no ip nat inside source list global-list pool natpool-Dialer100-0 overload
 egress-interface Dialer100
Device(config)# commit

Device(config)# no interface Dialer100
Device(config)# commit
```

Here is the complete configuration example for configuring a dialer interface with NAT DIA.

```
interface Dialer100
 mtu 1492
 ip address negotiated
 ip nat outside
 encapsulation ppp
 ip tcp adjust-mss 1452
 dialer pool 100
 dialer down-with-vInterface
 endpoint-tracker tracker-google
 ppp authentication chap callin
 ppp chap hostname branch1.ppp1
 ppp chap password 7 01100F175804
 ppp ipcp route default
 service-policy output shape_GigabitEthernet0/0/1
!
interface GigabitEthernet0/0/1
 no ip redirects
 pppoe enable group global
 pppoe-client dial-pool-number 100
!
sdwan
 interface Dialer100
  tunnel-interface
   encapsulation ipsec weight 1
```

```
   color mpls restrict
  exit
 exit
ip nat inside source list nat-dia-vpn-hop-access-list interface Dialer100 overload
ip nat route vrf 10 0.0.0.0 0.0.0.0 global
```

Verify a Dialer Interface Configuration

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1

The following sections provide information on verifying a dialer interface configuration.

Verify NAT DIA IP Route Configuration

The following is a sample output from the **show ip route vrf** command:

```
Device# show ip route vrf 10
Routing Table: 1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
& - replicated local route overrides by connected

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

n*Nd 0.0.0.0/0 [6/0], 4d01h, Null0
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
```

In the sample output, `n*Nd 0.0.0.0/0` is the configured NAT DIA route.

Verify Translation of IP Addresses

The following is a sample output from the **show ip nat translations** command:

```
Device# show ip nat translations
Pro   Inside global       Inside local        Outside local    Outside global
tcp   192.0.2.1:80        10.10.0.100:8080    ---               ---
---   192.0.2.2.198       10.10.0.254         ---               ---
tcp   192.0.2.1:8000      10.10.0.253:23      ---               ---
tcp   192.0.2.25:25185    10.0.0.1:43878      203.0.113.1:80    203.0.113.1:80
tcp   192.0.2.3:48871     10.0.0.2:48871      203.0.113.2:80    203.0.113.2:80
tcp   192.0.2.3:63242     10.0.0.2:63242      203.0.113.2:80    203.0.113.2:80
tcp   192.0.2.3:52929     10.0.0.2:52929      203.0.113.2:80    203.0.113.2:80
tcp   192.0.2.4:25184     10.0.0.4:28456      203.0.113.1:80    203.0.113.1:80
udp   192.0.2.3:64681     10.0.0.2:64681      203.0.113.1:53    203.0.113.1:53
udp   192.0.2.3:65504     10.0.0.2:64670      203.0.113.1:53    203.0.113.1:53
tcp   192.0.2.25:25186    10.0.0.1:28455      203.0.113.1:80    203.0.113.1:80
Total number of translations: 11
```

In the sample output, there are 11 translations.

Display Your PPPoE Sessions

The following is a sample output from the **show pppoe session** command:

```
Device# show pppoe session
     1 client session

Uniq ID  PPPoE  RemMAC          Port                    VT  VA         State
           SID  LocMAC                                      VA-st      Type
    N/A    391  84b2.61cc.9903  Gi0/0/1.100           Di100 Vi2        UP
                c884.a1f4.b981  VLAN: 100                   UP
```

In this sample output, the PPPoE dialer interface displays as `UP`.

The following is a sample output from the **show ppp all** command:

```
Device# show ppp all
Interface/ID OPEN+ Nego* Fail-     Stage    Peer Address    Peer Name
------------ -------------------- -------- --------------- --------------------
Vi2          LCP+ IPCP+ CDPCP-     LocalT   172.16.100.1    SDWAN-AGGREGE
```

Verify PPP Negotiation Information

The following is a sample output from the **show interfaces Dialer** command:

```
Device# show interfaces Dialer100
Dialer100 is up, line protocol is up
  Hardware is Unknown
  Internet address is 172.16.100.101/32
  MTU 1492 bytes, BW 56 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 255/255, rxload 255/255
  Encapsulation PPP, LCP Closed, loopback not set
  Keepalive set (10 sec)
  DTR is pulsed for 1 seconds on reset
  Interface is bound to Vi2
  Last input 00:09:05, output 00:00:09, output hang never
  Last clearing of "show interface" counters 1w0d
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/16 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 56 kilobits/sec
  5 minute input rate 42220429000 bits/sec, 23 packets/sec
  5 minute output rate 1520154000 bits/sec, 23 packets/sec
     755339342 packets input, 2706571669546067 bytes
     696497150 packets output, 97523835049377 bytes
Bound to:
Virtual-Access2 is up, line protocol is up
  Hardware is Virtual Access interface
  Internet address will be negotiated using IPCP
  MTU 1492 bytes, BW 56 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 177/255, rxload 177/255
  Encapsulation PPP, LCP Open
  Stopped: CDPCP
  Open: IPCP
```

In this sample output, `Dialer100` is up and the line protocol is up. `Virtual-Access2` is also up and the line protocol is up.

Configuration Example for Using a Dialer Interface with NAT DIA

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1

This example shows the configuration of a dialer interface with a NAT pool, inside static NAT, and port forwarding.

```
ip nat pool natpool10 203.0.113.1 203.0.113.25 prefix-length 24
ip nat inside source list nat-dia-vpn-hop-access-list interface Dialer100 overload
ip nat inside source list nat-dia-vpn-hop-access-list pool natpool10 overload
egress-interface Dialer100
ip nat inside source static 10.10.80.254 10.1.1.198 vrf 10 egress-interface Dialer100
ip nat inside source static tcp 10.10.80.100 8080 interface Dialer100 8080 vrf 10
ip nat inside source static tcp 10.10.80.253 23 10.1.1.200 8201 vrf 10 egress-interface
Dialer100
```

NAT DIA Static NAT Mapping with HSRP

The following sections provide information about configuring NAT DIA static NAT mapping with HSRP.

Information About Static NAT Mapping with HSRP

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1

HSRP is a first-hop redundancy protocol (FHRP) designed to allow transparent failover of the first-hop IP device. HSRP provides high availability by providing first-hop routing redundancy for IP hosts on networks configured with a default gateway IP address. HSRP is used for identifying an active and standby device in a group of routers.

Address Resolution with ARP

Address Resolution Protocol (ARP) finds the hardware address, also known as a Media Access Control (MAC) address, of a host from its known IP address. ARP maintains a cache table in which MAC addresses are mapped to IP addresses.

Gratuitous ARP

When a host sends an ARP request to resolve its own IP address, it is called gratuitous ARP. In the ARP request packet, the source and destination IP addresses are filled with the same source IP address itself. The destination MAC address is the Ethernet broadcast address.

When a router becomes active, it broadcasts a gratuitous ARP packet with the HSRP virtual MAC address to the affected LAN segment. If the segment uses an Ethernet switch, this allows the switch to change the location of the virtual MAC address so that packets flow to the active router instead of the one that is no longer active. End devices do not need gratuitous ARP if routers use the default HSRP MAC address.

Static NAT Mapping with HSRP

1. When an ARP query is triggered for an address that is configured with NAT static mapping and owned by the device, NAT responds with the virtual MAC address configured for this HSRP group. Two devices act as the HSRP active and standby. Configure the NAT inside interfaces of the active and standby devices to belong to an HSRP group.
2. When both the active and standby routers are configured with the same static NAT mapping, only the active device responds to the ARP request for a static NAT mapping entry. Traffic that fails over from the HSRP active device to the standby device does not have to wait for the ARP request to time out before failing over.

3. The new HSRP active device automatically resumes the ownership of the static NAT mapping entry without waiting for the ARP request to time out. The HSRP active device also sends out a gratuitous ARP request for the static NAT mapping entry. This is done by leveraging the HSRP group name that is mapped to the **ip nat outside source static** command.

Benefits of Static NAT Mapping with HSRP

- Ensures redundancy because traffic does not have to wait for the ARP entry to time out before getting failed over
- Only the HSRP active router responds to an incoming ARP request for a router configured with a NAT address

Restrictions for Static NAT Mapping with HSRP

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1

- NAT64 and NAT66 are not supported with static NAT mapping with HSRP.
- IPv6 addresses are not supported. Only IPv4 addresses are supported.
- Service-side object tracker is not supported with outside static NAT.
- Both HSRP routers (active and standby) should have the same group name and the same static NAT mapping.
- HSRP on the WAN interface is not supported.

Configure Static NAT Mapping with HSRP Using a CLI Template

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1

1. Configure an active and a standby HSRP router with an HSRP group name and **ip nat outside** with the **redundancy** keyword for high availability.

```
interface interface-type-number
 no shutdown
 vrf forwarding vrf-name
 ip address ip-address ip-address
 standby version number
 standby group-number ip ip-address
 standby group-number name hsrp_lan
 standby group-number preempt
 standby group-number priority priority-value
 standby group-number timers msec timer-value timer-value
 negotiation auto
exit
!
ip nat inside source list global interface interface-type-number overload
ip nat outside source static ip-address ip-address vrf vrf-name redundancy hsrp_lan
match-in-vrf
```

Note The `redundancy` keyword is not supported for the `ip nat outside source static` and `ip nat inside source static` commands. However, the mapping command has several other combinations which are supported when HSRP redundancy is enabled. So, the redundancy keyword is not disabled in the command entirely.

Configure both the HSRP active router and the standby router with the same HSRP group name and the same static NAT mapping.

Configure the **ip nat inside** command for translating the source IP in addition to configuring the **ip nat outside** command for destination NAT.

When you send a packet from the service side to the internet, NAT DIA translates the destination IP address, which can also be a private IP address, to a public IP address. This is known as destination NAT.

2. Configure a centralized data policy to support **ip nat outside** functionality. The traffic bound for destination NAT may not fall under the policy sequence.

```
policy
data-policy policy-name
vpn-list vpn_list
sequence number
match
source-ip ip-address
!
action accept
nat use-vpn 0
!
!
sequence number
match
source-ip      ip-address
destination-ip ip-address
!
action accept
nat pool pool-number
!
!
default-action accept
!
!
lists
vpn-list vpn_list
vpn vpn-name
vpn vpn-name
!
!
```

The `nat use-vpn 0` portion of the centralized policy ensures that matching traffic is sent to VPN 0 after the destination IP is translated.

Here is a complete configuration example for configuring static NAT mapping with HSRP.

```
!
interface GigabitEthernet1
ip address 209.165.201.96 255.255.255.0
ip nat outside
standby version 2
standby 300 ip 209.165.201.34
```

```
standby 300 priority 120
standby 300 preempt
standby 300 name hsrp_lan
!
interface GigabitEthernet3
vrf forwarding 2
ip address 192.168.0.96 255.255.255.0
standby version 2
standby 500 ip 192.168.0.94
standby 500 priority 120
standby 500 preempt
standby 500 name hsrp_lan
!
!
ip nat inside source list global interface GigabitEthernet1 overload
!
ip nat outside source static 209.165.201.1 192.168.0.1 vrf 2 redundancy hsrp_lan match-in-vrf
!
```

Here is a complete configuration example for configuring static NAT mapping with HSRP using a centralized data policy.

```
policy
data-policy test_policy
vpn-list vpn_list
sequence 10
match
source-ip 192.168.0.0/24
!
action accept
nat use-vpn 0
!
!
sequence 20
match
source-ip      192.168.0.0/24
destination-ip 209.195.201.0/32
!
action accept
nat pool 1
!
!
default-action accept
!
!
lists
vpn-list vpn_list
vpn 0
vpn 2
!
!
```

Verify Static NAT Mapping with HSRP

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1

The following sections provide information on verifying static NAT configuration with HSRP.

Display the IP Address Associated with the HSRP Group Name

The following is a sample output from the **show ip nat redundancy** command:

```
Device# show ip nat redundancy
IP             Redundancy-Name    ID     Use-count
192.168.0.200  hsrp_lan           0      1
```

The output above shows the IP address associated with the HSRP group name.

The number in the `Use-count` column indicates the number of static NAT CLIs that use this IP address.

A new command, **show ip nat redundancy**, is added for displaying the IP address associated with the HSRP group name. For more information, see the *Cisco IOS XE Catalyst SD-WAN Qualified Command Reference Guide*.

Display the Translated IP Addresses

The following is a sample output from the **show ip nat translations** command:

```
Device# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
---  ---                   ---                   192.168.0.200         209.165.201.1

icmp 192.168.0.1:174       192.168.0.1:174       192.168.0.200:174     209.165.201.1:174
icmp 192.0.2.1:174         192.168.0.1:174       209.165.201.1:174     209.165.201.1:174
icmp 192.168.0.1:174       192.168.0.1:174       192.168.0.200:174     209.165.201.1:174
Total number of translations: 4
```

The output above shows that there are four translations.

Display Information for the HSRP Standby Router

The following is a sample output from the **show standby** command displaying information for the standby router:

```
Device# show standby
GigabitEthernet1 - Group 300 (version 2)
  State is Active
    1 state change, last state change 22:33:42
  Virtual IP address is 209.165.201.1
  Active virtual MAC address is 0000.0c9f.f12c (MAC In Use)
    Local virtual MAC address is 0000.0c9f.f12c (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.584 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 120 (configured 120)
  Group name is "hsrp_wan" (cfgd)
  FLAGS: 1/1
GigabitEthernet3 - Group 500 (version 2)
  State is Active
    5 state changes, last state change 00:00:18
  Virtual IP address is 192.168.0.94
  Active virtual MAC address is 0000.0c9f.f1f4 (MAC In Use)
    Local virtual MAC address is 0000.0c9f.f1f4 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.544 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 120 (configured 120)
```

```
Group name is "hsrp_lan" (cfgd)
FLAGS: 1/1
```

Display the NAT IP Addresses in the ARP Table with Virtual MAC Addresses

The following is a sample output from the **show arp vrf** command:

```
Device# show arp vrf 2
Protocol  Address          Age (min)  Hardware Addr    Type   Interface
Internet  192.168.0.1            -   0000.0c9f.f1f4   ARPA   GigabitEthernet3
Internet  192.168.0.10          11  0050.56bc.780b    ARPA   GigabitEthernet3
Internet  192.168.0.11         100   0050.56bc.608e   ARPA   GigabitEthernet3
Internet  192.168.0.14          83   0050.56bc.4748   ARPA   GigabitEthernet3
Internet  192.168.0.94           -   0000.0c9f.f1f4   ARPA   GigabitEthernet3
Internet  192.168.0.96           -   0050.56bc.1378   ARPA   GigabitEthernet3
Internet  192.168.0.98          73   0050.56bc.3967   ARPA   GigabitEthernet3
```

The above output shows that the NAT address 192.168.0.1 is added to the ARP table with the virtual MAC address 0000.0c9f.f1f4.

Application-Level Gateways with NAT DIA

The following sections provide information about configuring application-level gateways (ALGs) with NAT DIA.

Information About Using ALGs with NAT DIA

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1

An application-level gateway (ALG), also known as an application-layer gateway, is an application that translates the IP address inside the payload of an application packet. You use an ALG to interpret the application-layer protocol and perform firewall and NAT translations.

Specific protocols that embed the IP address information within the packet payload require the support of an ALG. The following protocols require an ALG for NAT translations of the application payload:

- Domain Network System (DNS)
- File Transfer Protocol (FTP)
- Session Initiation Protocol (SIP)

  SIP adds the ability to deploy NAT on VoIP solutions based on SIP.

Starting with Cisco vManage Release 20.11.1 and Cisco IOS XE Catalyst SD-WAN Release 17.11.1a, following protocols are supported:

- Trivial File Transfer Protocol (TFTP)
- Point-to-Point Tunneling Protocol (PPTP)
- Sun Remote Procedure Call (SUNRPC)
- Skinny Client Control Protocol (SCCP)
- H.323

Note If a zone-based firewall (ZBFW) is enabled for NAT DIA, the NAT ALG feature interoperates with the ZBFW.

For more information on ALGs, see the *IP Addressing: NAT Configuration Guide*.

Benefits of Using ALGs with NAT DIA

- Allows client applications to use dynamic TCP or UDP ports to communicate with the server application.
- Supports interoperability between NAT ALGs configured with NAT DIA and a zone-based firewall (ZBFW).

Restrictions for Using ALGs with NAT DIA

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1

- No support for ALGs with service-side NAT. Only NAT DIA is supported.

  Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, includes support for ALGs with service-side NAT.
- No support for configuring an ALG using the **ip nat outside source** command.
- A Domain Name System (DNS) ALG requires a static entry in a NAT translation table to modify the payload. If there is no static entry in the NAT translation table, DNS ALG does not work.

  Use the following command to create a static entry in a NAT translation table:

  ```
  ip nat inside source static local-ip global-ip vrf vrf-id egress-interface
  interface-type-number
  ```
- If you run the **clear ip nat translations** command, the ALG session is cleared. To recreate translations by NAT, run new NAT commands. This is the expected behavior.

Configure ALGs with NAT DIA Using a CLI Template

1. Configure NAT DIA.
2. Enable NAT ALG global support.

   ```
   ip nat service all-algs
   ```
3. Enable NAT ALG per application protocol as shown in the following example:

   ```
   ip nat service dns tcp
   ip nat service dns udp
   ip nat service ftp
   ip nat service sip tcp port port-number
   ip nat service sip udp port port-number
   ```

Note Starting from Cisco vManage Release 20.11.1 and Cisco IOS XE Catalyst SD-WAN Release 17.11.1a, the following protocols are supported on NAT ALG.

- TFTP
- PPTP
- SUNRPC
- SCCP
- H.323

Here is a complete configuration example for configuring ALGs.

```
ip nat service all-algs
ip nat service sip tcp port 5060
ip nat service sip udp port 5060
ip nat service dns tcp
ip nat service dns udp
ip nat service ftp
ip nat service H323
ip nat service ras
ip nat service pptp
ip nat service tftp
ip nat service sunrpc tcp
ip nat service sunrpc udp
ip nat service skinny tcp port xxxx(default 2000)
```

Verify ALG Configuration

The following sections provide information on verifying NAT ALG configurations.

Display ALG Translations

```
show ip nat translations tcp
tcp  10.1.15.15:5062       10.20.24.150:57497    10.1.15.150:21        10.1.15.150:21
tcp  10.1.15.15:5063       10.20.24.150:49732    10.1.15.150:20        10.1.15.150:20
```

Note You cannot view the translation of the payload using a CLI template. To view the translation of a payload, capture a packet using Cisco SD-WAN Manager.

For more information on capturing packets using Cisco SD-WAN Manager, see Capture Packets in the *Cisco Catalyst SD-WAN Monitor and Maintain Guide*.

Verify the NAT Timeouts and Protocol Listening by NAT ALG

```
Device(config)# show platform hardware qfp active feature nat datapath summary
Nat setting mode: sdwan-default
Number of pools configured: none
Timeouts: 86400(tcp), 300(udp), 60(icmp), 300(dns),
          60(syn), 300(finrst), 86400(pptp), 3600(rmap-entry)
```

```
pool watermark: not configured
Nat active mapping inside:1 outside:0 static:0 static network:0
Nat debug: none
Nat synchronization: enabled
Nat bpa: not configured; pap: not configured
Nat gatekeeper: on
Nat limit configured: no
Vpns configured with match-in-vrf: no
Nat packet drop: true
Total active translations: 615 (0 static, 615 dynamic, 615 extended)
Platform specific maximum translations: 131072 configured: none
PAM table non-zero entries:
 0 0xeaa88be0 port=53, proto=6, appl_type=12
 12 0xeaa88c60 port=2000, proto=6, appl_type=8
 25 0xeaa88ba0 port=21, proto=6, appl_type=11
 34 0xeaa88c20 port=5060, proto=6, appl_type=9
 35 0xeaa889e0 port=496, proto=17, appl_type=16
 85 0xeaa88ce0 port=5060, proto=17, appl_type=9
 119 0xeaa88ca0 port=53, proto=17, appl_type=12
```

Port Forwarding with NAT DIA

The following sections provide information about configuring port forwarding with NAT DIA.

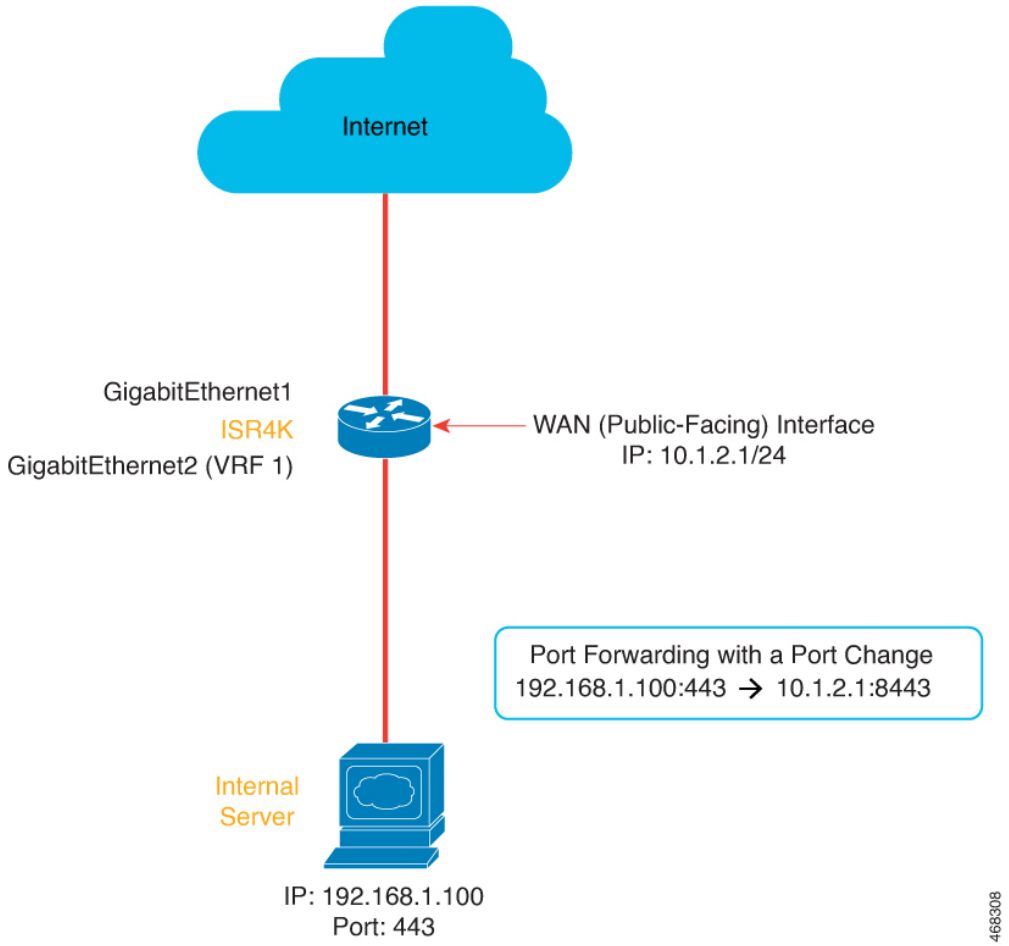
Information About Port Forwarding with NAT DIA

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1

Port forwarding with NAT DIA provides users who run servers within a private network the ability to share a public IP address and a port number that maps to an inside local IP address and port number. This feature can forward different ports to different internal IP addresses, allowing multiple servers to be accessible from the same public IP address.

Prior to Cisco IOS XE Catalyst SD-WAN Release 17.9.1a and Cisco vManage Release 20.9.1, port forwarding was available only for service-side NAT.

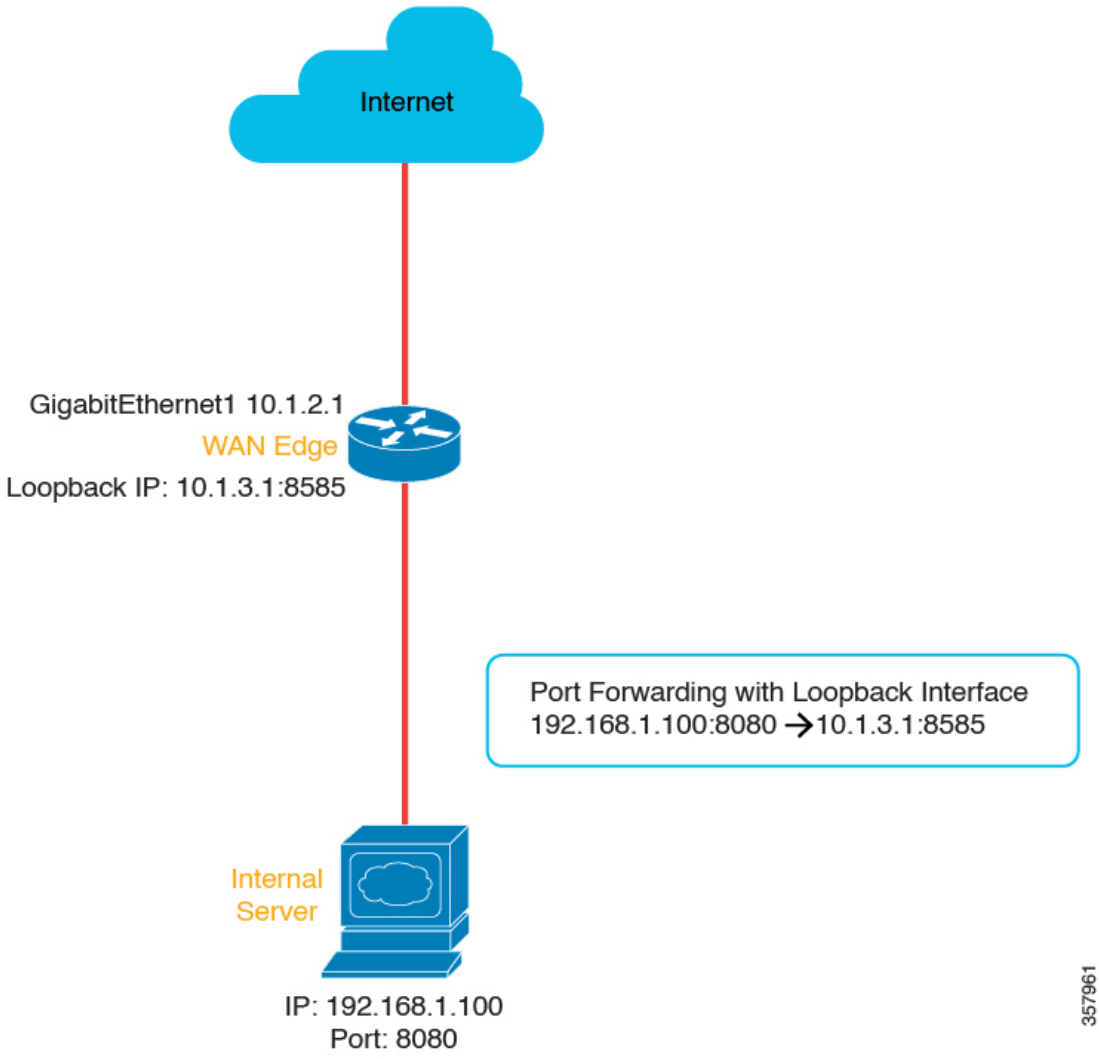
Figure 4: NAT DIA Port Forwarding with a Port Change



From Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and later releases, you can configure loopback interfaces for port forwarding with NAT DIA. Loopback interfaces ensure that the IP address assigned to the interface is always reachable if the IP routing protocols continue to advertise the subnet that is assigned to the loopback interface. After the loopback interface and the port number are configured, the source IP address and the source port number are translated to the loopback IP address and port number respectively.

From Cisco IOS XE Catalyst SD-WAN Release 17.11.1a, you can configure loopback interfaces by either using device CLI templates or CLI add-on feature templates.

Figure 5: NAT DIA Port Forwarding by Using a Loopback interface



Benefits of Port Forwarding with NAT DIA

- Allows you to reach servers in a private network (LAN) from the public domain
- Allows you to forward different ports to different internal IP addresses, allowing multiple servers to be accessible from the same public IP address

Restrictions for Port Forwarding with NAT DIA

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1

- TCP load balancing isn't supported for port forwarding with NAT DIA.
- Traffic can reach public IP addresses and ports from the public network only.

- If you have configured static NAT, you can't use the same static NAT IP addresses when configuring port forwarding.
- You can't use Cisco SD-WAN Manager-reserved ports when configuring port forwarding with NAT DIA.
- No support for loopback interfaces in Cisco IOS XE Catalyst SD-WAN Release 17.10.1a or earlier releases.

  In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a, you can configure loopback interfaces for port forwarding with NAT DIA. For more information about configuring the loopback interface, see *Configure Port Forwarding with NAT DIA Using a CLI Template*
- No support for dialer virtual interfaces.
- UDP ports 8000-48199 are reserved for VoIP traffic. If VoIP is enabled on a Cisco IOS XE Catalyst SD-WAN device, NAT DIA can't use the same UDP ports that are reserved for VoIP traffic.
- NAT DIA port forwarding for a TLOC egress interface doesn't support fragmented packets sourced from outside the network.
- Define up to 128 port-forwarding rules to allow requests from an external network to reach devices on the internal network.
- An IP address plus a port number to an IP address plus a port number translation is supported using Cisco SD-WAN Manager feature templates and CLI templates.
- Interface port forwarding is supported using a CLI template only.

  When you use an interface rather than an IP address in your port-forwarding rule, this is known as interface port forwarding.

Configure Port Forwarding with NAT DIA

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1

Create port-forwarding rules to allow access to a private network from the public domain.

Before You Begin

1. Configure and apply a data policy.
2. Configure a **Cisco VPN Interface Ethernet** template or edit an existing **Cisco VPN Interface Ethernet** template.
3. Configure interface overload mode. Interface overload mode is enabled by default.
4. Configure a NAT pool.

Configure Port Forwarding with NAT DIA

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

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

3. To edit a **Cisco VPN Interface Ethernet** template, click **…** adjacent to the template name and choose **Edit**.
4. Click **NAT**.
5. Under **NAT Pool**, click **New NAT Pool**.
6. Enter the required NAT pool parameters.
7. Click **Add**.
8. To create a port-forwarding rule, click **Port Forward** > **New Port Forwarding Rule** and configure the parameters as described in the table.

Table 5: Port-Forwarding Parameters for NAT DIA

Parameter Name	Description
Protocol	Choose the **TCP** or **UDP** protocol to which to apply the port-forwarding rule. To match the same ports for both TCP and UDP traffic, configure two rules.
Source IP Address	Enter the source IP address to be translated.
Source Port	Enter a port number to define the source port to be translated. Range is 0 to 65535.
Translated Source IP Address	Specify the NAT IP address that will be advertised into OMP. Port forwarding is applied to traffic that is destined to this IP address from the overlay with the translated port match.
Translate Port	Enter the port number to apply port forwarding to. Range is 0 to 65535. Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, static translated source IP addresses must be within the configured dynamic NAT pool IP address range.
Static NAT Direction	Select the direction in which to perform network address translation.
Source VPN ID	Specify the service-side VPN from which the traffic is being sent.

9. Click **Update**.

Note If you are using Cisco Catalyst SD-WAN Manager Release 20.12.x and Cisco IOS XE Catalyst SD-WAN Release 17.9.x, SD-WAN Manager cannot push NAT port forwarding configurations due to a YANG model incompatibility. To resolve this, either switch the router to CLI mode to configure port forwarding manually or upgrade the router to Cisco IOS XE Catalyst SD-WAN Release 17.12.x.

Configure Port Forwarding with NAT DIA Using a CLI Template

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1

For more information on using CLI templates, see CLI Templates and CLI Add-On Feature Templates.

1. Configure **ip nat outside** on the WAN interface.

```
interface interface-type-number
 ip address dhcp
 ip nat outside
 negotiation auto
 no mop enabled
 no mop sysid
end
```

2. Configure interface overload mode on the WAN interface.

```
ip nat inside source list nat-acl interface interface-type-number overload
```

3. Configure NAT DIA port forwarding using an egress interface.

```
ip nat inside source static tcp ip-address port ip-address port vrf number
egress-interface interface-type-number
ip nat inside source static tcp ip-address port interface interface-type-number port vrf
 number
```

The `ip nat inside source static tcp ip-address port interface interface-type-number port vrf number` command is an example of interface port forwarding, because you use an interface rather than an IP address in the port-forwarding rule.

Note You can configure interface port forwarding using a Cisco SD-WAN Manager feature template.

Here is a complete configuration example for configuring port forwarding with NAT DIA.

```
interface GigabitEthernet1
 ip address 10.1.2.1 255.255.255.0
 ip nat outside
 negotiation auto
 no mop enabled
 no mop sysid
end

ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet1 overload
ip nat inside source static tcp 192.168.1.100 443 interface GigabitEthernet1 8443 vrf 1
ip nat inside source static tcp 192.168.1.100 80 10.1.2.10 80 vrf 1 egress-interface
GigabitEthernet1
```

```
ip nat inside source static tcp 192.168.1.100 22 10.1.2.20 2020 vrf 1 egress-interface
GigabitEthernet1
```

Port forwarding with NAT DIA using a loopback interface

From Cisco IOS XE Catalyst SD-WAN Release 17.11.1a, you can configure loopback interfaces for port forwarding with NAT DIA. While configuring a loopback interface, provide the egress interface, which is the internet-facing interface.

Here is a configuration example for configuring port forwarding with NAT DIA by using a loopback interface.

Configure **ip nat outside** on the WAN interface:

```
interface GigabitEthernet1
 ip address 10.1.2.1 255.255.255.0
 ip nat outside
 negotiation auto
 no mop enabled
 no mop sysid
exit
```

Define the loopback interface:

```
interface Loopback3
 ip address 10.1.3.1 255.255.255.255
exit
```

Configure the loopback interface:

```
ip nat inside source static tcp 192.168.1.100 8080 interface Loopback3 8585 vrf 1
egress-interface GigabitEthernet1
ip nat inside source static tcp 192.168.1.100 80 interface Loopback3 5050 egress-interface
 GigabitEthernet1
```

In the preceding configuration example, the incoming TCP packet with the source IP address of 192.168.1.100 is translated to the IP address assigned to Loopback3, which is 10.1.3.1. The source port 8080 is translated to 8585.

If you specify a VRF number in the range of 1–512, port forwarding occurs within the service VPN. When you don't specify a value for the VRF number, port forwarding is configured on the transport VPN, which is VPN 0, by default.

The loopback interface remains active till you run the **shutdown** command in the interface configuration mode.

Verify Configuration of Port Forwarding with NAT DIA

Verify Translations for Port Forwarding with NAT DIA

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1

The following is a sample output from the **show ip nat translations** command:

```
Device# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
tcp  10.0.1.7:2022         10.0.100.14:22        ---                   ---
tcp  10.0.1.7:2022         10.0.100.14:22        10.0.1.16:46275       10.0.1.16:46275
Total number of translations: 2
```

In the output above, inside global IP 10.0.1.7 with port 2022 is translated to an inside local IP of 10.0.100.14 with port 22.

Verify Translations for Port forwarding using a loopback interface

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.11.1a, Cisco vManage Release 20.11.1

The following is a sample output from the **show ip nat translations** command:

```
Device# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
tcp  10.1.3.1:5050         192.168.1.100:80        ---                   ---
tcp  10.1.3.1:8585         192.168.1.100:8080      ---                   ---
Total number of translations: 2
```

In the output above, the source IP 192.168.1.100 with port 8080 is translated to the loopback IP 10.1.3.1 with port 8585.

NAT High-Speed Logging

The following sections provide information on configuring Network Address Translator (NAT) High-Speed Logging (HSL) with NAT Direct Internet Access (DIA).

Information About NAT HSL

Minimum supported releases:
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a
Cisco IOS XE Release 17.6.4 and later 17.6.x releases

NAT HSL lets you enable or disable NAT high-speed logging for virtual routing and forwarding (VRF) instances. When HSL is configured, NAT provides a log of the packets flowing through the routing devices (similar to the Version 9 NetFlow-like records) to an external collector. NAT translations exported to an external collector can include service-side VRF to global DIA and intra-service VRF (service-side VRF NAT) translations. When sessions are created and deleted, records are generated for each binding (binding is the address binding the local address and the global address to which the local address is translated).

You can turn on the collector for viewing the HSL information for NAT. You can turn on HSL only when required, and HSL log records are created and sent to the collector accordingly. This saves CPU cycles and bandwidth by not creating and sending HSL logging records when not needed.

Benefits of NAT HSL

- Supports the sending of flow monitor records for NAT operations to an external collector.
- Enables creation and sending of HSL records only when required, which saves CPU cycles and bandwidth.
- Sends an HSL message automatically when a NAT pool runs out of addresses (also referred to as pool exhaustion).

Restrictions for NAT HSL

- Service-side NAT VRF does not support IPv6 addresses.
- Export of an IPv6 target in a service-side VRF is not supported.
- Export of translations using IPv6 in a VRF is not supported.

Prerequisites for NAT HSL

- Ensure that the NAT translations are available on the router.
- Confirm that the log messages are being generated.

Best Practices for NAT HSL

- Verify that the configured IP address and port address for logging are as per the configurations in the collector.
- Use the **show interface statistics** command to verify the output packet counters and confirm the flow of packets from the router interface connecting to the collector.

Configure NAT HSL Using a CLI Template



Note By default, CLI templates execute commands in global configuration mode.

The following is a sample CLI configuration to enable the high-speed logging of translations by NAT using a flow exporter:

ip nat log translations flow-export v9 udp destination *IPv4address-port* **source** *interface-name interface-number*

The following is a configuration example to enable translation logging for a specific destination and source interface:

```
ip nat log translations flow-export v9 udp destination 10.10.0.1 1020 source gigabithethernet
 0/0/1
```

Verify NAT HSL Configuration

The following is a sample output from the **show ip nat translations** command. You can view the translations log in the export target collector.

```
Device# show ip nat translations
Pro  Inside global      Inside local          Outside local         Outside global
---------------------------------------------------------------------------------------
tcp  10.0.0.16:5092     10.0.0.16:56991       209.165.202.129:80    209.165.202.129:80
tcp  10.0.0.16:5078     10.0.0.16:55951       172.16.128.7:80       172.16.128.7:80
tcp  10.0.0.16:5070     10.0.0.16:57141       172.16.128.7:80       172.16.128.7:80
tcp  10.0.0.16:5089     10.0.0.16:55823       209.165.202.129:80    209.165.202.129:80
tcp  10.0.0.16:5103     10.0.0.16:58717       172.16.128.7:80       172.16.128.7:80
tcp  10.0.0.16:5064     10.0.0.16:55413       209.165.202.129:80    209.165.202.129:80
tcp  10.0.0.16:5091     10.0.0.16:59331       209.165.202.129:80    209.165.202.129:80
tcp  10.0.0.16:5100     10.0.0.16:59795       209.165.202.129:80    209.165.202.129:80
tcp  10.0.0.16:5097     10.0.0.16:57695       209.165.202.129:80    209.165.202.129:80
tcp  10.0.0.16:5096     10.0.0.16:55665       209.165.202.129:80    209.165.202.129:80
tcp  10.0.0.16:5066     10.0.0.16:58671       172.16.128.7:80       172.16.128.7:80
```

The following is a sample output from the **show platform hardware qfp active feature nat datapath hsl** command that is used to verify the configurations:

```
Device# show platform hardware qfp active feature nat datapath hsl
HSL cfg dip 10.10.0.1 dport 1020 sip 10.21.0.16 sport 53738 vrf 0
nat hsl handle 0x3d007d template id 261 pool_exh template id 263
```

```
LOG_TRANS_ADD 132148
LOG_TRANS_DEL 132120
LOG_POOL_EXH 0
```

The following is a sample output from the **show vrf detail** command:

```
Device# show vrf detail
VRF 1 (VRF Id = 1); default RD <not set>; default VPNID <not set>
  New CLI format, supports multiple address-families
  Flags: 0x1808
  Interfaces:
    Gi0/0/1      Gi0/0/2.102      Lo0    Vl103
Address family ipv4 unicast (Table ID = 0x1):
  Flags: 0x0
  No Export VPN route-target communities
  No Import VPN route-target communities
  No import route-map
  No global export route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
Address family ipv6 unicast (Table ID = 0x1E000001):
  Flags: 0x0
  No Export VPN route-target communities
  No Import VPN route-target communities
  No import route-map
  No global export route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
Address family ipv4 multicast not active
Address family ipv6 multicast not active
```

Source Port Preservation for Known Cisco Catalyst SD-WAN Ports

The following sections provide information for well-known Cisco Catalyst SD-WAN ports.

Information About Source Port Preservation for the Well-Known Cisco Catalyst SD-WAN Ports

Cisco Catalyst SD-WAN deployment uses UDP port number ranging 12346 to 12445 and TCP ports ranging 23456 to 24356 for control connections on Cisco IOS XE Catalyst SD-WAN devices. When an external Cisco IOS XE Catalyst SD-WAN device is behind the firewall during NAT, the control traffic port can translate to a different port. This is normally not an issue but when BFD sessions go down, NAT translates the new BFD control packet to a different port. The firewall doesn't accept the newly translated port and drops BFD packets as it has saved translated port of the older BFD session.

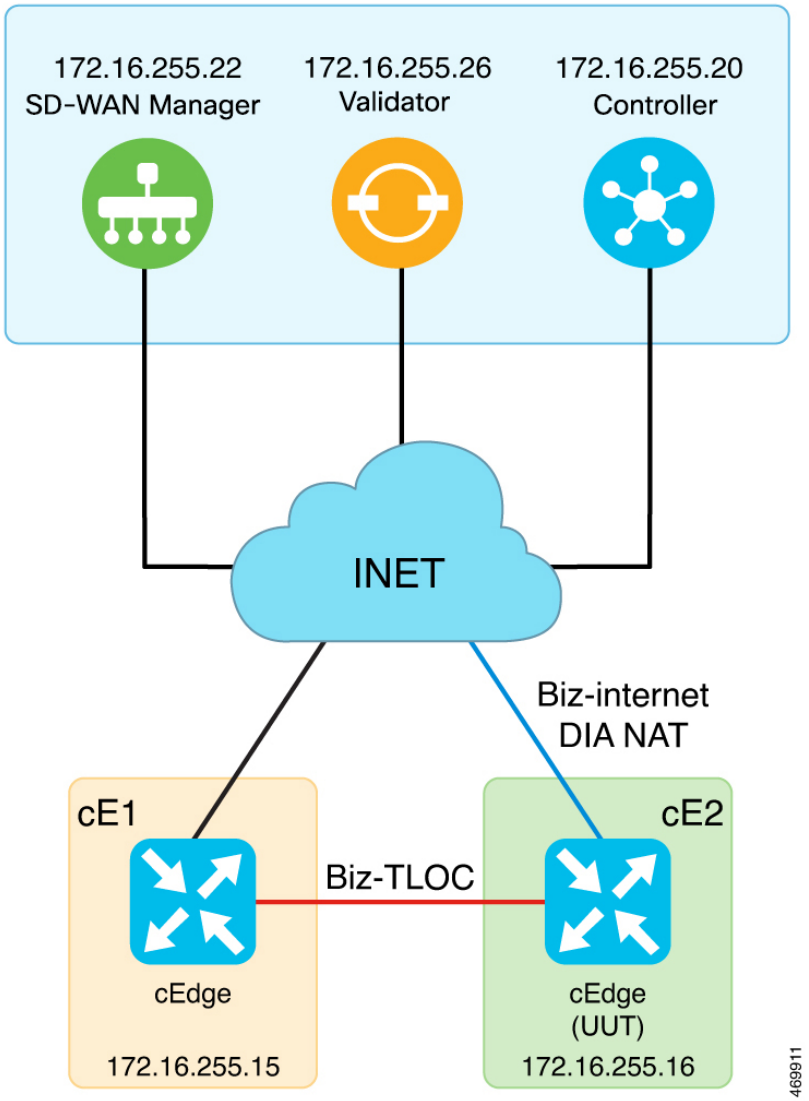
With this feature, you can configure Cisco IOS XE Catalyst SD-WAN devices to preserve the source ports for the known Cisco Catalyst SD-WAN ports during NAT. There is a set of reserved ports for the control traffic and within this range the ports are preserved during NAT. On enabling this feature, Cisco IOS XE Catalyst SD-WAN device preserves the source port from the known SD-WAN port range. Thus, firewall can handle Cisco Catalyst SD-WAN devices behind NAT.

Note Ensure that no service side traffic uses these port ranges, else it results in control connections failure.

Enabling the feature allows source port preservation for control traffic using Cisco Catalyst SD-WAN known ports for the following NAT mapping conditions:

- Interface overload
- Loopback overload

Figure 6: Topology of Source Port Preservation in Cisco Catalyst SD-WAN Deployment



The topology depicts a dual router site. cE1 has tloc-extension configured to use cE2 for INET connectivity to reach controllers. cE1 is using the known Cisco Catalyst SD-WAN port 12346, when the packet reaches cE2. The NAT functionality on cE2 preserves this source port number 12346 and doesn't change it before sending the packets out.

Features of Source Port Preservation

- The traffic with the specified port within the reserved port range is translated to the same port after configuring **ip nat settings preserve-sdwan-ports** command.

- As the locally generated traffic does not go through NAT, they always get port preservation in the reserved port range. If a local and an external device are using the same port in the reserved port range, the local traffic gets the preference.
- Reserved ports for UDP are in the range 12346—12426, and for TCP reserved port range is 23456—24356.
- TLS (TCP) control connections can take port value > 1024. As source port preservation is only supported for the reserved port range 23456—24356 for TCP, any other port value may not be preserved after translation.

Prerequisites for Source Port Preservation

If there are existing NAT mapping configurations, ensure that you reboot the device after configuring the **ip nat settings preserve-sdwan-ports** command to achieve the expected behavior. If not, add NAT mapping configurations after configuring the **ip nat settings preserve-sdwan-ports** command.

Restrictions for Source Port Preservation

- Service-side traffic cannot use the reserved port range.
- If the Cisco Catalyst SD-WAN well-known port is already allocated for a flow and another flow requests translation for the same port, then the packets for the new flows are dropped.
- If there are existing NAT mapping configurations, reboot the device after executing the **ip nat settings preserve-sdwan-ports** command to achieve the expected behavior. If not, add the NAT mapping configurations after executing the **ip nat settings preserve-sdwan-ports** command.

Configure Source Port Preservation for DIA Interface Overload Using a CLI Template



Note By default, CLI templates execute commands in global config mode.

This section provides example CLI configurations to configure source ports preservation for the known Cisco Catalyst SD-WAN ports during NAT.

1. Enable source port preservation during NAT:

   ```
   ip nat settings preserve-sdwan-ports
   ```

2. Enable NAT of the inside source address for DIA interface overload:

   ```
   ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet1 overload
   ```

3. Configure an interface type and enter the interface configuration mode:

   ```
   interface GigabitEthernet1
   ```

4. Enable the interface:

   ```
   no shutdown
   ```

5. Configure the IP address:

   ```
   ip address 10.1.16.16 255.255.255.0
   ```

6. Connect the interface to the outside network:

```
ip nat outside
```

Here's the complete configuration examples for port preservation during DIA interface overload:

```
ip nat settings preserve-sdwan-ports
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet1 overload
!
interface GigabitEthernet1
 no shutdown
 ip address 10.1.16.16 255.255.255.0
 ip nat outside
```

Configure Source Port Preservation for DIA Pool Overload Using a CLI Template

Note By default, CLI templates execute commands in global config mode.

This section provides example CLI configurations to configure source ports preservation for the known Cisco Catalyst SD-WAN ports during NAT.

1. Enable source port preservation during NAT:

   ```
   ip nat settings preserve-sdwan-ports
   ```

2. Define a pool of IP addresses for NAT:

   ```
   ip nat pool natpool-GigabitEthernet1-0 10.1.16.201 10.1.16.250 prefix-length 24
   ```

3. Enable NAT of the inside source address for DIA pool overload:

   ```
   ip nat inside source list global-list pool natpool-GigabitEthernet1-0 overload
   egress-interface GigabitEthernet1
   ```

4. Configure an interface type and enter the interface configuration mode.

   ```
   interface GigabitEthernet1
   ```

5. Enable the interface:

   ```
   no shutdown
   ```

6. Configure the IP address.

   ```
   ip address 10.1.16.16 255.255.255.0
   ```

7. Connect the interface to the outside network.

   ```
   ip nat outside
   ```

Here's the complete configuration examples for port preservation during DIA pool overload:

```
ip nat settings preserve-sdwan-ports
ip nat pool natpool-GigabitEthernet1-0 10.1.16.201 10.1.16.250 prefix-length 24
ip nat inside source list global-list pool natpool-GigabitEthernet1-0 overload
egress-interface GigabitEthernet1
!
interface GigabitEthernet1
 no shutdown
```

```
ip address 10.1.16.16 255.255.255.0
ip nat outside
```

Configure Source Port Preservation for DIA Loopback Overload Using a CLI Template

Note By default, CLI templates execute commands in global config mode.

This section provides example CLI configurations to configure source ports preservation for the known Cisco Catalyst SD-WAN ports during NAT.

1. Enable source port preservation during NAT:

   ```
   ip nat settings preserve-sdwan-ports
   ```

2. Enable NAT of the inside source address for DIA loopback overload:

   ```
   ip nat inside source list global-list interface Loopback16 overload egress-interface
   GigabitEthernet1
   ```

3. Configure the loopback interface:

   ```
   interface Loopback16
   ```

4. Configure the IP address on the loopback interface:

   ```
   ip address 10.20.16.16 255.255.255.0
   ```

5. Configure an interface type and enter the interface configuration mode:

   ```
   interface GigabitEthernet1
   ```

6. Configure the IP address:

   ```
   ip address 10.1.16.16 255.255.255.0
   ```

7. Connect the interface to the outside network:

   ```
   ip nat outside
   ```

Here's the complete configuration examples for port preservation during DIA loopback overload:

```
ip nat settings preserve-sdwan-ports
ip nat inside source list global-list interface Loopback16 overload egress-interface
GigabitEthernet1
!
interface Loopback16
 ip address 10.20.16.16 255.255.255.0
!
interface GigabitEthernet1
 ip address 10.1.16.16 255.255.255.0
 ip nat outside
```

Verify Source Port Preservation

The following is a sample output from the **show ip nat translations** command displaying the translations with well-known Cisco Catalyst SD-WAN source ports. Observe the inside local and inside global columns for the translations and verify the source ports being preserved:

```
Device# show ip nat translations
Pro  Inside global          Inside local          Outside local         Outside global
udp  10.1.16.201:12406      10.1.19.15:12406      10.0.5.21:12377       10.0.5.21:12377
udp  10.1.16.201:12406      10.1.19.15:12406      10.0.5.19:12355       10.0.5.19:12355
udp  10.1.16.201:12406      10.1.19.15:12406      10.0.5.11:12367       10.0.5.11:12367
udp  10.1.16.201:12406      10.1.19.15:12406      10.0.12.26:12346      10.0.12.26:12346
udp  10.1.16.201:12406      10.1.19.15:12406      10.1.14.14:12366      10.1.14.14:12366
udp  10.1.16.201:12406      10.1.19.15:12406      10.0.12.20:12356      10.0.12.20:12356
Total number of translations: 6
```

The following is a sample output from the **show sdwan bfd sessions table** command displaying the traffic with ports in control plane:

```
Device# show sdwan bfd sessions table
                                SRC    DST                    SITE
           DETECT      TX
SRC IP      DST IP      PROTO  PORT   PORT   SYSTEM IP      ID    LOCAL COLOR   COLOR
    STATE  MULTIPLIER  INTERVAL  UPTIME      TRANSITIONS
-------------------------------------------------------------------------------------------
10.1.15.15  10.0.5.11   ipsec  12366  12367  172.16.255.11  100   lte           lte
    up     7           1000      0:01:37:43  3
10.1.19.15  10.0.5.11   ipsec  12406  12367  172.16.255.11  100   biz-internet  lte
    up     7           1000      0:00:00:51  0
10.1.15.15  10.1.14.14  ipsec  12366  12366  172.16.255.14  400   lte           lte
    up     7           1000      0:01:37:43  3
10.1.19.15  10.1.14.14  ipsec  12406  12366  172.16.255.14  400   biz-internet  lte
    up     7           1000      0:00:00:51  0
10.1.15.15  10.1.16.16  ipsec  12366  12386  172.16.255.16  600   lte           biz-internet
  up     7           1000      0:00:31:41  0
10.1.19.15  10.1.16.16  ipsec  12406  12386  172.16.255.16  600   biz-internet  biz-internet
  down   7           1000      NA          0
10.1.15.15  10.0.5.21   ipsec  12366  12377  172.16.255.21  100   lte           lte
    up     7           1000      0:01:37:43  3
10.1.19.15  10.0.5.21   ipsec  12406  12377  172.16.255.21  100   biz-internet  lte
    up     7           1000      0:00:00:51  0
```

Destination NAT

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1

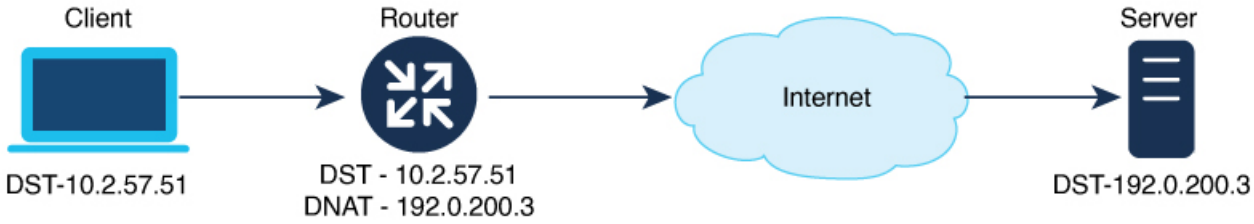
The following sections provide information on configuring Destination NAT with NAT Direct Internet Access (DIA).

Information about Destination NAT

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1

When you send a packet from the service side to the internet, NAT Direct Internet Access (DIA) translates the destination IP address, which can also be a private IP address, to a public IP address. This is known as destination NAT.

Any WAN edge device situated between two endpoints can be used to perform destination NAT. Destination NAT is used to redirect incoming packets with the destination of a private IP address to a public IP address. It is generally used to redirect packets destined for a specific IP address on one host to a different address on a different host.



Restrictions for Destination NAT

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1

- Only NAT DIA is supported with destination NAT.
- Only traffic originating from inside to outside direction is supported.
- Only data-policy-based DIA is supported.
- Does not support route-based DIA configurations.
- Does not support port forwarding with NAT DIA.
- Same NAT rules for packets are not applicable on different VRFs.
- NAT is not supported over SIG tunnel interface.

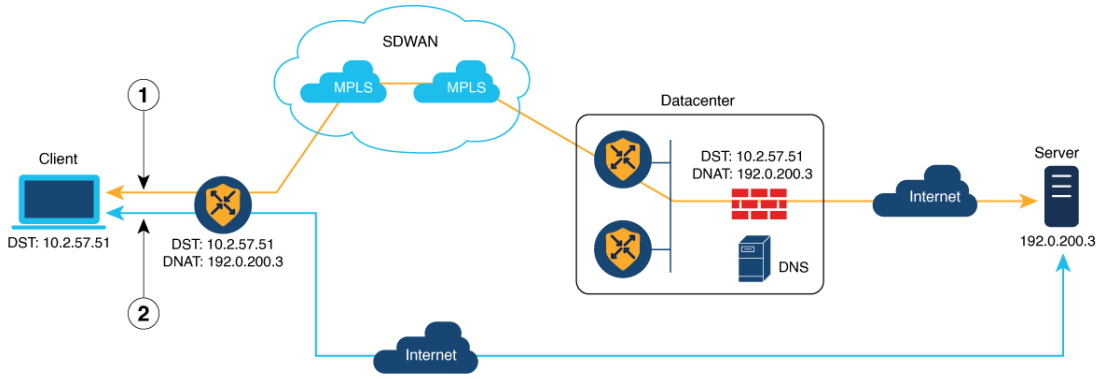
Use Case for Destination NAT

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1

A customer device using a Cisco VPN client initiates a DNS query to the device operating the firewall service, which is assigned with a private IP address. This private IP address is the overlay IP address. In case NAT DIA is not configured, the data policy uses VPN 0 fallback to the overlay to send the traffic to the firewall with the private IP address. The overlay IP address, which is a private IP address, is translated to a public IP address.

The prefered path for the traffic route is through the path with NAT DIA configured, where both the source and the destination IP addresses are translated.

Figure 7: Use Case for Destination NAT



1	Path without NAT configured	2	Path with NAT configured

Configure Destination NAT Using a CLI Template

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1

Note By default, CLI templates execute commands in global config mode.

To enable NAT of the outside source address:

ip nat outside source static *local-ip-address global-ip-address* **vrf** *vrf-name*

Here's a complete configuration example for destination NAT:

```
ip nat outside source static 192.0.200.3 10.2.57.51 vrf 1
```

Verify Destination NAT

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1

The following is a sample output from the **show sdwan policy from-vsmart** command.

```
Device# show sdwan policy from-vsmart

from-vsmart data-policy _1_vm5-vpn1-dia-policy
 direction all
 vpn-list 1
  sequence 1
   match
    source-ip      10.20.24.0/24
    destination-ip 10.2.57.51/24
   action accept
    nat use-vpn 0
    nat fallback
from-vsmart lists vpn-list 1
 vpn 1
```

In this example, you can check for the destination IP address and if the NAT fallback feature is configured.

The following is a sample output from the **show ip nat translations** command.

```
Device# show ip nat translations

Pro   Inside global    Inside local    Outside local     Outside global
---   ---              ---             10.2.57.51        192.0.2.1
tcp   203.0.113.1:5062 10.0.0.1:30427  10.2.57.51:1024   192.0.2.1:1024
```

In this example, the **outside local** IP address shows the private IP address that is translated to a public IP address in **outside global**.

Troubleshoot Destination NAT

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1

To check the original and the translated IP address, use the **show platform hardware qfp active feature nat datapath bind** command.

```
Device# show platform hardware qfp active feature nat datapath bind

Bind longest chain 1 avg non-zero bucket len 1 non-zero bkts 2
bind 0xed7739c0 oaddr 8.8.8.8 taddr 4.1.1.5 oport 0 tport 0 vrfid 1 tableid 1 proto 0 domain
 1 create time 78840 refcnt 1 mask 0x0 cgn flags 0 timeout 0 ifhandle 0 wlan_info 0x0 flags
 0x2100 mapping 0x0 cp_mapping_id 1 limit_type 0  last_use_ts 82071 mibp 0x0 bind_pool_id:
 0 rg 0 nak_retry 0 parent 0x0 egress_ifh 0 in2out_pkts 0 out2in pkts 0
```

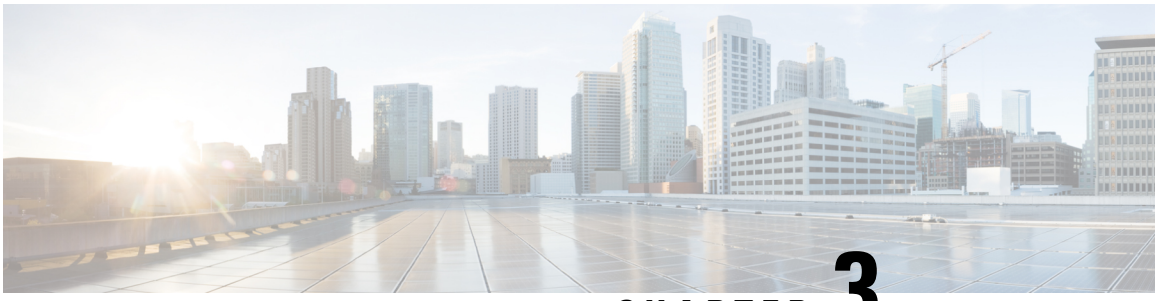
To check if the traffic is going on the DIA interface, check the packet count using the **show sdwan policy data-policy-filter** command.

```
Device# show sdwan policy data-policy-filter
                                                        POLICER  OOS      OOS
NAME  NAME   COUNTER NAME          PACKETS  BYTES  NAME     PACKETS  BYTES
------------------------------------------------------------------------------
u5    vpn-1  DNAT-DIA-COUNTER      5        570
             default_action_count  158      14340
```

To check the traffic flow on the fallback interface when the DIA interface is down, use the **show plat hard qfp active feature sdwan datapath statistics | inc fallback**

```
Device# show plat hard qfp active feature sdwan datapath statistics | inc fallback

data-policy-in-sig-fallback-flow-set-fail 0
data-policy-in-nat-fallback 0
data-policy-out-nat-fallback 0
```



CHAPTER 3

NAT DIA Tracker

Table 6: Feature History

Feature Name	Release Information	Description
NAT DIA Tracker for Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature allows you to configure a system tracker to probe the transport interface periodically to determine if the internet or external network becomes unavailable. You can configure the DIA tracker using the **Tracker** tab of the **Cisco System** template. You can apply the tracker to a transport interface using either the **Cisco VPN Interface Ethernet** or the **Cisco VPN Interface Cellular** template.
Dual Endpoint Support for Interface Status Tracking 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 tracker groups with dual endpoints using the Cisco SD-WAN Manager system template and associate each tracker group to an interface. Despite having an active Internet connection, a single endpoint may sometimes be inactive. This condition leads to false negatives. To overcome this disadvantage of a single endpoint tracker, you can use a dual endpoint tracker configuration.

Feature Name	Release Information	Description
NAT DIA Tracker for IPv6 Interface	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	NAT DIA tracker is now supported on IPv6 interfaces. You can configure IPv6 DIA tracker using the **IPv6-Tracker** and **IPv6-Tracker Group** options under transport profile in configuration groups.
ICMP Endpoint Tracker for NAT DIA for IPv4 or IPv6 Interfaces	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	This feature allows you to configure an ICMP endpoint tracker over a DIA path. You can configure ICMP probes for NAT DIA on IPv4 or IPv6 endpoints. You can configure the ICMP tracker using the **Tracker** or the **IPv6 Tracker** features under transport profile in configuration groups. Configure a **Tracker DIA Stabilize Status** setting in the **Basic** feature profile to stabilize rapid tracker status changes that cause interface flaps.

- Information About NAT DIA Tracking, on page 60
- ICMP Endpoint Tracker for NAT DIA, on page 61
- Supported Interfaces for NAT DIA Tracker, on page 63
- Restrictions for NAT DIA Tracker, on page 63
- Workflow for NAT DIA Tracker on IPv4 Interfaces, on page 64
- Configure NAT DIA Tracker on IPv4 Interfaces in Cisco SD-WAN Manager, on page 64
- Configure NAT DIA Tracker, on page 66
- Monitor NAT DIA Tracker Configuration on IPv4 Interfaces, on page 72
- Verify the Configurations for NAT DIA Tracker on IPv4 Interfaces , on page 73
- Workflow for NAT DIA Tracker on IPv6 Interfaces, on page 75

Information About NAT DIA Tracking

The DIA tracker helps determine if the internet or external network has become unavailable. The NAT DIA Tracking 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 to determine the status of the internet and return 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 from Service VPN, 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.

From Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, you can configure a tracker group with two trackers, and associate this tracker group to an interface. Probing a tracker group with two trackers (two endpoints) helps in avoiding false negatives that might be introduced when an internal or external network gets erroneously marked as unavailable.

From Cisco IOS XE Catalyst SD-WAN Release 17.11.1a, you can configure NAT DIA tracker on IPv6 interfaces. The tracker and tracker group address type should match IPv4 or IPv6 address types on the interface configuration. For example, if an IPv4 address is configured on a NAT DIA interface, only an IPv4 tracker can be applied. If an IPv6 address is configured on a NAT DIA interface, only an IPv6 tracker can be applied. If both IPv4 and IPv6 addresses are configured on a NAT DIA interface, both IPv4 and IPv6 tracker can be applied correspondingly.

ICMP Endpoint Tracker for NAT DIA

From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, you can configure ICMP endpoint trackers on any NAT-enabled IPV4 or IPv6 transport interfaces used for NAT DIA. The ICMP tracker detects failures along the internet path to a given external service by sending probes to a configured external endpoint and monitors whether the probes fail or succeed. If the number of probes exceed the configured multiplier value, or if the ICMP probes exceed the configured threshold, the tracker considers the external endpoint unreachable and makes the transport interface unavailable for DIA.

ICMP probes ensure shorter failovers when the transport interface becomes unavailable for DIA. You can configure either endpoint IP or the endpoint DNS name for ICMP endpoint trackers. You can create a tracker group if you have configured more than one IPv4 or IPv6 tracker.



Warning Ensure that you configure a host route to egress through the DIA interface where you've configured the ICMP tracker. This ensures that the intended tracker interface receives the ICMP probe. When an endpoint is reachable through an interface other than the interface configured for ICMP tracker, the ICMP probes may be sent to the interface which is not tracked, causing ICMP probes to egress via an unintended interface.

You can configure the following types of ICMP Endpoint Tracker for NAT DIA:

Table 7: Types of ICMP Endpoint Trackers

Tracker	Supported Tracker Type
Single NAT DIA ICMP tracker	Tracker type: • IPv4 • IPv6 Tracker endpoint type: • Endpoint IP • DNS
NAT DIA ICMP tracker group	Tracker type: • IPv4 • IPv6 Tracker endpoint type: • Endpoint IP
NAT DIA Mixed Tracker Group (HTTP and ICMP)	Tracker type: • IPv4 • IPv6 Tracker endpoint type: • Endpoint IP

Supported Devices for ICMP Trackers

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1.

Restrictions for ICMP Trackers

- You cannot configure ICMP endpoint tracker type through feature templates.
- You cannot configure both an IPv4 and an IP6 tracker type in the same tracker group.
- You can configure the ICMP endpoint tracker for NAT DIA for the following interfaces only:
  - Ethernet Interfaces
  - Ethernet (PPPoE) Interfaces
  - Subinterfaces

- If only one DIA interface (default route) is configured, and the ICMP tracker goes down, the default route is withdrawn.

Supported Interfaces for NAT DIA Tracker

You can configure the NAT DIA tracker for the following interfaces:

- Cellular Interfaces

Note Cellular interfaces don't support negotiated IP addresses.

- Ethernet Interfaces
- Ethernet (PPPoE) Interfaces
- Subinterfaces
- DSL Dialer Interfaces (PPPoE and PPPoA)

Note IPv6 NAT DIA tracker is supported only on physical and subinterfaces of Ethernet interfaces.

Restrictions for NAT DIA Tracker

Restrictions for Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Earlier Releases

- In Cisco IOS XE Release 17.6.x and earlier, the NAT DIA tracker is not supported on dialer interfaces. From Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, subinterfaces and dialer interfaces support single endpoint and dual endpoint trackers.
- DNS URL endpoint is not supported on Cisco IOS XE Catalyst SD-WAN devices.
- You can apply only one tracker or tracker group to an interface.
- The NAT fallback feature is supported only from Cisco IOS XE Catalyst SD-WAN Release 17.3.2.
- The IP address of the tunnel with address 169.254.x.x is not supported to track the zScaler endpoint on manual tunnels.
- You must configure a minimum of two single endpoint trackers to configure a tracker group.
- A tracker group can incorporate only a maximum of two single endpoint trackers.
- In Cisco IOS XE Release 17.10.1 and previous releases, you cannot configure IPv4 tracker on a IPv6 interface or vice versa. The tracker will not be active.

Restrictions for Cisco IOS XE Catalyst SD-WAN Release 17.11.1a

- API URL endpoint is supported only on IPv6 DIA tracker and not supported on IPv4 DIA tracker.
- Both IPv4 and IPv6 trackers cannot be used in the same tracker group.
- You must configure the **allow service all** command under the TLOC tunnel interface for IPv6 trackers to work with a TLOC tunnel interface.
- Multiple NAT66 DIA interfaces are not supported.

Restrictions for Cisco IOS XE Catalyst SD-WAN Release 17.13.1a

- Name resolution process is not bond to the ET interface. Name resolution is using VPN 0 routing table. It can exit any active interface with proper routing.

Workflow for NAT DIA Tracker on IPv4 Interfaces

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

1. Configure an interface tracker using a **Cisco System** template. From Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, you can configure a dual tracker or a tracker group.
2. Apply the tracker to a transport interface.
3. Verify NAT DIA tracker configuration.

Configure NAT DIA Tracker on IPv4 Interfaces in Cisco SD-WAN Manager

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

Use the **Cisco System** template to track the status of transport interfaces.

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



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

3. Click **…** adjacent to the **Cisco System** template that you want to modify and choose **Edit**.
4. Click **Tracker**, and click **New Endpoint Tracker** to configure the tracker parameters.

Table 8: Tracker Parameters

Parameter Field	Description
Name	Name of the tracker. The name can be up to 128 alphanumeric characters. You can configure up to eight trackers.
Threshold	Duration 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	Frequency at which a probe is sent to determine the status of the transport interface. *Range:* 20 to 600 seconds. *Default:* 60 seconds (1 minute)
Multiplier	Number of times a probe can be resent before declaring that the transport interface is down. *Range:* 1 to 10. *Default:* 3
Tracker Type	Choose **Interface** to configure the DIA tracker.
End Point Type: IP Address	IP address of the end point. This is the destination in the internet to which the router sends probes to determine the status of the transport interface. Make sure that the IP address is enabled to respond to HTTP port 80 probes.
End Point Type: DNS Name	DNS name of the end point. This is the destination in the internet to which the router sends probes to determine the status of the transport interface.

5. Click **Add**.
6. To create a tracker group and configure the parameters, click **Tracker Groups** > **New Endpoint Tracker Groups**.

Table 9: Tracker Group Parameters

Parameter Field	Description
Tracker Type: Tracker Elements	This field is displayed only if you chose **Tracker Type** as the **Tracker Group**. 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 an interface.
Tracker Type: 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.

Note Ensure that you have configured two single endpoint trackers before configuring a tracker group.

7. Click **Add**.
8. Click **Advanced** and enter the **Track Interface** information.

   Enter the name of the tracker to track the status of transport interfaces that connect to the internet.

Note Tracking the interface status is useful when you enable NAT in 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 in 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 functioning again, the route to the internet is reinstalled.

Note Ensure that you complete filling all the mandatory fields before you update the template.

9. Click **Update**.

Configure NAT DIA Tracker

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco Catalyst SD-WAN Control Components Release 20.7.1.

From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, you can configure ICMP trackers for NAT DIA.

Configure NAT DIA Tracker on IPv4 Interfaces using Configuration Groups in Cisco SD-WAN Manager

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1

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

   In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.

2. Configure a Tracker in a Transport and Management Profile.

   Table 10: Tracker

Field	Description
Tracker Name*	Name of the tracker. The name can be up to 128 alphanumeric characters.

Field	Description
Endpoint Tracker Type*	Choose a tracker type to configure endpoint trackers: • **http** • **icmp** This tracker type is available from Cisco Catalyst SD-WAN Manager Release 20.13.1.
Endpoint	Choose an endpoint type: • **Endpoint IP**: When you choose this option, the following field appears: **Endpoint IP**: IP address of the endpoint. This is the destination on the internet to which the probes are sent to determine the status of an endpoint. • **Endpoint DNS Name**: When you choose this option, the following field appears: **Endpoint DNS Name**: DNS name of the endpoint. This is the destination on the internet to which probes are sent to determine the status of the endpoint. The DNS name can contain a minimum of one character and a maximum of 253 characters. • **Endpoint API URL**: When you choose this option, the following field appears: **API URL of endpoint***: API URL for the endpoint of the tunnel. This is the destination on the internet to which probes are sent to determine the status of the endpoint.
Interval	Time interval between probes to determine the status of the configured endpoint. From Cisco Catalyst SD-WAN Manager Release 20.13.1, this option is called **Probe Interval**, allowing you to configure the time interval between probes. Range: 20 to 600 seconds Default: 60 seconds (1 minute). From Cisco Catalyst SD-WAN Manager Release 20.13.1, if you select **icmp** as the endpoint tracker type, the default probe interval is 2 seconds.
Multiplier	Number of times probes are sent before declaring that the endpoint is down. Range: 1 to 10 Default: 3

Field	Description
Threshold	Wait time for the probe to return a response before declaring that the configured endpoint is down. Range: 100 to 1000 milliseconds Default: 300 milliseconds

3. Configure **Tracker Group**.

Table 11: 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.
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.

4. After you create a configuration group, add devices to the group. For more information, see Add Devices to a Configuration Group in *Cisco Catalyst SD-WAN Configuration Groups Reference Guide*. You can then go ahead and deploy the devices associated to the configuration group. For more information, see Deploy Devices in *Cisco Catalyst SD-WAN Configuration Groups Reference Guide*.

Configure NAT DIA Tracker on IPv4 Interfaces Using the CLI

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

Configure a NAT DIA Tracker Using the CLI (Single Endpoint)

You can configure NAT DIA tracking using a CLI add-on feature template or CLI device template.

```
Device# config-transaction
Device(config)# endpoint-tracker tracker1
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)# tracker-type interface
```

Configure Tracker Groups

You can create tracker groups to probe NAT DIA tracker from Cisco IOS XE Catalyst SD-WAN Release 17.7.1a:

```
Device# config-transaction
Device(config)# endpoint-tracker tracker-name1
Device(config-endpoint-tracker)# tracker-type interface
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-transaction
Device(config)# endpoint-tracker tracker-name2
Device(config-endpoint-tracker)# tracker-type interface
Device(config-endpoint-tracker)# endpoint-dns-name <dns-name>
Device(config-endpoint-tracker)# threshold value
Device(config-endpoint-tracker)# multiplier value
Device(config-endpoint-tracker)# interval value

Device(config)# endpoint-tracker tracker-group-name
Device(config-endpoint-tracker)# tracker-type tracker-group
Device(config-endpoint-tracker)# boolean or
Device(config-endpoint-tracker)# tracker-elements tracker-name1 tracker-name2
Device(config)# interface GigabitEthernet0/0/1
Device(config-if)# endpoint-tracker tracker-group-name
```

Note A tracker group can have a mix of endpoint trackers. You can combine an IP-address tracker with a DNS tracker to create a tracker group.

Configure an ICMP Tracker for NAT DIA Using the CLI

Configure an ICMP Tracker for NAT DIA Using the CLI

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1.

You can configure ICMP tracking for NAT DIA by using a CLI add-on profile or the Transport profile in a configuration group.

To configure single endpoints:

```
Device# config-transaction
Device(config)# endpoint-tracker t1
Device(config-endpoint-tracker)# tracker-type interface-icmp
Device(config-endpoint-tracker)# endpoint-ip ip-address
Device(config-endpoint-tracker)# threshold value
Device(config-endpoint-tracker)# multiplier value
Device(config-endpoint-tracker)# icmp-interval value
```

To configure a tracker group:

```
Device# config-transaction
Device(config)# endpoint-tracker tracker-name1
Device(config-endpoint-tracker)# tracker-type interface-icmp
Device(config-endpoint-tracker)# endpoint-ip <ip-address>
Device(config-endpoint-tracker)# threshold <value>
```

```
Device(config-endpoint-tracker)# multiplier <value>
Device(config-endpoint-tracker)# icmp-interval <value>

Device# config-transaction
Device(config)# endpoint-tracker <tracker-name2>
Device(config-endpoint-tracker)# tracker-type interface-icmp
Device(config-endpoint-tracker)# endpoint-dns-name <dns-name>
Device(config-endpoint-tracker)# threshold <value>
Device(config-endpoint-tracker)# multiplier <value>
Device(config-endpoint-tracker)# icmp-interval <value>

Device(config)# endpoint-tracker tracker-group-name
Device(config-endpoint-tracker)# tracker-type tracker-group
Device(config-endpoint-tracker)# boolean or
Device(config-endpoint-tracker)# tracker-elements tracker-name1 tracker-name2
Device(config)# interface GigabitEthernet0/0/1
Device(config-if)# endpoint-tracker tracker-group-name
```

The following example shows how to configure a tracker with endpoint IP address:

```
Device(config)# endpoint-tracker tracker1
Device(config-endpoint-tracker)# endpoint-ip 10.1.1.1
Device(config-endpoint-tracker)# threshold 100
Device(config-endpoint-tracker)# multiplier 5
Device(config-endpoint-tracker)# interval 2
Device(config-endpoint-tracker)# tracker-type interface
```

The following example shows how to configure a tracker with endpoint as a DNS:

```
Device(config)# endpoint-tracker tracker2
Device(config-endpoint-tracker)# endpoint-dns-name www.example.com
Device(config-endpoint-tracker)# threshold 100
Device(config-endpoint-tracker)# multiplier 5
Device(config-endpoint-tracker)# interval 2
```

The following example shows how to configure an ICMP tracker with endpoint IP address:

```
Device(config)# endpoint-tracker tracker3
Device(config-endpoint-tracker)# tracker-type interface-icmp
Device(config-endpoint-tracker)# endpoint-ip 10.1.1.1
Device(config-endpoint-tracker)# threshold 100
Device(config-endpoint-tracker)# multiplier 5
Device(config-endpoint-tracker)# icmp-interval 2
```

The following example shows how to configure an ICMP tracker with endpoint as a DNS:

```
Device(config)# endpoint-tracker tracker4
Device(config-endpoint-tracker)# tracker-type interface-icmp
Device(config-endpoint-tracker)# endpoint-dns-name www.example.com
Device(config-endpoint-tracker)# threshold 100
Device(config-endpoint-tracker)# multiplier 5
Device(config-endpoint-tracker)# icmp-interval 2
```

Configuration Examples for NAT DIA Tracking on IPv4 Interfaces Using the CLI

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

The following sections provide examples for configuring NAT DIA trackers using the CLI.

Configuration Example: Single Endpoint NAT DIA Tracker Using the CLI

This example shows how to configure a single endpoint NAT DIA tracker:

```
config-transaction
    endpoint-tracker tracker1
    tracker-type interface
    endpoint-ip 10.1.1.1
    threshold 100
    multiplier 5
    interval 20
exit
```

Configuration Example: Tracker Groups

This example shows how to configure a tracker group with two trackers (two endpoints). You can create tracker groups to probe an interface from Cisco IOS XE Catalyst SD-WAN Release 17.7.1a.

```
config-transaction
    endpoint-tracker tracker1
    endpoint-ip 10.1.1.1
    interval 20
    threshold 100
    multiplier 1
    tracker-type interface
exit

endpoint-tracker tracker2
    endpoint-dns-name www.cisco.com
    interval 600
    threshold 1000
    multiplier 10
    tracker-type interface
exit

endpoint-tracker group1
    tracker-type tracker-group
    boolean or
    tracker-elements tracker1 tracker2
exit
```

This example shows how to apply a tracker group to an interface and configure it in the supported interfaces:

```
interface GigabitEthernet0/0/1
    endpoint-tracker group1
```

Stabilize NAT DIA Tracker Status

From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, you can configure a global configuration setting called **Tracker DIA Stabilize Status** using the **Basic** feature profile in Cisco SD-WAN Manager. Alternatively, you can use the **dia-stabilize-status** command by using the CLI. This configuration is applied to all endpoint-tracker state changes across DIA interfaces, both HTTP, and ICMP to stabilize the tracker states and avoid rapid interface flaps due to rapid status changes.

When you configure the endpoint tracker for an interface, the tracker starts tracking that endpoint by sending HTTP or ICMP probes. If the endpoint is reachable, or when the probe is successful, the tracker is marked as UP. If the endpoint is not reachable, or when the probe is unsuccessful, the tracker is marked as DOWN. To avoid a continuous change in the tracker status, a multiplier is applied to ensure that the tracker status changes only after a significant number of probes.

The Multiplier specifies the number of times probes are sent before declaring that the endpoint is down. The range is 1–10 and the default is 3. The multiplier is used to probe the tracker repeatedly, based on the configured value, and marks the tracker as UP if the probe is successful only after the expiry of the multiplier. For example, if the multiplier is configured as 3, the status of the tracker changes to UP after 3 continuous successful probes.

The configured multiplier or retry value is applied to ensure that the probes are successful in bringing the tracker object up and notifying NAT. When the tracker state is up, NAT installs the route. This avoids interface flaps since the retries ensure that the tracker object is up. Prior to Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, for HTTP probes, the tracker is marked as down after probing for a number of times, as configured by the multiplier. Tracker is marked UP after the first successful probe. This mechanism causes network flaps. The **dia-stabilize-status** command stabilizes this behavior by using the value 'Multiplier+1' to change the status of the tracker. For example, if the value for the multiplier is 3, a tracker whose status is DOWN, is pinged 3+1 times (2 seconds apart, based on the ICMP interval). After the fourth probe is successful, the tracker is marked as UP.

In Cisco IOS XE Catalyst SD-WAN Release 17.12.x and earlier, the multiplier was used for SIG trackers (from UP to DOWN and DOWN to UP) and HTTP trackers (from UP to DOWN). From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **dia-stabilize-status** setting is applied to ICMP and HTTP trackers to track status transitions from DOWN to UP.

Configure Using CLI

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1

The following example shows how to configure this feature using the CLI:

```
device(config)# endpoint-tracker-settings dia-stabilize-status
```

Configure Using Cisco Catalyst SD-WAN Manager

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1

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

   For more information on creating a configuration group, see Configuration Group Workflows.

2. Add a feature to the configuration group.

   For more information on adding a feature, see Feature Management.

3. Under **System Profile**, configure the **Basic** feature.

   For more information about configuring the **Basic** feature, see Basic.

4. Click **Track Settings**.

5. Under **Tracker DIA Stabilize Status**, choose **Global** from the drop-down list, and enable the setting.

6. Click **Save**.

Monitor NAT DIA Tracker Configuration on IPv4 Interfaces

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

View Interface DIA Tracker

To view information about DIA tracker on a transport interface:

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**.

2. Choose a device from the list of devices.
3. Click **Real Time**.
4. For single endpoint tracker, from the **Device Options** drop-down list, choose **Endpoint Tracker Info**.
5. For dual endpoint tracker, from the **Device Options** drop-down list, choose **Endpoint Tracker Group Info**.

Verify the Configurations for NAT DIA Tracker on IPv4 Interfaces

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

You can check the command syntax after you attach a template to a device. The following sample configuration shows tracker definition for the NAT DIA tracker and how to apply a tracker to a transport interface:

```
endpoint-tracker tracker-t1
  threshold 1000
  multiplier 3
  interval 20
  endpoint-ip 10.1.16.13
  tracker-type interface

interface GigabitEthernet1
 no shutdown
 endpoint-tracker tracker-t1
 ip nat outside
```

The following sample configuration shows how to verify if the configuration is committed:

```
Device# show endpoint-tracker interface GigabitEthernet1

Interface          Record Name          Status        RTT in msecs    Probe ID        Next
 Hop
GigabitEthernet1   tracker-t1              UP             2               1
10.1.16.13
```

The following sample configuration shows timer-related information about the tracker, to help debug tracker-related issues, if any:

```
Device# show endpoint-tracker records
Record Name            Endpoint       EndPoint Type   Threshold    Multiplier   Interval
   Tracker-Type
p1                     10.1.16.13          IP              300          3          60
    interface
```



Note The **show endpoint-tracker** command does not display the NAT history records for a tracker when the interface is down and has an invalid network condition.

Verify Configuration for an ICMP Tracker

From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, you can check the command syntax after you configure the ICMP tracker. The following sample configuration shows ICMP tracker definition for the NAT DIA tracker and how to apply a tracker to a transport interface:

```
endpoint-tracker tracker-t2
  tracker-type interface-icmp
  endpoint-ip 10.1.16.13
  threshold 1000
  multiplier 3
  icmp-interval 2



interface GigabitEthernet1
 no shutdown
 endpoint-tracker tracker-t2
```

The following sample configuration shows how to verify if the configuration is committed:

```
Device# show endpoint-tracker interface GigabitEthernet1

Interface          Record Name          Status        RTT in msecs    Probe ID        Next
 Hop
GigabitEthernet1   tracker-t2             UP             2               1
10.1.16.13
```

Dual-Tracker Show Commands

The following is a sample output of the **show endpoint-tracker tracker-group** command:

```
Device# show endpoint-tracker tracker-group
Tracker Name               Element trackers name       Status      RTT in msec    Probe ID
interface-tracker-group     tracker1, tracker2      UP(UP OR UP)      1,1          53, 54
```

```
Device# show ip sla summary

IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending
All Stats are in milliseconds. Stats with u are in microseconds

ID           Type        Destination       Stats       Return Code     Last Run

*9           dns         10.1.1.1           RTT=3       OK          12 seconds ago
*10          http        10.1.1.10 .        RTT=89      OK          23 seconds ago
```

```
Device# show endpoint-tracker records
Record Name            Endpoint       EndPoint Type   Threshold    Multiplier   Interval
   Tracker-Type
group1          tracker1 OR tracker2       N/A            N/A          N/A         N/A
   tracker-group
group3          tracker3 OR tracker4       N/A            N/A          N/A         N/A
   tracker-group
tracker1             198.168.20.2          IP             300          3            60
     interface
tracker2             198.168.20.3          IP             300          3            60
     interface
tracker3         www.cisco.com.com      DNS_NAME          300          3            60
     interface
tracker4         www.cisco.com.com      DNS_NAME          300          3            60
     interface
```

The following is a sample output of the **show ip sla summary** command:

```
Device# show ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending
All Stats are in milliseconds. Stats with u are in microseconds
ID           Type       Destination      Stats   Return Code       Last Run
*53          http         10.1.1.1       RTT=2        OK        35 seconds ago
*54          http         10.1.1.10      RTT=2        OK        1 minute, 35 seconds ago
```

The following is a sample output of the **show endpoint-tracker tracker-group** command for ICMP endpoint trackers:

```
Device# show endpoint-tracker tracker-group
Tracker Name     Element trackers name     Address Family    Status            RTT in msec
      Probe ID
trackergroup1    tracker1, tracker2        IPv4              UP(UP OR UP)      1, 2
      5, 4
```

The following is a sample output of the **show ip sla summary** command for the ICMP endpoint tracker:

```
Device# show ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending
All Stats are in milliseconds. Stats with u are in microseconds
ID           Type       Destination      Stats   Return Code       Last Run
*4          icmp-echo    10.1.29.99      RTT=1        OK        1 seconds ago
```

Workflow for NAT DIA Tracker on IPv6 Interfaces

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1

Configure NAT DIA Tracker on IPv6 Interfaces using Configuration Groups in Cisco SD-WAN Manager

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1

Note You can configure the IPv6 DIA Tracker feature using a configuration group, device CLI template, or CLI-Add on feature template. This feature cannot be configured through a feature template.

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

   In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, choose **Configuration** > **Templates** > **Configuration Groups**.

2. Configure an IPv6 Tracker in a Transport and Management Profile.

Table 12: IPv6 Tracker

Field	Description
Type	Choose a feature from the drop-down list.

Field	Description
Feature Name*	Enter a name for the feature.
Description	Enter a description of the feature. The description can contain any characters and spaces.
Tracker Name*	Name of the tracker. The name can be up to 128 alphanumeric characters.
Endpoint Tracker Type*	Choose a tracker type to configure endpoint trackers: • **ipv6-interface** **Note** This tracker type is available only in Cisco Catalyst SD-WAN Manager Release 20.12.x and earlier. • **http** • **icmp** This tracker type is available from Cisco Catalyst SD-WAN Manager Release 20.13.1.
Endpoint	Choose an endpoint type: • **Endpoint DNS Name**: When you choose this option, the following field appears: **Endpoint DNS Name**: DNS name of the endpoint. This is the destination on the internet to which probes are sent to determine the status of the endpoint. The DNS name can contain a minimum of one character and a maximum of 253 characters. • **Endpoint IP**: When you choose this option, the following field appears: **Endpoint IP**: IPv6 address of the endpoint. This is the destination on the internet to which the probes are sent to determine the status of an endpoint. The IPv6 address can be a valid IPv6 address in dotted-decimal notation. • **Endpoint API URL**: When you choose this option, the following field appears: **API url of endpoint**: API URL of the endpoint. The API URL can be a valid URL as described by RFC 3986.

Field	Description
Interval	Time interval between probes to determine the status of the configured endpoint. From Cisco Catalyst SD-WAN Manager Release 20.13.1, this option is called **Probe Interval**, allowing you to configure the time interval between probes. Range: 20 to 600 seconds Default: 60 seconds (1 minute) From Cisco Catalyst SD-WAN Manager Release 20.13.1, if you select **icmp** as the endpoint tracker type, the default probe interval is 2 seconds.
Multiplier	Number of times probes are sent before declaring that the endpoint is down. Range: 1 to 10 Default: 3
Threshold	Wait time for the probe to return a response before declaring that the configured endpoint is down. Range: 100 to 1000 milliseconds Default: 300 milliseconds

3. Configure IPv6 tracker group.

Table 13: IPv6 Tracker Group

Field	Description
Tracker Name	Enter a tracker name.
Tracker Elements	This field is displayed only if you chose **Tracker Type** as the **Tracker Group**. 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 an interface.
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.

4. After you create a configuration group, add devices to the group. For more information, see Add Devices to a Configuration Group in *Cisco Catalyst SD-WAN Configuration Groups Reference Guide*. You can then go ahead and deploy the devices associated to the configuration group. For more information, see Deploy Devices in *Cisco Catalyst SD-WAN Configuration Groups Reference Guide*.

Configure NAT DIA Tracker on IPv6 Interfaces using a CLI Template

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1

Note You can't configure ICMP tackers using CLI templates.

Configure IPv6 Endpoint Tracker

1. Configure the endpoint tracker for tracking the status of an endpoint:

   endpoint-tracker *tracker-name*

2. Configure the tracker type for the tracker:

   tracker-type *ipv6-interface*

Note From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, you can configure ICMP tracking for NAT DIA using *ipv6-interface-icmp*.

3. Configure the IPv6 address of an endpoint:

   ipv6-endpoint *ipv6-address*

Note You can't configure an IPv4 and an IPv6 tracker in the same tracker group.

Here is the complete configuration example to configure an IPv6 endpoint tracker:

```
endpoint-tracker t1
   tracker-type ipv6-interface
   ipv6-endpoint 2001:DB8:1::1
```

Here is the complete configuration example to configure an IPv6 endpoint ICMP tracker:

```
endpoint-tracker t1
   tracker-type ipv6-interface-icmp
   ipv6-endpoint 2001:DB8:1::1
```

Configure DNS Tracker

1. Configure the endpoint tracker for tracking the status of an endpoint:

   endpoint-tracker *tracker-name*

2. Configure the tracker type for the tracker:

   tracker-type *ipv6-interface*

Note From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, you can configure ICMP tracking for NAT DIA using *ipv6-interface-icmp*.

3. Configure the domain name of an endpoint:

   endpoint-dns-name *dns-name*

Here is the complete configuration example to configure DNS tracker:

```
endpoint-tracker dns_t1
   tracker-type ipv6-interface
   endpoint-dns-name cisco.com
```

Here is the complete configuration example to configure DNS ICMP tracker:

```
endpoint-tracker dns_t1
   tracker-type ipv6-interface-icmp
   endpoint-dns-name cisco.com
```

Configure IPv6 Tracker Group

1. Configure an HTTP or ICMP IPv6 endpoint tracker.
2. Configure an HTTP or ICMP DNS tracker in IPv6 interface.
3. Configure the endpoint tracker for tracking the status of an endpoint:

   endpoint-tracker *tracker-group-name*
4. Configure the tracker type for the tracker:

   tracker-type *tracker-group*

Note From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, you can configure ICMP tracking for NAT DIA using *ipv6-interface-icmp*.

5. Enable Boolen logic while configuring a tracker group:

   boolean{**and** | **or**}
6. Add tracker names to create a dual endpoint tracker group:

   tracker-elements *tracker1 tracker2*

Here is the complete configuration example to configure IPv6 tracker group:

```
endpoint-tracker t1
   tracker-type ipv6-interface
   ipv6-endpoint 2001:DB8:1::1
!
endpoint-tracker t2
   tracker-type ipv6-interface
   endpoint-dns-name cisco.com
```

```
!
endpoint-tracker groupv6
   tracker-type tracker-group
   boolean or
   tracker-elements t1 t2
```

Here is the complete configuration example to configure IPv6 ICMP tracker group:

```
endpoint-tracker t3
   tracker-type ipv6-interface-icmp
   ipv6-endpoint 2001:DB8:1::1
!
endpoint-tracker t4
   tracker-type ipv6-interface-icmp
   endpoint-dns-name cisco.com
!
endpoint-tracker groupv7
   tracker-type tracker-group
   boolean or
   tracker-elements t3 t4
```

Configure Both IPv4 and IPv6 Trackers on the Same Interface

1. Configure the IPv4 endpoint tracker:

   ```
   endpoint-tracker t1
      tracker-type interface-ip
      endpoint-ip 10.1.1.1
   ```

2. Configure a DNS tracker in IPv4 interface.

   ```
   endpoint-tracker t2
      tracker-type interface-ip
      endpoint-dns-name example.com
   ```

3. Configure an IPv6 endpoint tracker.

   ```
   endpoint-tracker t3
      tracker-type ipv6-interface
      ipv6-endpoint 2001:DB8:1::1
   ```

4. Configure a DNS tracker in IPv6 interface.

   ```
   endpoint-tracker t4
      tracker-type ipv6-interface
      endpoint-dns-name cisco.com
   ```

5. Add IPv4 trackers to a tracker group:

   ```
   endpoint-tracker groupv4
      tracker-type tracker-group
      boolean and
      tracker-elements t1 t2
   ```

6. Add IPv6 trackers to a tracker group:

   ```
   endpoint-tracker groupv6
      tracker-type tracker-group
   ```

```
      boolean or
      tracker-elements t3 t4
```

7. Apply the tracker group to an interface:

```
interface GigabitEthernet1
 endpoint-tracker groupv4
 ipv6-endpoint-tracker groupv4
```

Here is the complete configuration example to configure both IPv4 and IPv6 trackers on the same interface:

```
endpoint-tracker t1
   tracker-type interface-ip
   endpoint-ip 10.1.1.1
!
endpoint-tracker t2
   tracker-type interface-ip
   endpoint-dns-name example.com
!
endpoint-tracker t3
   tracker-type ipv6-interface
   ipv6-endpoint 2001:DB8:1::1
!
endpoint-tracker t4
   tracker-type ipv6-interface
   endpoint-dns-name cisco.com
!
endpoint-tracker groupv4
   tracker-type tracker-group
   boolean and
   tracker-elements t1 t2
!
endpoint-tracker groupv6
   tracker-type tracker-group
   boolean or
   tracker-elements t3 t4
```

Configure an HTTP and an ICMP Tracker for a Tracker Group

Configure an HTTP IPv4 tracker and an ICMP IPv6 tracker, or vice versa on Cisco Catalyst SD-WAN devices, from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a

1. Configure an HTTP IPv4 endpoint tracker:

```
endpoint-tracker t1
   tracker-type interface
   endpoint-ip 10.1.1.1
```

2. Configure an ICMP IPv4 endpoint tracker.

```
endpoint-tracker t2
   tracker-type ipv6-interface-icmp
   endpoint-ip 10.1.1.2
```

3. Configure a tracker group with an HTTP and an ICMP endpoint tracker.

```
endpoint-tracker t3
   tracker-type tracker-group
   tracker-elements t1 t2
```

4. Apply the tracker group to an interface.

```
interface GigabitEthernet1
    endpoint-tracker t3
```

Apply a Defined IPv6 Tracker or Tracker Group to a Supported IPv6 Interface

1. Configure an interface type and enter the interface configuration mode:

```
interface GigabitEthernet1
```

2. Apply a predefined IPv6 endpoint tracker name:

   ipv6-endpoint-tracker *tracker-name*

Here is the complete configuration example to apply a tracker to an interface and configure it in the supported interfaces:

```
interface GigabitEthernet1
    ipv6-endpoint-tracker t1
```

Verify the Configurations for NAT DIA Tracker on IPv6 Interfaces

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1

The following is a sample output from the **show endpoint-tracker** command for a single IPv6 endpoint tracker configuration.

```
Device# show endpoint-tracker

endpoint-tracker t1
ipv6-endpoint 2001:DB8:1::1
tracker-type ipv6-interface
```

The following is a sample output from the **show endpoint-tracker** command for a single IPv6 endpoint tracker applied to an interface.

```
Device# show endpoint-tracker

Interface                    Record Name            Status          Address Family   RTT
in msecs    Probe ID        Next Hop
GigabitEthernet1                  t1                  Up              IPv6             1
             6               2001:DB8:1::1
```

The following is a sample output from the **show endpoint-tracker** command for a DNS tracker configuration.

```
Device# show endpoint-tracker

Interface                    Record Name            Status          Address Family   RTT
in msecs    Probe ID        Next Hop
GigabitEthernet1                 dns_t1              Up              IPv6             1
           9               2001:DB8:1::1
```

The following is a sample output from the **show endpoint-tracker tracker-group** command for an IPv6 tracker group configuration.

```
Device# show endpoint-tracker tracker-group

Tracker Name                      Element trackers name              Address Family   Status
                        RTT in msec      Probe ID
groupv6                                t1, t2                          IPv6             UP(UP
 OR UP)                  1, 0             10, 11
```

The following is a sample output from the **show endpoint-tracker** command when both IPV4 and IPv6 trackers are configured on the same interface.

```
Device# show endpoint-tracker

Interface                     Record Name            Status          Address Family   RTT
in msecs    Probe ID        Next Hop
GigabitEthernet1                   t1                 Up              IPv4             1
            7               10.0.29.99
GigabitEthernet1                   t2                 Up              IPv6             1
            8               2001:DB8:1::1
```

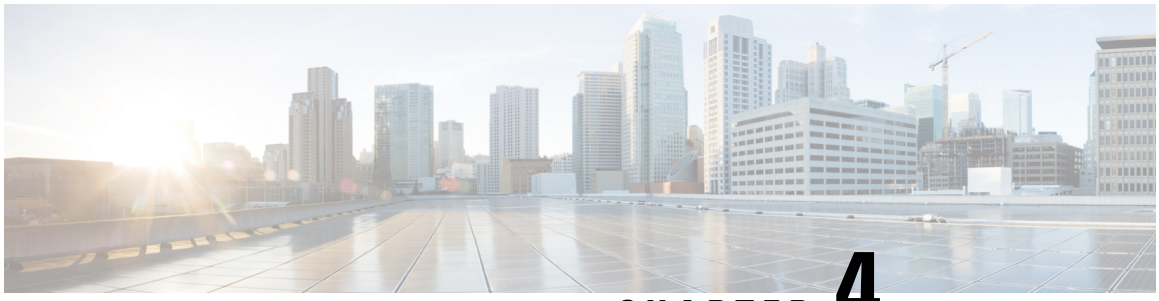
Verify Configuration for an ICMP Tracker

From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, you can check the command syntax after you attach a template to a device.

The following is a sample output from the **show endpoint-tracker** command for a single IPv6 ICMP endpoint tracker applied to an interface.

```
Device# show endpoint-tracker

Interface                     Record Name            Status          Address Family   RTT
in msecs    Probe ID        Next Hop
GigabitEthernet1                   t2                 Up              IPv6             1
             6              2001:DB8:1::1
```



CHAPTER 4

Service-Side NAT

Table 14: Feature History

Feature Name	Release Information	Description
Service-Side NAT on Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature allows you to configure inside and outside NAT on data traffic traveling to and from the service-side hosts of the network overlay. The service-side NAT configuration allows you to translate the source IP addresses for data traffic from service-side hosts to the overlay and traffic from the overlay to service-side hosts.
Intra-VPN Service-Side NAT Support	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	Intra-VPN allows service-side LAN interfaces to communicate with other service-side LAN interfaces within the same VPN. Configure the **ip nat outside** command on the LAN interface for which you require translation of the source IP addresses to the outside local addresses. You can apply static or dynamic NAT rules for packets to be routed from other LAN interfaces to the interface configured as the outside interface. You can configure intra-VPN service-side NAT using a device CLI template or a CLI add-on template.

Feature Name	Release Information	Description
Service-Side Conditional Static NAT Support	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This feature allows you to translate the same source IP address to different IP addresses based on the destination IP addresses. You can configure service-side conditional static NAT using a device CLI.
Service-Side Static Network NAT Support	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	This feature supports configuration of service-side static NAT for a subnet. Instead of configuring multiple static NAT pools, you can configure a single static NAT pool for an entire subnet. You can configure service-side static network NAT using Cisco SD-WAN Manager or a device CLI template.
Application-Level Gateway (ALG) in Service-Side NAT	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	Use an application-level gateway (ALG) to interpret the application-layer protocol and perform service-side NAT translations for FTP protocol.

- Information About Service-Side NAT, on page 86
- Traffic Flows for Service-Side NAT, on page 88
- Restrictions for Service-Side NAT, on page 88
- Configure Service-Side NAT, on page 89
- Configure Service-Side NAT Using the CLI, on page 94
- Intra-VPN Service-Side NAT, on page 99
- Service-Side Conditional Static NAT, on page 103
- Service-Side Static Network NAT, on page 105
- Application-Level Gateways with Service-Side NAT, on page 107

Information About Service-Side NAT

On a Cisco IOS XE Catalyst SD-WAN device, you can configure NAT on the service-side of the device so that data traffic is NATed before entering the overlay tunnel that is located in the transport VPN. The service-side NAT masks the IP address of data traffic it receives.

You can configure both dynamic and 1:1 static NAT on the service-side of a device. To do this, you configure a NAT pool interface within a service VPN on the device, and then you configure a centralized data policy on the Cisco Catalyst SD-WAN Controller. The policy directs data traffic with the desired prefixes to the service-side NAT. You configure either dynamic NAT or static NAT on the desired NAT pool interface.

When service-side NAT is enabled, all matching prefixes in VPN 1 are directed to the NAT pool interface. This traffic is NATed, with the NAT swapping out the service-side IP address and replacing it with its NAT pool IP address. The packet then gets forwarded to its destination.

You can configure NAT for data that enters or exits the service-side of the network. The service-side NAT translates data traffic, of inside and outside host addresses, that match a configured centralized data policy.

Inside Source Address Translation

When service-side or LAN-side hosts send traffic to remote branches, the inside address translation services allow the source IP address (inside host) translation. This translation occurs before the data traffic is sent out to the overlay tunnels. The NAT inside pool and the inside static NAT addresses are redistributed to the overlay. These addresses are advertised to all the remote branches using the Overlay Management Protocol (OMP). Thus, the remote host is aware of the path to reach inside hosts.

For inside-address translation, the data traffic from service-side is matched with the centralized data policy match condition for dynamic NAT. If the source IP address satisfies the match condition, the data traverses the NAT configured on the service VPN before entering the remote edge router through the overlay. Address translation occurs on the tunnel egress interface. In releases before Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and earlier up to Cisco IOS XE Catalyst SD-WAN Release 17.3.1a, the static-inside NAT does not need a match condition in a centralized data policy. The static translation occurs if the source IP address matches the configured IP address for static NAT.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, you must map static NAT to a pool and static NAT is applied to the traffic if there is a data policy match.

Outside Source Address Translation

When the traffic from a remote site traverses through the overlay tunnels, the outside address translation service translates the remote host source IP address (outside host). The translation occurs before the traffic is sent to the LAN (VPN) side of the network. If route redistribution is configured, the NAT outside pool address or routes are redistributed to the LAN side of the network through Open Shortest Path First (OSPF) or other protocols. Thus, the inside host is aware of the path to reach remote hosts.

In releases before Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and earlier up to Cisco IOS XE Catalyst SD-WAN Release 17.3.1a, both inside and outside service-side NAT must be a dynamic NAT configuration. You can also configure 1:1 static NAT mapping for both inside and outside address translation.

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, you must configure a NAT pool action for static NAT as well, using a centralized data policy in order to operate for both source and destination directions.

Note Configure dynamic NAT before you configure static NAT.

Data Policy for Service-Side NAT

To enable NAT on the Cisco IOS XE Catalyst SD-WAN devices, configure a centralized data policy for static and dynamic NAT. A data policy provides the match criteria and NAT pool action for dynamic NAT.

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, you can create a data policy to configure match criteria and a NAT pool action for static NAT.

Benefits of Service-Side NAT

- Provides translation of source IPv4 addresses to destination IPv4 addresses
- Maps a public IPv4 address to a private source IPv4 address
- Provides a way for service providers to implement a seamless transition to IPv6

Traffic Flows for Service-Side NAT

The following are the two data traffic flows for service-side NAT:

- Source translation for traffic from service-side of the network destined to the remote edge through the overlay network
- Source translation for traffic destined to the service-side of the network from the remote edge through the overlay network

NAT Feature Invocation Array (FIA) from service-side—When the traffic is from the service-VPN that is destined to the remote edge through the tunnel, NAT FIA is enabled on the egress interface, which is the tunnel interface. The data policy direction is configured as from-service.

NAT FIA from-tunnel—When the traffic is from the remote edge that comes through the tunnel and reaches the service VPN, NAT FIA is enabled on the egress interface, which is the service VPN LAN interface. The data policy direction is configured as from-tunnel.

When the data policy direction is configured as all (all directions), NAT FIA is enabled on service VPN interfaces and tunnel interfaces.

Note The IP addresses of a centralized data policy and static NAT source IP address must not overlap in Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and earlier releases up to Cisco IOS XE Catalyst SD-WAN Release 17.3.1a. The centralized data policy must be clearly defined so that there are no overlapping traffic match conditions.

Restrictions for Service-Side NAT

- Only NAT pool translations are supported.
- Translations between different VRFs are not supported.
- In Cisco SD-WAN Manager, you can configure a maximum of 31 pools.

- Specify the NAT pool name as **natpool** *natpool-number*, where *natpool-number* must match the NAT pool value specified in the data policy.

  Example: `natpool10`

- In Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, Cisco IOS XE Catalyst SD-WAN Release 17.3.1a, and Cisco IOS XE Catalyst SD-WAN Release 17.3.2, a static NAT address must not be shared in pool addresses.
- Starting from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, the static NAT address may belong to the configured NAT pool address list, if it is used along with a data policy.
- A data policy and dynamic NAT pool must be defined for static NAT for a VRF.
- IPv4 translations for NAT64 are not supported.
- Each service VPN must have a unique NAT pool number.
- NAT entries cannot be edited after they are first created.

Configure Service-Side NAT

Workflow for Configuring Service-Side NAT

1. Configure a centralized data policy for the Cisco Catalyst SD-WAN Controller to include a NAT pool number and action. The direction of the centralized data policy for NAT inside must be **from-service**. The direction of the policy for NAT outside must be **from-tunnel**.
2. Configure a dynamic NAT pool number using a **Cisco VPN** template, which is a service-side VPN.
3. Configure dynamic NAT mappings using a **Cisco VPN** template.
4. (Optional) Configure a static NAT mapping using a **Cisco VPN** template.

   Starting from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, you can configure a NAT pool for static NAT and create a data policy to provide match criteria and a NAT pool action for static NAT.

   For more information on configuring service-side static NAT, see Configure Service-Side Static NAT.
5. For NAT inside, the NAT pool subnet and static NAT translation of IP addresses are automatically advertised into OMP. For NAT outside, you can manually configure redistribution of the NAT pool subnet and static NAT translation of IPv4 addresses to the service-side protocols.

Note If the data policy action is configured for VPN 0, the action is configured for DIA traffic. If the data policy action is configured for any of the service VPNs (example: VPN 1), which includes a NAT pool configuration, the action is for service-side NAT.

Create and Apply a Centralized Data Policy for Service-Side NAT

A centralized data policy is a policy that is configured on a Cisco Catalyst SD-WAN Controller and that affects data traffic being transmitted between the routers on the Cisco Catalyst SD-WAN overlay network.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Centralized Policy**.
3. Click **Add Policy**.

   The policy configuration wizard opens. For more information on creating a centralized data policy, see Configure Centralized Policies Using Cisco SD-WAN Manager.
4. Create policy lists.

   For more information on configuring groups of interest, see Configure Groups of Interest for Centralized Policy.
5. Configure traffic rules.

   For more information on configuring traffic rules, see Configure Traffic Rules.
6. Apply policies to sites and VPNs.

   For more information on applying policies to sites and VPNs, see Apply Policies to Sites and VPNs.

   Choose the direction for applying the policy as **All**, **From Tunnel**, or **From Service**.

   Table 15: Dynamic and Static NAT Application

NAT Configuration	Data-Policy Direction
Dynamic NAT Inside only (NAT Pool)	From-service
Dynamic NAT Outside only (NAT Pool)	From-tunnel
Dynamic NAT Inside (NAT Pool) + Static NAT Inside only	From-service
Dynamic NAT Inside (NAT Pool) + Static Port Forwarding only	From-service
Dynamic NAT Outside (NAT Pool) + Static NAT Outside only	From-tunnel
Two or more of above combinations	all

7. Activate the policy.

   For more information on activating a policy, see Activate a Centralized Data Policy.

Configure Service-Side Dynamic NAT

Before You Begin

1. Configure a centralized data policy for the Cisco Catalyst SD-WAN Controller to include a NAT pool number and an action.
2. Create a new **Cisco VPN** template or edit an existing **Cisco VPN** template. The **Cisco VPN** template corresponds to the service-side VPN you want to configure NAT for.

Configure a Dynamic NAT Pool

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

2. Click **Feature Templates**.



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

3. To edit a **Cisco VPN** template, click **…** adjacent to the template name and choose **Edit**.
4. Click **NAT**.
5. Under **NAT Pool**, click **New NAT Pool**.
6. Enter the required parameters and click **Update**.

Table 16: NAT Pool Parameters

Parameter Name	Description
NAT 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 (1–31) NAT pools per router.
NAT Pool Prefix Length	Enter the NAT pool prefix length.
NAT Pool Range Start	Enter a starting IP address for the NAT pool. **a.** Change the scope from **Default** to **Global** to enable the field. **b.** Enter the last IP address for the NAT pool.
NAT Pool Range End	Enter a closing IP address for the NAT pool. **a.** Change the scope from **Default** to **Global** to enable the field. **b.** Enter the last IP address for the NAT pool.
NAT Overload	Click **On** to enable per-port translation. Default is **On**. If **NAT Overload** is set to **Off**, only dynamic NAT is configured on the end device. Per-port NAT is not configured.
NAT Direction	Choose the NAT direction.

Configure Service-Side Static NAT

Before You Begin

1. Configure and apply a data policy.

2. Configure a **Cisco VPN** template or edit an existing **Cisco VPN** template.
3. Configure dynamic NAT.

Configure Service-Side Static NAT

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



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

3. To edit a **Cisco VPN** template, click **…** adjacent to the template name and choose **Edit**.
4. Click **NAT**.
5. Click **Static NAT**.
6. Under **Static NAT**, click **New Static NAT**.
7. Enter the required parameters and click **Update**.

Table 17: Static NAT Parameters

Parameter Name	Description
NAT Pool Name	Starting from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, you can use a NAT pool for static NAT as well. Choose the NAT pool number using the **Global** settings option.
Source IP Address	Enter the inside local address as the source IP address.
Translated Source IP Address	Enter the inside global address as the translated source IP address. Maps a public IP address to a private source address. In Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, if using a NAT pool for static NAT, static translated source IP addresses must be within the configured dynamic NAT pool IP address range.
Static NAT Direction	Select the direction in which to perform network address translation.
Inside	Select **Inside** to translate the IP address of packets that are coming from the service-side of the device and are destined for the transport side of the router.
Outside	Select **Outside** to translate the IP address of packets that are coming to the device from the transport-side device and are destined for a service-side device.

Note In Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and earlier releases up to Cisco IOS XE Catalyst SD-WAN Release 17.3.1a (when the service-side NAT feature was introduced), static NAT IP addresses must not overlap with NAT pool IP addresses.

In Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, static translated source IP addresses may be within the configured dynamic NAT pool IP address range.

Configure Service-Side Port Forwarding for NAT

You can configure port forwarding rules to allow requests from an external network to reach devices on the internal network.

Before You Begin

1. Configure and apply a data policy.
2. Configure a **Cisco VPN** template or edit an existing **Cisco VPN** template.
3. Configure a NAT pool.

Configure Service-Side Port Forwarding for NAT

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

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

3. To edit a **Cisco VPN** template, click **…** adjacent to the template name and choose **Edit**.
4. Click **NAT**.
5. Under **NAT Pool**, click **New NAT Pool**.
6. Enter the required NAT pool parameters.

   For more information on the NAT pool parameters, see Configure a NAT Pool and a Loopback Interface.
7. Click **Add**.
8. To create a port forwarding rule, click **Port Forward** > **Add New Port Forwarding Rule** and configure the required 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 18: Port-Forwarding Parameters

Parameter Name	Description
NAT Pool Name	Starting from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, you can use a NAT pool for static NAT. Choose the NAT pool number using the **Global** settings option.
Source Port	Enter a port number to define the source port to be translated.*Range:* 0 through 65535
Source IP Address	Enter the source IP address to be translated.
Translate Port	Enter the port number to apply port forwarding to. *Range:* 0 through 65535 In Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, static translated source IP addresses must be within the configured dynamic NAT pool IP address range.
Protocol	Choose the **TCP** or **UDP** protocol to which to apply the port-forwarding rule. To match the same ports for both TCP and UDP traffic, configure two rules.
Translated Source IP Address	Specify the NAT IP address that will be advertised into OMP. Port forwarding is applied to traffic that is destined to this IP address from the overlay with the translated port match.

9. Click **Update**.

Configure Service-Side NAT Using the CLI

Configure a Centralized Data Policy: Match Condition for Source to Any Destination

Configure a centralized data policy that includes a match condition for a source IP to any destination IP.

```
policy
 data-policy edge1
  vpn-list vpn_1
   sequence 101
    match
     source-ip 192.168.11.0/24
    !
    action accept
     count nat_vrf_1
     nat pool 1
    !
   !
   default-action accept
  !
  vpn-list vpn_2
   sequence 102
    match
     source-ip 192.168.22.0/24
    !
```

```
    action accept
     count nat_vrf_2
     nat pool 2
    !
   !
   default-action accept
  !
  vpn-list vpn_3
   sequence 103
    match
     source-ip 192.168.13.0/24
    !
    action accept
     count nat_vrf_3
     nat pool 3
    !
   !
   default-action accept
  !
 !
 lists
  vpn-list vpn_1
   vpn 1
  !
  vpn-list vpn_2
   vpn 2
  !
  vpn-list vpn_3
   vpn 3
  !
  site-list edge1
   site-id 500
  !
 !
!
```

Configure Inside Dynamic and Static NAT

Configure inside dynamic and static NAT for the NAT pools.

```
ip nat pool natpool1 10.11.11.1 10.11.11.2 prefix-length 24
ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1 match-in-vrf
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf overload
!
ip nat pool natpool2 10.22.22.1 10.22.22.2 prefix-length 24
ip nat outside source list global-list pool natpool2 vrf 2 overload match-in-vrf
ip nat outside source static 192.168.22.10 10.22.22.10 vrf 2 match-in-vrf
!
ip nat pool natpool3 10.13.13.1 10.13.13.2 prefix-length 24
ip nat inside source list global-list pool natpool3 vrf 3 match-in-vrf overload
ip nat inside source static tcp 192.168.13.10 80 10.13.13.10 8080 vrf 3 extendable
match-in-vrf
```

Configure Static NAT Using NAT Pool for Inside Static NAT (Starting Cisco IOS XE Catalyst SD-WAN Release 17.5.1a)

Configure static NAT inside for a NAT pool.

```
ip nat pool natpool1 10.11.11.1 10.11.11.30 prefix-length 24
ip nat pool natpool2 10.11.11.5 10.11.11.6 prefix-length 24
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf
ip nat inside source list global-list pool natpool2 vrf 1 match-in-vrf
ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1 match-in-vrf pool natpool1
```

Configure static NAT inside and static NAT outside for a NAT pool.

```
ip nat pool natpool1 10.11.11.1 10.11.11.30 prefix-length 24
ip nat pool natpool2 10.11.11.5 10.11.11.6 prefix-length 24
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf
ip nat inside source list global-list pool natpool2 vrf 1 match-in-vrf
ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1 match-in-vrf pool natpool1
ip nat outside source static 192.168.21.10 10.22.22.10 vrf 1 match-in-vrf pool natpool1
```

Use Case 1: Inside Static NAT Using an Inside NAT Pool

In this example, when only the static inside NAT is mapped to the NAT pool, sequence 101 specifies the data-policy configuration for static NAT traffic destined to the service-side of the network from the remote edge through the overlay network (in to out). Sequence 102 specifies the data-policy configuration for traffic from service-side of the network destined to the remote edge device for a destination global IP address of 10.11.11.10 (out to in).

```
policy
 data-policy edge1
  vpn-list vpn_1
   sequence 101
    match
     source-ip 192.168.11.0/24
     destination-ip 192.168.21.0/24
    !
    action accept
     count nat_vrf_1
     nat pool 1
    !
   !
   default-action accept
  !
 sequence 102
    match
     source-ip 192.168.21.0/24
     destination-ip 10.11.11.0/27
    !
    action accept
     count nat_vrf_2
     nat pool 2
    !
   !
   default-action accept
  !
   default-action accept
  !
 !
```

Use Case 2: Static Inside NAT and Static Outside NAT Mapped to Inside NAT Address Pool

In this example, when the static inside NAT and static outside NAT are mapped to the NAT pool, sequence 101 specifies the data-policy configuration for static NAT traffic destined to the service-side of the network from the remote edge devices through the overlay network (in to out). Sequence 102 specifies the data-policy configuration for traffic from service-side of the network destined to the remote edge device for a destination global IP address of 10.11.11.10 (out to in).

```
policy
data-policy vedge1
  vpn-list vpn_1
   sequence 101
    match
     source-ip 192.168.11.0/24
```

```
     destination-ip 10.22.22.10/27
    !
    action accept
     count nat_vrf_1
     nat pool 1
    !
   !
   sequence 102
    match
     source-ip 192.168.21.0/24
     destination-ip 10.11.11.0/27
    action accept
     nat pool 1
  default-action accept
 !
```

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.3.1a, the **ip nat settings central-policy** command is required for NAT on Cisco IOS XE Catalyst SD-WAN devices to work in Cisco Catalyst SD-WAN mode. If you use a Cisco SD-WAN Manager feature template to enable NAT on the device, Cisco SD-WAN Manager automatically pushes this command to the device. However, if you are using a device CLI template only to configure NAT on the device, you need to add the **ip nat settings central-policy** command to the device CLI template configuration.

Verify Configuration of Service-Side NAT

Example for VRF 1

Traffic from 192.168.11.10 gets translated based on the static NAT rule. Traffic from any other source in 192.168.11.0/24 gets translated to a pool IP.

```
Device# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
tcp  10.13.13.10:8080      192.168.13.10:80      ---                   ---
---  ---                   ---                   10.22.22.10           192.168.22.10

---  10.11.11.10           192.168.11.10         ---                   ---
icmp 10.11.11.1:18193      192.168.11.2:18193    192.168.21.2:18193    192.168.21.2:18193
tcp  10.11.11.10:59888     192.168.11.10:59888   192.168.21.10:21      192.168.21.10:21
tcp  10.11.11.10:50069     192.168.11.10:50069   192.168.21.10:35890   192.168.21.10:35890
tcp  10.11.11.10:39164     192.168.11.10:39164   192.168.21.10:80      192.168.21.10:80
Total number of translations: 7
```

Example for VRF 2

Traffic from 192.168.22.10 gets translated to 10.22.22.10 based on the static NAT rule. Traffic from any other source 192.168.22.0/24 gets translated to a pool IP.

```
Device# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
tcp  10.13.13.10:8080      192.168.13.10:80      ---                   ---
---  ---                   ---                   10.22.22.10           192.168.22.10

---  10.11.11.10           192.168.11.10         ---                   ---
tcp  192.168.12.10:21      192.168.12.10:21      10.22.22.10:56602     192.168.22.10:56602
tcp  192.168.12.10:46238   192.168.12.10:46238   10.22.22.10:49532     192.168.22.10:49532
icmp 10.22.22.1:18328      192.168.22.2:18328    192.168.12.2:18328    192.168.12.2:18328
```

```
tcp  192.168.12.10:80      192.168.12.10:80      10.22.22.10:46340     192.168.22.10:46340
Total number of translations: 7
```

Example for VRF 3

Any traffic to 10.13.13.10:8080 gets translated to 192.168.13.10:80. Any other traffic from 192.168.11.0/24 gets translated to a pool IP.

```
Device# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
tcp  10.13.13.10:8080      192.168.13.10:80      ---                   ---
---  ---                   ---                   10.22.22.10           192.168.22.10

---  10.11.11.10           192.168.11.10         ---                   ---
tcp  10.13.13.1:43162      192.168.13.10:43162   192.168.23.10:21      192.168.23.10:21
tcp  10.13.13.1:41753      192.168.13.10:41753   192.168.23.10:34754   192.168.23.10:34754
icmp 10.13.13.1:19217      192.168.13.2:19217    192.168.23.2:19217    192.168.23.2:19217
tcp  10.13.13.10:8080      192.168.13.10:80      192.168.23.10:40298   192.168.23.10:40298
tcp  10.13.13.1:43857      192.168.13.10:43857   192.168.23.10:80      192.168.23.10:80
Total number of translations: 8
```

Verify Service-Side NAT when a NAT Pool is Used for Static NAT (From Cisco IOS XE Catalyst SD-WAN Release 17.5.1a)

The following sample output shows UDP traffic from client 1 (192.168.11.10) to server 2 (192.168.21.11):

```
Device# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
---  10.11.11.2            192.168.11.10         ---                   ---
---  10.11.11.5            192.168.11.10         ---                   ---
udp  10.11.11.5:5001       192.168.11.10:5001    192.168.21.11:5001    192.168.21.11:5001
----> NAT IP from Pool 2
Total number of translations: 3
```

The following sample output shows UDP traffic from client 1 (192.168.11.10) to server 1 (192.168.21.10):

```
Device# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
---  10.11.11.2            192.168.11.10         ---                   ---
---  10.11.11.5            192.168.11.10         ---                   ---
udp  10.11.11.5:5001       192.168.11.10:5001    192.168.21.11:5001    192.168.21.11:5001
----> NAT IP from Pool 2
udp  10.11.11.2:5001       192.168.11.10:5001    192.168.21.10:5001    192.168.21.10:5001
----> NAT IP as per static NAT rule mapped to Pool 1
Total number of translations: 4
```

The following sample output shows UDP traffic from client 2 (192.168.11.11) to server 2 (192.168.21.11):

```
Device# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
---  10.11.11.2            192.168.11.10         ---                   ---
---  10.11.11.6            192.168.11.11         ---                   ---
---  10.11.11.5            192.168.11.10         ---                   ---
udp  10.11.11.5:5001       192.168.11.10:5001    192.168.21.11:5001    192.168.21.11:5001
----> NAT IP from pool 2
udp  10.11.11.6:5001       192.168.11.11:5001    192.168.21.11:5001    192.168.21.11:5001
----> NAT IP from pool 2
udp  10.11.11.2:5001       192.168.11.10:5001    192.168.21.10:5001    192.168.21.10:5001
----> NAT IP as per static NAT rule mapped to Pool 1
Total number of translations: 6
```

Configuration Examples for Service-Side NAT

Example: NAT Configuration on a Cisco VPN Interface Ethernet Template

```
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet1 overload
  ip nat translation tcp-timeout 3600
  ip nat translation udp-timeout 60
  ip nat route vrf 1 10.0.0.1 10.0.0.1 global

interface GigabitEthernet1
   no shutdown
   arp timeout 1200
   ip address 10.1.15.15 255.255.255.0
   ip redirects
   ip mtu    1500
   ip nat outside
```

Example: Configuration of Dynamic NAT

```
ip nat pool natpool-gigabitethernet1-0 198.51.100.1 198.51.100.2 prefix-length 24
ip nat inside source list global-list pool natpool-gigabitethernet1-0 egress-interface
GigabitEthernet1
```

Example: Configuration of Interface Overload

```
ip nat pool natpool-gigabitethernet1-0 209.165.201.1 209.165.201.2 prefix-length 24
ip nat inside source list global-list pool natpool-gigabitethernet1-0 overload
egress-interface GigabitEthernet1
```

Example: Configuration of Interface Overload with a Loopback Interface

```
ip nat inside source list global-list interface loopback1 overload egress-interface
GigabitEthernet1
```

Intra-VPN Service-Side NAT

The following sections provide information about configuring intra-VPN service-side NAT.

Information About Intra-VPN Service-Side NAT

Intra-VPN service-side NAT is an extension to service-side NAT, which allows a service-side LAN interface to communicate with another service-side LAN interface within the same VPN. Intra-VPN service-side NAT uses static or dynamic NAT so that data traffic can be initiated in either direction. You can apply static or dynamic NAT rules for packets to be routed from other LAN interfaces to the interface configured as the outside interface using the **ip nat outside** command.

You configure intra-VPN service-side NAT using a device CLI template or a CLI add-on template.

You can configure port forwarding for intra-VPN service-side NAT.

For more information on configuring port forwarding for intra-VPN service-side NAT, see Configure Service-Side Port Forwarding for NAT.

Benefits of Intra-VPN Service-Side NAT

- Supports LAN-to-LAN traffic in the same VPN
- Supports static or dynamic NAT for a mapping between real and mapped IP addresses
- Supports bidirectional traffic between two LAN interfaces within the same VPN

Restrictions for Intra-VPN Service-Side NAT

- NAT for a service-side LAN interface to a remote branch is not supported.
- Direct Internet Access (DIA) is not supported for packets from a service-side LAN interface.
- A service-to-service-side LAN interface must be in the same VPN.

  NAT is not supported across different VPNs.
- Firewall, AppNav-XE, and multicast are not supported.
- Configure intra-VPN service-side NAT using a device CLI template or a CLI add-on template. Cisco SD-WAN Manager feature template support is not available for Cisco IOS XE Catalyst SD-WAN Release 17.7.1a.

Note If you use a Cisco SD-WAN Manager feature template for other NAT-related features, **ip nat outside** configuration is removed from the interface. Consequently, intra-VPN service-side NAT functionality is not available.

- Configure the data policy direction as **All** (all directions).
- Only LAN-side physical interfaces and Ethernet sub interfaces are supported. Loopback and Bridge Domain Interface (BDI) interfaces are not supported.
- NAT DIA with port forwarding is not supported.

Configure Intra-VPN Service-Side NAT

Workflow for Configuring Intra-VPN Service-Side NAT

1. Configure a centralized data policy for the Cisco Catalyst SD-WAN Controller for static or dynamic NAT mapping.

   For more information on configuring a centralized data policy, see Create and Apply a Centralized Data Policy for NAT.
2. Configure static or dynamic NAT using a **Cisco VPN** template.
3. (Optional) Configure a pool name for static or dynamic NAT mapping.

   For more information on configuring a pool name for static or dynamic NAT mapping, see Configure Service-Side Static NAT.

4. Use a device CLI template or a CLI add-on template to configure an outside interface for NAT translation and apply the configurations to the device.
5. Attach the device CLI template or the CLI add-on template to the device.

Configure Intra-VPN Service-Side NAT Using a CLI Add-On Template

Before You Begin

Create a new CLI add-on template or edit an existing CLI add-on template.

For more information on CLI add-on feature templates, see CLI Add-On Feature Templates.

Configure Intra-VPN Service-Side NAT Using a CLI Add-On Template

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

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

3. Click **Add Template**.
4. Choose a device from the device list.
5. Click **CLI Add-On Template** under **OTHER TEMPLATES**.
6. In **CLI Add-On Template** area, enter the configuration.
7. Configure an outside interface using the **ip nat outside** command.
8. Click **Save**.

   The CLI add-on template that you created is displayed in the **CLI Configuration** table.
9. Attach the CLI add-on template to your device.

Configuration Examples for Intra-VPN Service-Side NAT

Example: Policy Configuration

The following is a sample configuration of a centralized data policy for the Cisco Catalyst SD-WAN Controller that includes a NAT pool:

```
Device# show running policy
policy
data-policy cedge1
vpn-list vpn_1
sequence 101
match
source-ip 192.168.11.0/24
!
action accept
```

```
count nat_vrf_1
nat pool 1
!
!
default-action accept
!
!
lists
vpn-list vpn_1
vpn 1
!
site-list cedge1
site-id 500
.
.
.
```

Example: LAN Interface 1 Configured with IP NAT Outside

The following example shows that an **ip nat outside** interface has been configured on the GigabitEthernet 5.102 interface.

```
Device# interface GigabitEthernet5.102
encapsulation dot1Q 102
vrf forwarding 1
ip address 192.168.12.1 255.255.255.0
ip mtu 1496
ip nat outside
ip ospf dead-interval 40
ip ospf 1 area 0
pool configuration:
ip nat pool natpool1 10.11.11.1 10.11.11.2 prefix-length 24
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf overload

static nat inside config:
ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1 match-in-vr
end
```

Example: LAN Interface 2

The following example shows that the GigabitEthernet 5.101 interface has been configured on the same VPN and VRF.

```
Device# interface GigabitEthernet5.101
encapsulation dot1Q 101
vrf forwarding 1
ip address 192.168.11.1 255.255.255.0
ip mtu 1496
ip ospf dead-interval 40
ip ospf 1 area 0
pool configuration:
ip nat pool natpool1 10.11.11.1 10.11.11.2 prefix-length 24
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf overload

static nat inside config:
ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1 match-in-vr
end
```

Service-Side Conditional Static NAT

The following sections provide information about configuring service-side conditional static NAT.

Information About Service-Side Conditional Static NAT

Configure service-side conditional static NAT to translate the same source IP address to different global IP addresses based on the destination IP addresses.

Service-side conditional static NAT allows you to configure the same source IP address within another configured static NAT pool IP address range. Prior to Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, this functionality was not supported.

Configure service-side conditional static NAT using a device CLI.

Benefits of Service-Side Conditional Static NAT

- Translates the same source IP address to different IP addresses based on the destination IP addresses in a data policy.
- Allows you to use the same source IP address within another configured static NAT pool IP address range.

Restrictions for Service-Side Conditional Static NAT

- Service-side conditional static NAT is for inside static NAT and service-side traffic only.
- Outside static NAT is not supported.
- DIA traffic is not supported.

Workflow for Configuring Service-Side Conditional Static NAT

1. Configure a centralized data policy and configure the sequences with different destination IP addresses.

   For more information, see Create and Apply a Centralized Data Policy for Service-Side NAT.

2. Configure at least two NAT pools with the same local IP address.

   For more information on configuring service-side conditional static NAT using the CLI, see Configure Service-Side Conditional Static NAT Using the CLI.

3. Verify the translations for the destination IP addresses.

   For more information on verifying the translations for the destination IP addresses, see Verify Conditional Static NAT Using the CLI.

Configure Service-Side Conditional Static NAT Using the CLI

1. Configure a centralized data policy and configure the sequences:

```
data-policy EDGE1
vpn-list vpn_1
sequence 101
match
source-ip 192.168.11.10/32
destination-ip 192.168.21.10/32
!
action accept
count vrf1_In2Out1
nat pool 1
!
!
sequence 102
match
source-ip 192.168.11.10/32
destination-ip 192.168.21.2/32
!
action accept
count vrf1_In2Out2
nat pool 2
!
!
default-action accept
!
!
lists
vpn-list vpn_1
vpn 1
!
site-list EDGE1
site-id 500
!
!
!
```

2. Configure at least two NAT pools:

```
Device(config)# ip nat pool natpool1 10.11.11.1 10.11.11.10 prefix-length 24
Device(config)# ip nat pool natpool2 10.22.22.1 10.22.22.10 prefix-length 24
```

3. Configure inside static NAT using the same source IP address for the corresponding NAT pools:

```
Device(config)# ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1 match-in-vrf
 pool natpool1
Device(config)# ip nat inside source static 192.168.11.10 10.22.22.10 vrf 1 match-in-vrf
 pool natpool2
Device(config)# ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf
overload
Device(config)# ip nat inside source list global-list pool natpool2 vrf 1 match-in-vrf
overload
```

Verify Service-Side Conditional Static NAT Configuration

Sample Source IP Translations for NAT Pool 1 and NAT Pool 2

For natpool1, the Cisco IOS XE Catalyst SD-WAN device translates the source IP address `192.168.11.10` to `10.11.11.10`, which is destined for `192.168.21.10`.

```
Device# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
---  10.11.11.10           192.168.11.10         ---                   ---
---  10.22.22.10           192.168.11.10         ---                   ---
```

```
icmp 10.22.22.10:8371      192.168.11.10:8371    192.168.21.2:8371    192.168.21.2:8371
icmp 10.11.11.10:8368      192.168.11.10:8368    192.168.21.10:8368   192.168.21.10:8368
Total number of translations: 4
```

For natpool2, the Cisco IOS XE Catalyst SD-WAN device translates the source IP address `192.168.11.10` to `10.22.22.10`, which is destined for `192.168.21.2`.

Service-Side Static Network NAT

The following sections provide information about configuring service-side static network NAT.

Information About Service-Side Static Network NAT

You can configure service-side static NAT for an entire network using one configuration.

You can configure service-side static network NAT using Cisco SD-WAN Manager or a device CLI template.

Benefits of Service-Side Static Network NAT

- Supports configuration of a single static NAT pool for configuring an entire subnet.
- Supports the object tracker functionality for LAN prefixes and LAN interfaces.

Restrictions for Service-Side Static Network NAT

- Configuration of service-side static network CLI using a centralized data policy is not supported. But needs a data policy for the CLI to work.
- Overlapping of NAT pool addresses is not supported.
- Only inside service-side network NAT is supported.
- Outside static network NAT is not supported.
- DIA configuration is not supported.

Configure Service-Side Static Network NAT

Before You Begin

- Configure and apply a data policy.

  For more information on creating and applying a centralized data policy for service-side NAT, see Create and Apply a Centralized Data Policy for Service-Side NAT.

- Configure a **Cisco VPN** template or edit an existing **Cisco VPN** template.
- Configure service-side static NAT.

Note You need to configure a NAT pool prior to configuring service-side static network NAT.

For more information on configuring service-side static NAT and a NAT pool, see Configure Service-Side Static NAT.

Configure Service-Side Static Network NAT

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. To edit a **Cisco VPN** template, click **…** adjacent to the template name and choose **Edit**.
4. Click **NAT**.
5. Click **Static NAT**.
6. Under **Static NAT**, click **New Static NAT Subnet**.
7. Enter the required parameters.

Table 19: New Static NAT Subnet Parameters

Parameter Name	Description
Source IP Subnet	Enter the inside local address as the source IP subnet address.
Translated Source IP Subnet	Enter the outside global subnet address as the translated source IP subnet address. Maps a public IP address to a private source address.
Network Prefix Length	Enter the network prefix length.
Static NAT Direction	Select the direction for the network address translation. Choose **Inside** as the direction for performing network address translation.
Add Object /Group Tracker	(Optional) Enter the object ID number if you want to track an object. The object tracker functionality is supported for service-side static network NAT.

8. Click **Update**.

Configure Service-Side Static Network NAT Using the CLI

1. Configure service-side static network NAT using the following command:

```
Device(config)# ip nat inside source static network 192.168.11.0 192.168.70.0 /24 vrf 1
match-in-vrf
```

2. (Optional) Configure a service-side NAT object tracker.

For more information, see Configure Service-Side NAT Object Tracker.

Verify Service-Side Static Network NAT Configuration

The following sections provide information on how to verify service-side static network NAT configuration.

Verify Translations for Service-Side Static Network NAT

The following is a sample output from the **show ip nat translations** command:

```
Device# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
---  192.168.70.0          192.168.11.0          ---                   ---
---  192.168.70.11         192.168.11.11         ---                   ---
---  192.168.70.10         192.168.11.10         ---                   ---
icmp 192.168.70.11:16528   192.168.11.11:16528   192.168.21.11:16528   192.168.21.11:16528
icmp 192.168.70.10:16525   192.168.11.10:16525   192.168.21.10:16525   192.168.21.10:16525
icmp 192.168.70.10:16526   192.168.11.10:16526   192.168.21.10:16526   192.168.21.10:16526
icmp 192.168.70.10:16527   192.168.11.10:16527   192.168.21.10:16527   192.168.21.10:16527
```

Verify Service-Side Static Network NAT Route Creation

The following is a sample output from the **show ip route vrf** command:

```
Device# show ip route vrf 1
Routing Table: 1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
n Nd     10.0.1.0/24 [6/0], 2d00h, Null0
C        10.0.100.0/24 is directly connected, GigabitEthernet8
L        10.0.100.15/32 is directly connected, GigabitEthernet8
C        10.20.24.0/24 is directly connected, GigabitEthernet5
L        10.20.24.15/32 is directly connected, GigabitEthernet5
n Ni  192.168.70.0/24 [7/0], 00:00:12, Null0
```

Application-Level Gateways with Service-Side NAT

The following sections provide information about configuring application-level gateways (ALGs) with Service-Side NAT.

Information About Using ALGs with Service-Side NAT

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, Cisco Catalyst SD-WAN Manager Release 20.15.1

An application-level gateway (ALG), also known as an application-layer gateway, is an application that translates the IP address inside the payload of an application packet. Use an ALG to interpret the application-layer protocol and perform firewall and NAT translations.

Specific protocols that embed the IP address information within the packet payload require the support of an ALG. The following protocol requires an ALG for NAT translations of the application payload:

- File Transfer Protocol (FTP)

For more information about ALGs, see the *IP Addressing: NAT Configuration Guide*.

Benefits of Using ALGs with Service-Side NAT

- Allows client applications to use dynamic TCP or UDP ports to communicate with the server application.

Restrictions for Using ALGs with Service-Side NAT

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, Cisco Catalyst SD-WAN Manager Release 20.15.1

- Outside NAT:
  - You cannot configure ALGs with Service-Side NAT using the **ip nat outside source** command.

Configure ALGs with Service-Side NAT Using a CLI Template

For more information on using CLI templates, see CLI Templates and CLI Add-On Feature Templates.

Note By default, CLI templates execute commands in global config mode.

This section provides example CLI configurations to configure ALGs with service-side NAT:

1. Configure service-side NAT.

   For more information, see Configure Service-Side NAT.

2. Enable NAT ALG global support.

   ```
   ip nat service all-algs
   ```

3. Enable NAT ALG for FTP as shown in the following example:

   ```
   ip nat service ftp
   ```

4. Configure NAT pool on the router

```
ip nat pool pool-name pool-range prefix/length
ip nat inside  source list global-list pool pool-name vrf number match-in-vrf
overload
```

Here's the complete configuration example for configuring ALGs.

Configure a centralized data policy that includes a match condition for a source IP to any destination IP

```
policy
 data-policy vedge1
  vpn-list vpn_1
   sequence 101
    match
     destination-ip 203.0.113.21/32
    !
    action accept
     count nat_vrf_1
     nat pool 1
    !
   sequence 102
    match
     source-ip 198.51.100.150/32
    !
    action accept
     count nat_vrf_1
     nat pool 1
   !
   default-action accept
  !
 !
 lists
  vpn-list vpn_1
   vpn 1
  !
  site-list vedge1
   site-id 500
  !
 !
!
apply-policy
 site-list vedge1
  data-policy vedge1 all
```

Enable NAT ALG global support

```
ip nat service all-algs
```

Enable NAT ALG for FTP

```
ip nat service ftp
```

Configure NAT pool on the router

```
ip nat pool natpool1 203.0.113.21 203.0.113.21 prefix-length 24
ip nat inside source static 192.0.2.150 203.0.113.99 vrf 1 match-in-vrf pool natpool1
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf overload
```

Verify ALG Configuration

The following sections provide information about verifying configuration of ALG with service-side NAT.

Display NAT Translations

```
show ip nat translations tcp
tcp  203.0.113.21:37713     192.0.2.150:37713    198.51.100.150:21       198.51.100.150:21
tcp  203.0.113.21:40586     192.0.2.150:40586    198.51.100.150:38366    198.51.100.150:38366
```

Note You cannot view the translation of the payload using a CLI template. To view the translation of a payload, capture a packet using Cisco SD-WAN Manager.

For more information on capturing packets using Cisco SD-WAN Manager, see Capture Packets in the *Cisco Catalyst SD-WAN Monitor and Maintain Guide*.

Display ALG Translations

```
Device(config)# show platform hardware qfp active feature nat datapath sess-dump

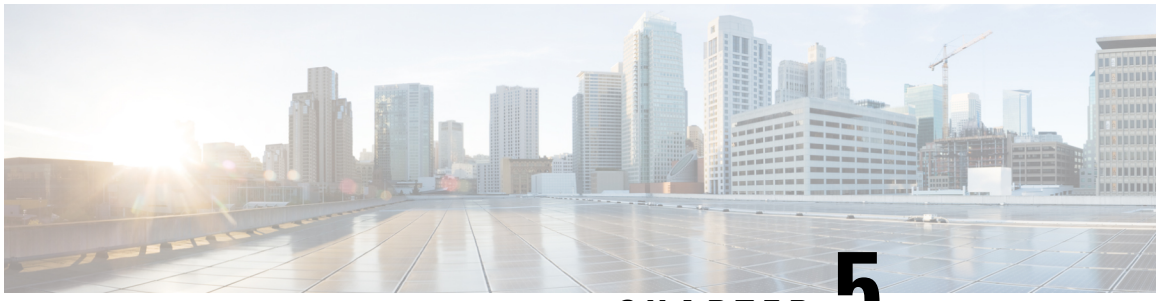
id 0xeec305c0 io 192.0.2.150 oo 198.51.100.150 io 51967 oo 27734 it 203.0.113.21 ot
198.51.100.150 it 51967 ot 27734 pro 6 vrf 5 tableid 5 bck 8490 in_if 0 out_if 0 ref 1 flags
 0xc0204014 ext_flags 0x0 in_pkts 783 in_bytes 1073640 out_pkts 435 out_bytes 13928 flowdb
 in2out fh 0x0 flowdb out2in fh 0x0 rg 0
id 0xeec30470 io 192.0.2.150 oo 198.51.100.150 io 37715 oo 21 it 203.0.113.21 ot
198.51.100.150 it 37715 ot 21 pro 6 vrf 5 tableid 5 bck 12489 in_if 0 out_if 0 ref 1 flags
 0xc0204014 ext_flags 0x0 in_pkts 15 in_bytes 597 out_pkts 16 out_bytes 788 flowdb in2out
fh 0x0 flowdb out2in fh 0x0 rg 0
```

Display NAT Statistics

```
Device(config)# show platform hardware qfp active feature nat datapath stats

Counter                                                          Value
------------------------------------------------------------------------
number_of_session                                                    2
udp                                                                  0
tcp                                                                  2
icmp                                                                 0
non_extended                                                         1
statics                                                              1
static_net                                                           0
entry_timeouts                                                       0
hits                                                                 0
misses                                                               0
cgn_dest_log_timeouts                                                0
ipv4_nat_alg_bind_pkts                                               5
ipv4_nat_alg_sd_not_found                                            0
ipv4_nat_alg_sd_tail_not_found                                       0
ipv4_nat_rx_pkt                                                  21686
ipv4_nat_tx_pkt                                                  21892
ipv4_nat_flowdb_hits                                                 0
ipv4_nat_stick_rx_pkts                                               0
ipv4_nat_stick_i2o_pkts                                              0
ipv4_nat_stick_o2i_pkts                                              0
ipv4_nat_stick_forus_hits_pkts                                       0
ipv4_nat_stick_hit_sb                                                0
```

```
ipv4_nat_stick_ha_divert_pkts                                0
ipv4_nat_stick_ha_ar_pkts                                    0
ipv4_nat_stick_ha_tcp_fin                                    0
ipv4_nat_stick_ha_failed_pkts                                0
ipv4_nat_non_natted_in2out_pkts                           2762
ipv4_nat_non_nated_out2in_pkts                           18955
ipv4_nat_bypass_pkts                                         0
ipv4_nat_unmarked_pkts                                   16330
ipv4_nat_res_port_in2out_pkts                                0
ipv4_nat_res_port_out2in_pkts                                0
ipv4_nat_ipc_retry_fail                                      0
ipv4_nat_cfg_rcvd                                            9
ipv4_nat_cfg_rsp                                            13
```



CHAPTER 5

Service-side NAT Object Tracker

- Feature history of service-side NAT object tracker, on page 113
- Service-side NAT object tracker, on page 113
- Restrictions for service-side NAT object tracker, on page 114
- Use case for service-side NAT object tracker, on page 114
- How to configure the service-side NAT with an object tracker, on page 114
- Verify the service-side NAT object tracker configuration, on page 119
- Monitor service-side NAT object tracker, on page 120

Feature history of service-side NAT object tracker

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

Table 20: Feature history

Feature name	Release information	Description
Service-Side NAT Object Tracker Support	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	This feature supports tracking LAN prefixes and LAN interfaces for service-side inside static NAT. When an associated object tracker changes state (up or down), the device adds or removes the corresponding NAT route from the routing table through OMP. View event notifications in Cisco SD-WAN Manager to monitor NAT route and interface changes.

Service-side NAT object tracker

A service-side NAT object tracker is a tracking mechanism that

- monitors LAN prefixes and LAN interfaces to control NAT route advertisements through OMP based on their operational state

- detects changes in tracked object states and communicates them to interested client processes immediately or after a configured delay, and
- adds or removes corresponding NAT route advertisements through OMP based on the tracked object states.

NAT route tracking and advertisement management

- Each tracked object has a unique number that client processes use to identify and track it.
- The tracking process periodically polls tracked objects to detect changes in their states.
- If a tracked prefix is missing from the routing table, the tracker removes the corresponding NAT prefix route from OMP.
- You can configure the tracker through Cisco SD-WAN Manager, device CLI, or a CLI add-on template.
- The **track** keyword is available in the **ip nat inside source**command.
- You can monitor NAT route advertisement changes through event logs in Cisco SD-WAN Manager.

Restrictions for service-side NAT object tracker

Observe these restrictions when you use the service-side NAT object tracker.

- Object tracking for service-side static NAT supports only inside static NAT and inside dynamic NAT.
- Outside static NAT and NAT DIA are not supported.
- Outside translations and port forwarding are not supported.
- Cisco SD-WAN Manager does not support IP route tracking.

  Use a device CLI template or CLI add-on template to configure IP route tracking. You can track an interface as an object using Cisco SD-WAN Manager.

Use case for service-side NAT object tracker

When a LAN interface or LAN prefix goes down, the service-side NAT object tracker automatically transitions to a down state. Cisco SD-WAN Manager event logs show when NAT route advertisements are added or removed, allowing you to monitor route advertisement changes.

How to configure the service-side NAT with an object tracker

Summary

This workflow outlines ordered steps to set up service-side NAT: configure a centralized data policy, create the tracker, configure dynamic or static NAT, define a static NAT pool, and associate the tracker with the inside static NAT pool.

Workflow

1. Configure a centralized data policy for the Cisco Catalyst SD-WAN Controller to include a NAT pool number and an action.

   For more information on configuring and applying a centralized data policy for the service-side NAT object tracker, see Create and Apply a Centralized Data Policy for Service-Side NAT.

2. Configure a service-side NAT object tracker or a tracker group using a Cisco System template.

   For more information on configuring a service-side NAT object tracker, see Configure Service-Side NAT Object Tracker.

3. (Optional) Configure service-side dynamic NAT.

   For more information on configuring service-side dynamic NAT, see Configure Service-Side Dynamic NAT.

4. Configure a NAT pool for service-side static NAT.

   For more information on configuring a NAT pool for service-side static NAT, see Configure Service-Side Static NAT.

5. Associate the service-side NAT object tracker with the static inside NAT pool using a Cisco VPN template.

   For more information on associating the service-side NAT object tracker with the static inside NAT pool using a Cisco VPN template, see Associate the Service-Side NAT Object Tracker with a NAT Pool Using a Cisco VPN Template.

Configure service-side NAT object tracker using templates

Procedure

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

Step 2 Select **Feature Templates**.

Step 3 To edit a **Cisco System** template, select **…** adjacent to the template name and choose **Edit**.

Step 4 Select **Tracker** and choose **New Object Tracker** to configure the service-side NAT object tracker parameters.

Table 21: Service-side NAT object tracker parameters

Field	Description
Tracker Type	Choose **Interface** or **Route** to track a LAN interface or LAN prefix.
Object ID	Enter the object ID number. The object number identifies the tracked object and can be from 1 to 1000.
Interface	Choose a global or device-specific interface.

Step 5 Click **Add**.

Step 6 Click **Update**.

Step 7 (Optional) To create a tracker group, choose **Tracker**, and click **Tracker Groups** > **New Object Tracker Groups** to configure the service-side NAT object tracker.

Note Ensure that you have created two trackers to create a tracker group.

Table 22: Service-side NAT 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**. • **AND**: Reports the transport interface as active only when both associated trackers report the route as active. • **OR** Reports the transport interface as active when either associated tracker reports the route as active.

Step 8 Select **Add** and then **Update** .

Configure service-side NAT object tracker using CLI commands

Use this task to configure a service-side NAT object tracking to control NAT translation behavior using centralized data policy and tracked conditions such as route reachability or interface state.

Procedure

Step 1 Configure a centralized data policy on the Cisco Catalyst SD-WAN Controller with a NAT pool number and an action, as shown in the following example.

Example:

```
policy
 data-policy ssn_policy
  vpn-list ssn_vpn_list
   sequence 10
    match
     destination-ip 192.168.21.0/24
!
    action accept
     count counter_dst_192
     nat pool 1
    !
   !
   sequence 20
```

```
    match
     destination-ip 10.11.11.0/27
   !
    action accept
     count counter_dst_10
     nat pool 2
    !
   !
   sequence 101
    match
     source-ip 192.168.11.0/24
     protocol  1
    !
    action accept
     nat pool 1
    !
   !
   default-action accept
  !
 !
 lists
  vpn-list ssn_vpn_list
   vpn 1
  !
  site-list ssn_site_list
   site-id 500
  !
 !
!
apply-policy
 site-list ssn_site_list
  data-policy ssn_policy all
 !
!
```

Step 2 Configure an inside static NAT mapping and associate it with a tracker.

Example:

```
Device(config)# ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1
match-in-vrf track 1
```

Step 3 Configure an inside static NAT pool with a prefix length:

Example:

```
Device(config)# ip nat pool natpool2 10.11.11.0 10.11.11.25 prefix-length 27
```

Step 4 Configure an inside static NAT global pool with overload mode and a tracker ID:

Example:

```
Device(config)# ip nat inside source list global-list pool natpool2 vrf 1 match-in-vrf overload track
 1
```

Step 5 Track IP route reachability:

Example:

```
Device(config)# track 1 ip route 192.168.11.0 255.255.255.0 reachability

Device(config-track)# ip vrf 1
```

Note The tracker considers the object up when the routing table contains the specified route and the route is accessible.

Step 6 Track the line-protocol state of an interface:

Example:

```
Device(confige)# track 1 interface GigabitEthernet5.101 line-protocol
```

Configure service-side NAT object tracker using a CLI add-on template

Before you begin

Create a new CLI add-on template or edit an existing CLI add-on template.

Follow these steps to configure a service-side NAT object tracker with a CLI add-on template:

Procedure

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

Step 2 Select **Feature Templates**.

Step 3 Select **Add Template**.

Step 4 Choose a device from the device list.

Step 5 Select **CLI Add-On Template** under **Other templates**.

Step 6 In the CLI Add-On Template pane, enter the configuration as shown in this example:

Example:

```
track 1 ip route 192.168.11.0 255.255.255.0 reachability
ip vrf 1
ip nat pool natpool1 10.11.11.1 10.11.11.30 prefix-length 24
ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1 match-in-vrf pool natpool1 track 1
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf overload track 1
```

Step 7 Select **Save**.

The CLI add-on template that you created is displayed in the CLI Configuration table.

Step 8 Attach the CLI add-on template to your device.

Associate the service-side NAT object tracker with a NAT pool using a Cisco VPN template

Use this task to associate a service-side NAT object tracker with a NAT pool by editing a Cisco VPN template in Cisco SD-WAN Manager to support tracking-based NAT behavior.

Procedure

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

Step 2 Select **Feature Templates**.

Step 3 To edit a Cisco VPN template, select **…** adjacent to the template name and choose **Edit**.

Step 4 Configure a NAT pool for dynamic or static NAT.

Step 5 In NAT Direction, change the scope from Default to Global, then select **Inside**.

Step 6 In Add Object/Object Group Tracker, enter the object ID of the interface or route to track.

Step 7 Select **Add** and then select **Update**.

Verify the service-side NAT object tracker configuration

Verify the service-side NAT object tracker configuration by checking tracker state and validating that NAT routes through OMP are present in the routing table.

Verify the service-side NAT object tracker state

To verify the service-side NAT object tracker state, use the **show track object-id** command.

```
Device# show track 1
 Track 1
  Interface GigabitEthernet5.101 line-protocol
  Line protocol is Up
    1 change, last change 01:38:57
  Tracked by:
    NAT 0
```

In this output, `Line protocol is Up (OMP)`, indicates that the service-side object tracker is up.

Verify NAT routes in the routing table

To verify that OMP advertises NAT routes and adds them to the routing table, use the **show ip route vrf** command.

```
Device# show ip route vrf 1
Routing Table: 1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected
Gateway of last resort is not set
      10.0.0.0/24 is subnetted, 3 subnets
m        10.11.11.1 [251/0] via 192.168.11.10, 04:03:35, Sdwan-system-intf
```

```
m        10.11.11.6 [251/0] via 192.168.13.10, 04:03:35, Sdwan-system-intf
m        10.11.11.30 [251/0] via 192.168.11.21, 04:03:35, Sdwan-system-intf
```

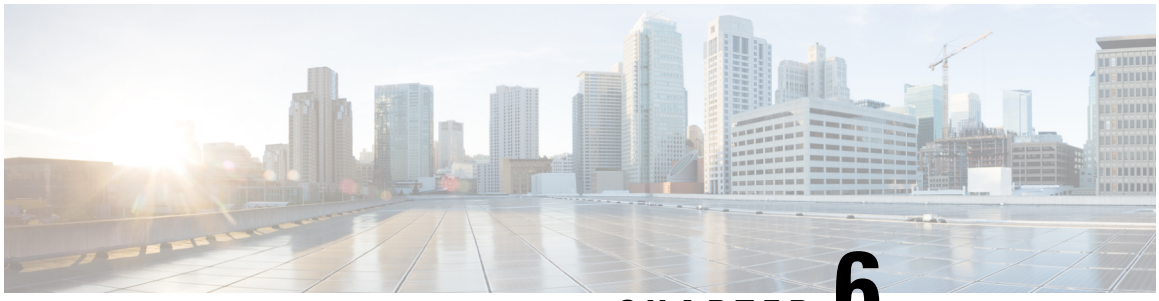
In this output, `Ni - NAT inside` is configured.

In this output, the lines beginning with `m` indicate that the NAT routes are added to the routing table.

Monitor service-side NAT object tracker

Monitor changes to NAT route advertisements and tracked interfaces.

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs**.
2. Click **Events**.



CHAPTER 6

Configure NAT64

Objective

Guides the configuration of Network Address Translation for Internet Protocol version 6 to Internet Protocol version 4, including direct internet access, service-side translation, and address and port mapping techniques using encapsulation.

- Configure NAT64, on page 121
- NAT64 direct internet access, on page 121
- Service-side NAT64, on page 128
- Mapping of address and port using encapsulation with NAT64, on page 136

Configure NAT64

Describes how to configure NAT64.

A NAT64 configuration allows you to translate IPv6 addresses to IPv4 addresses for connecting IPv6 and IPv4 networks.

Traffic origination is always from the transport-side (WAN) to the service-side (LAN) in the overlay network.

NAT64 direct internet access

Describes NAT64 direct internet access.

Table 23: Feature history

Feature Name	Release Information	Description
NAT64 DIA for Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 16.12.1b Cisco vManage Release 19.2.1	The NAT64 Direct Internet Access (DIA) feature supports routing of traffic from branch sites directly to the internet instead of tunneling the internet traffic to a central site or data center for internet access. NAT64 DIA allows IPv6 clients from a branch site to access IPv4 enterprise application servers in a data center or locally in the branch. IPv6 clients can also access IPv4 servers from the branch directly using the internet.

Information about NAT64 DIA

NAT64 DIA allows an IPv4 server to access an IPv6 server either from a remote branch or from a data center.

NAT64 DIA allows an IPv4 server to access an IPv6 server either from a remote branch or from a data center.

The traffic flow for NAT64 DIA is from the LAN to DIA.

How NAT64 DIA works

Summary

Enable IPv4 and IPv6 using a Cisco VPN Interface Ethernet template.

Workflow

1. Enable IPv4 and IPv6 using a **Cisco VPN Interface Ethernet** template.
2. Configure an IPv6 route in a **Cisco VPN** template, which is the service-side VPN.

   The source and destination IPv6 addresses are translated.
3. Because NAT IPv4 DIA is configured, the source IPv4 address gets translated because of interface overload. The destination IPv4 address remains the same.

Benefits of NAT64 DIA

Summarizes the benefits of NAT64 DIA.

- Enables good application performance
- Contributes to reduced bandwidth consumption and latency
- Contributes to lower bandwidth cost
- Enables improved branch office user experience by providing DIA at remote site locations

Restrictions for NAT64 DIA

NAT64 DIA uses interface overload only.

- NAT64 DIA uses interface overload only.
- NAT DIA pool or loopback is not supported with NAT64.
- Advertisement of NAT routes into OMP is not supported.

Restrictions for a NAT64 DIA route

- You can use the following NAT64 DIA routes for installing routes in the routing table:

  Example of a NAT64 DIA route for a /128 prefix:

  ```
  nat64 route vrf 4 64:FF9B::1E00:102/128 global
  ```

  Example of a NAT64 DIA route for a /96 prefix:

  ```
  nat64 route vrf 4 64:FF9B::/96 global
  ```

- You cannot use the following NAT64 DIA route configurations for installing routes in the routing table:

  ```
  nat64 route vrf 4 64:ff9b::/64 global
  nat64 route vrf 4 ::0/0 global
  ```

Configure NAT64 DIA and a DIA route

Describes how to configure NAT64 DIA and a DIA route.

Workflow for enabling NAT64 DIA

Procedure

Step 1 Enable NAT64 using a **Cisco VPN Interface Ethernet** template for both IPv4 and IPv6.

Note NAT64 IPv4 DIA uses interface overload by default.

When configuring NAT64 for IPv6 DIA, interface overload is already configured.

A **Cisco VPN Interface Ethernet** template is a transport interface.

Step 2 Configure a NAT64 DIA IPv6 route using a **Cisco VPN** template, which is the service VPN.

NAT64 is enabled for IPv4 and IPv6, and the NAT64 DIA route is configured.

What to do next

Verify the NAT64 DIA route configuration. See Verify NAT64 DIA route configuration

Configure NAT64 DIA

Describes how to configure NAT64 DIA.

Configure NAT64 DIA with interface overload

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 Edit a **Cisco VPN Interface Ethernet** template by clicking **. . .** and then clicking **Edit**.

Step 4 In the **Interface Name** field, choose an interface.

Step 5 Click **NAT** and choose **IPv4**.

a) Change the scope from **Default** to **Global**.

b) Click **On** to enable NAT for IPv4.

a) In the **NAT Type** field, click **Interface** for interface overload.

Ensure that the **Interface** option is set to **On** for IPv4.

Table 24: NAT IPv4 parameters

Parameter Name	Description
NAT	Specify if NAT translation is used. The default is **Off**.
NAT Type	Specify the NAT translation type for IPv4. Available options include: **Interface**, **Pool**, and **Loopback**. The default is the **Interface** option. The **Interface** option is supported for NAT64.
UDP Timeout	Specify when NAT translations over UDP sessions time out. Range: 1–536870 seconds Default: 300 seconds (5 minutes) **Note** Starting 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 been changed to 300 seconds (5 minutes).

Parameter Name	Description
TCP Timeout	Specify when NAT translations over TCP sessions time out. Enter a timeout value. Default: 3600 seconds (1 hour) **Note** Starting 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).

Step 6 Repeat Step 5, but choose **IPv6** to enable NAT for IPv6.

Note Configure both IPv4 and IPv6 for NAT64 DIA.

Step 7 In the **NAT Selection** field, click **NAT64** to enable NAT64.

Note For IPv6, interface overload is already configured.

Table 25: NAT IPv6 parameters

Parameter Name	Description
NAT	Specify if NAT translation is used. The default is **Off**.
NAT Selection	Specify NAT64. The default is the **NAT66** option.

Step 8 Click **Update**.

NAT64 DIA is configured for the selected IPv4 and IPv6 interfaces.

What to do next

Verify the NAT64 DIA route configuration. See Verify NAT64 DIA route configuration

Configure a NAT64 DIA route

Describes how to configure a NAT64 DIA route.

Configure a NAT64 DIA route using a Cisco VPN template

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 Edit a **Cisco VPN** feature template by clicking **. . .** and then clicking **Edit**.

Note You configure an IPv6 DIA route in a **Cisco VPN** feature template, which is the service-side VPN.

Step 4 Click **IPv6 Route**.

Step 5 Click **New IPv6 Route**.

Step 6 In the **Prefix** field, enter the well-known prefix, `64:FF9B::/96`.

Step 7 In the **Gateway** field, click **VPN**.

Step 8 In the **Enable VPN** field, change the scope from **Default** to **Global**, and click **On** to enable VPN.

Step 9 In the **NAT** field, click **NAT64**.

Step 10 Click **Update**.

The NAT64 DIA route is configured with the specified prefix and global VPN scope.

What to do next

Verify the NAT64 DIA route configuration. See Verify NAT64 DIA route configuration

Configure a NAT64 DIA route using the CLI

Describes how to configure a NAT64 DIA route using the CLI.

Procedure

Example: Configure a NAT64 DIA route

Example:

```
Device(config)# nat64 route vrf 4 64:FF9B::1E00:102/128 global
```

The NAT64 DIA route is configured.

What to do next

Verify the NAT64 DIA route configuration. See Verify NAT64 DIA route configuration

Verify NAT64 DIA route configuration

Objective

Describes how to verify NAT64 DIA route configuration.

Example 1

The following is a sample output from the **show ipv6 route vrf** command, which is for the service VPN:

```
Device# show ipv6 route vrf 4
IPv6 Routing Table - 4 - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy
       lp - LISP publications, a - Application, m - OMP
m   64:FF9B::/96 [251/0]
     via 172.16.255.15%default, Sdwan-system-intf%default
```

In this example, `64:FF9B::/96`, is the NAT64 well-known prefix for translating IPv6 to IPv4 addresses.

Example 2

Because NAT64 DIA is configured in the transport VPN, the routing table in the transport VPN appears as the following:

```
Device# show ipv6 route
IPv6 Routing Table - default - 2 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy
       lp - LISP publications, a - Application, m - OMP, Nd - Nat-Route DIA
S   64:FF9B::/96 [1/0]
```

Configuration example for NAT64 DIA

Objective

This example shows what is configured for NAT64 DIA.

This example shows what is configured for NAT64 DIA.

```
interface GigabitEthernet1
          no shutdown
          arp timeout 1200
          ip address 10.1.15.15 10.255.255.255
          no ip redirects
```

```
         ip mtu    1500
         ip nat outside
         load-interval 30
         mtu           1500
         negotiation auto
         nat64 enable
         !
         nat64 v6v4 list nat64-global-list interface GigabitEthernet1 overload
         !
         ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet1
overload
```

Note GigabitEthernet1 is a transport VPN interface.

Service-side NAT64

Describes service-side NAT64.

Table 26: Feature history

Feature Name	Release Information	Description
Service-Side NAT64 for Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 16.12.1b Cisco vManage Release 19.2.1	The service-side Network Address Translation (NAT) 64 feature translates a source IPv6 address to available IPv4 addresses in a NAT pool. The destination IPv6 address is translated to the server's actual IPv4 address since the destination IPv6 address is an IPv4 embedded IPv6 address. Service-side NAT64 allows IPv4 servers to communicate with IPv6 clients.

Information about service-side NAT64

With the dwindling IPv4 public address space and the growing need for more routable addresses, service providers and enterprises continue to build and roll out IPv6 networks.

With the dwindling IPv4 public address space and the growing need for more routable addresses, service providers and enterprises continue to build and roll out IPv6 networks. As the IPv4 internet is going to stay for a while, communication between IPv4 and IPv6 networks is an important requirement for a seamless end-user experience.

NAT IPv6 to IPv4, or NAT64, technology facilitates communication between IPv6 and IPv4 networks.

The service-side NAT64 feature translates a source IPv6 address to available IPv4 addresses in a NAT pool. The destination IPv6 address is translated to the server's actual IPv4 address since the destination IPv6 address is an IPv4-embedded IPv6 address.

Cisco IOS XE Catalyst SD-WAN devices use stateful NAT64 for translating IPv6 addresses to IPv4 addresses and IPv4 addresses to IPv6 addresses. Stateful NAT64 with NAT overload provides a 1:*n* mapping between IPv4 and IPv6 addresses.

How service-side NAT64 works

Summary

An IPv6 client attempts to connect to an IPv4 server.

Workflow

1. An IPv6 client attempts to connect to an IPv4 server.
2. The IPv6 client makes an IPv6 AAAA record DNS query, which is an IPv6 query for an IPv4 address.

   The DNS64 server responds with an IPv4-embedded IPv6 address.

   Example:

   ```
   64:ff9b::c000:0201
   ```

   which uses the NAT64 well-known prefix (WKP), `64:FF9B::/96`. The WKP is used for algorithmic mapping between address families.

   An IPv4-embedded IPv6 address consists of a variable length prefix, an embedded IPv4 address, and a variable length suffix. The last 32 bits are the hexadecimal representation of the original IPv4 address, which is 192.0.2.1 in this example.
3. The IPv6 client now tries to connect to the IPv4 server.
4. An IPv6 to IPv4 translation is performed.

   A source IPv6 address is translated to one of the available IPv4 addresses in the pool.

   A destination IPv6 address is translated to the server's actual IPv4 address since the destination IPv6 address is an IPv4-embedded IPv6 address.

Benefits of service-side NAT64

Summarizes the benefits of service-side NAT64.

- Supports communication between IPv6 clients in the service VPN with IPv4 servers on the internet
- Provides translation of IPv6 to IPv4 addresses for maintaining dual access to IPv6 and IPv4 networks
- Requires little or no changes to existing IPv4 network infrastructures when using stateful NAT64
- Provides a seamless internet experience for IPv6 users accessing IPv4 internet services, thus maintaining IPv4 business continuity
- Supports configuration of NAT64 without having to configure a data policy

Use cases for service-side NAT64

Supported traffic flow is from the IPv6 client on the remote site, in the data center, or in another branch site, to the IPv4 client or server on the local LAN.

Supported traffic flow is from the IPv6 client on the remote site, in the data center, or in another branch site, to the IPv4 client or server on the local LAN.

Note Traffic origination is always from the transport-side (WAN) to the service-side (LAN) in the overlay network.

Prerequisites for service-side NAT64

For Domain Name System (DNS) traffic to work, you must have a separate working installation of DNS64.

- For Domain Name System (DNS) traffic to work, you must have a separate working installation of DNS64.

Restrictions for service-side NAT64

Traffic must always originate on the remote branch site and go to the IPv4 server on the local LAN.

- Traffic must always originate on the remote branch site and go to the IPv4 server on the local LAN.
- Traffic cannot originate from the IPv4 server to any IPv6 client in the data center or to a remote branch site.

IPv4 address restrictions for service-side NAT64

- For more information on the usable IPv4 destination IP addresses, see the Deployment Guidelines, RFC 6052, Section 3.1.
- The well-known prefix (WKP) must not be used to represent non-global IPv4 addresses, such as those listed in the Deployment Guidelines, Section 3 of RFC 5735.

  For example, the following IPv4 prefixes are not allowed:

  - 0.0.0.0/8
  - 10.0.0.0/8
  - 127.0.0.0/8
  - 169.254.0.0/16

- You cannot use a private IPv4 address range on the service-side (LAN).

Configure service-side NAT64

Describes how to configure service-side NAT64.

The following sections provide information about configuring service-side NAT64.

Enable service-side NAT64 using a feature template

Describes how to enable service-side NAT64 using a feature template.

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 Edit a **Cisco VPN Interface Ethernet** template by clicking **. . .** and then clicking **Edit**.

Note The **Cisco VPN Interface Ethernet** template is a service-side interface.

Step 4 Click **NAT** and choose **IPv6** for NAT64.

Step 5 Change the scope from **Default** to **Global**.

Step 6 In the **NAT64** field, click **On** to enable NAT64.

Step 7 Click **Update**.

Service-side NAT64 is enabled using the feature template.

What to do next

Configure a service-side NAT64 pool. See Configure a service-side NAT64 pool

Configure a service-side NAT64 pool 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) NAT

Table 27: NAT

Field	Description
Add NAT64 v4 Pool	

Field	Description
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

The service-side NAT64 pool is configured using a configuration group.

What to do next

Also see Deploy a Configuration Group.

Verify the service-side NAT64 configuration. See Verify configuration of service-side NAT64

Configure a service-side NAT64 pool

Describes how to configure a service-side NAT64 pool.

Before you begin

Configure a service-side NAT64 pool

Before you begin

You must have enabled service-side NAT64 using a **Cisco VPN Interface Ethernet** template before configuring a NAT64 IPv4 pool.

Procedure

Step 1 Create a new **Cisco VPN** feature template or edit an existing **Cisco VPN** feature template. The **Cisco VPN** feature template corresponds to the service-side VPN you want to configure NAT64 for.

Step 2 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 3 Click **Feature Templates**.



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

Step 4 Edit a **Cisco VPN** template by clicking **. . .** and then clicking **Edit**.

Step 5 Click **NAT**.

Step 6 Click **NAT64 v4 Pool**.

Step 7 Click **New NAT64 v4 Pool**.

Step 8 In the **NAT64 Pool name** field, specify the pool name.

Note You have to specify a number for the pool name.

Step 9 In the **NAT 64 v4 Pool Range Start** field, specify the IPv4 address for the start of the pool range.

Step 10 In the **NAT 64 v4 Pool End Start** field, specify the IPv4 address for the end of the pool range.

Step 11 From the drop-down list, choose **Global**.

Step 12 Click **On** to enable **NAT 64 Overload**.

Note **NAT 64 Overload** is set to **Off** by default.

Step 13 Click **Add**.

Step 14 Click **Update** to push the configuration to the device.

The service-side NAT64 pool is configured with the specified IPv4 range and overload settings.

What to do next

Verify the service-side NAT64 configuration. See Verify configuration of service-side NAT64

Configure service-side NAT64 using the CLI

Describes how to configure service-side NAT64 using the CLI.

Table 28: Feature history

Feature Name	Release Information	Description
IPv6 Support for NAT64 Devices	Cisco IOS XE Catalyst SD-WAN Release 16.12.1b	This feature supports NAT64 to facilitate communication between IPv4 and IPv6 on Cisco IOS XE Catalyst SD-WAN devices.

Procedure

Step 1 Enable service-side NAT64 using the CLI

This section provides an example CLI configuration for enabling service-side NAT64.

Enable service-side NAT64 on the LAN interface, which is equivalent to the **Service VPN** template on Cisco SD-WAN Manager.

The IPv4 application server is on the local LAN site and the IPv6 client is in the data center or on the remote site of the LAN.

```
Device# interface GigabitEthernet 5.104
                        nat64 enable
```

Step 2 Configure a service-side NAT64 pool using the CLI

This section provides an example CLI configuration for configuring a service-side NAT64 pool.

```
Device# nat64 v4 pool pool10 192.0.2.0 192.0.2.254

nat64 v6v4 list global-list_nat64 pool pool10 vrf 4 overload
```

Service-side NAT64 is enabled and the NAT64 pool is configured.

What to do next

Verify the service-side NAT64 configuration. See Verify configuration of service-side NAT64

Verify configuration of service-side NAT64

Objective

Describes how to verify configuration of service-side NAT64.

Example - what displays in the routing table for the specified device

The following is a sample output from the **show ipv6 route vrf** command:

```
Device# show ipv6 route vrf 4
IPv6 Routing Table - 4 - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy
       lp - LISP publications, a - Application, m - OMP, Nd - Nat-Route DIA
Nd  64:FF9B::/96 [6/0]
     via Null0%default, directly connected
m   2001:DB8:AA:A::/64 [251/0]
     via 172.16.255.16%default, Sdwan-system-intf%default
C   2001:DB8:BB:A::/64 [0/0]
     via GigabitEthernet5.104, directly connected
L   2001:DB8:BB:A::1/128 [0/0]
     via GigabitEthernet5.104, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

In this example, the NAT64 well-known prefix, `64:FF9B::/96`, displays in the IPv6 routing table of a service VPN.

The following is a sample output from the **show ip route vrf 4** command:

```
Device# show ip route vrf 4
Routing Table: 4
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected
```

The NAT64 IPv4 pool address is installed in the routing table as `nat inside route` in the IPv4 routing table of a service VPN.

Example - what displays in the routing table on OMP

The following is a sample output from the **show ipv6 route vrf** command:

```
Device# show ipv6 route vrf 4
IPv6 Routing Table - 4 - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy
       lp - LISP publications, a - Application, m - OMP
m   64:FF9B::/96 [251/0]
     via 172.16.255.15%default, Sdwan-system-intf%default
C   2001:DB8:AA:A::/64 [0/0]
     via GigabitEthernet5.104, directly connected
L   2001:DB8:AA:A::1/128 [0/0]
     via GigabitEthernet5.104, receive
m   2001:DB8:BB:A::/64 [251/0]
     via 172.16.255.15%default, Sdwan-system-intf%default
L   FF00::/8 [0/0]
     via Null0, receive
```

In this example, the NAT64 well-known prefix, `64:FF9B::/96`, is received as an Overlay Management Protocol (OMP) route.

The NAT64 IPv4 pool addresses are received as an OMP route.

Configuration examples for service-side NAT64

Objective

This example shows the configuration of service-side NAT64.

This example shows the configuration of service-side NAT64.

```
nat64 v4 pool 1-4 192.0.2.0 192.0.2.254
nat64 v6v4 list nat64-list pool 1-4 vrf 4 overload
!
interface GigabitEthernet5.104
```

```
 encapsulation dot1Q 104
 vrf forwarding 4
 ip address 10.1.19.15 10.255.255.255
 ip mtu 1496
 ip ospf network broadcast
 ip ospf 4 area 0
 nat64 enable
end
```

This example shows the configuration of a NAT64 pool.

```
nat64 v4 pool 1-4 192.0.2.0 192.0.2.254
nat64 v6v4 list nat64-list pool 1-4 vrf 4 overload
!
interface GigabitEthernet5.104
 encapsulation dot1Q 104
 vrf forwarding 4
 ip address 10.1.19.15 10.255.255.255
 ip mtu 1496
 ip ospf network broadcast
 ip ospf 4 area 0
 nat64 enable
end
```

Mapping of address and port using encapsulation with NAT64

Mapping of address and port using encapsulation with NAT64

Table 29: Feature history

Feature Name	Release Information	Description
Mapping of Address and Port Using Encapsulation (MAP-E) with NAT64	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This feature provides support for an IPv4 client to access IPv4 servers when using an IPv6-only network. IPv4 traffic is routed to the internet over an IPv6 tunnel. With this feature, you can configure a MAP-E domain and MAP-E parameters for transporting IPv4 packets over an IPv6 network using IP encapsulation. When the MAP-E customer edge (CE) device starts or when an IPv4 address changes, the device obtains the MAP-E parameters automatically from the MAP-E rule server using HTTP. This feature lets you configure a MAP-E domain and MAP-E parameters for transporting IPv4 packets over an IPv6 network using IP encapsulation. When the MAP-E customer edge (CE) device starts or when an IPv4 address changes, the device obtains the MAP-E parameters automatically from the MAP-E rule server using HTTP.

Feature Name	Release Information	Description
Mapping of Address and Port Using Encapsulation (MAP-E) with Transport Locator (TLOC)	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	This feature extends the support for IP over Ethernet (IPoE) MAP-E to include TLOC interfaces. The integration of MAP-E with TLOC allows the device to handle IPv4 traffic efficiently over an IPv6 network.

Information about MAP-E with NAT64

Information about MAP-E with NAT64

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a

Mapping of Address and Port with Encapsulation (MAP-E) is an Internet Engineering Task Force (IETF) draft that describes a mechanism for transporting IPV4 packets over an IPv6-only network using encapsulation.

Within the MAP-E domain, IPv4 packets are exchanged between MAP-E CE devices and the public IPv4 internet by encapsulating and transporting the packets through the IPv6-only network.

The MAP-E with NAT64 feature supports the following configurations:

- Shared-IPv4 configuration

  MAP-E enables multiple MAP-E CE devices within a MAP-E domain to share a single IPv4 address. Each MAP-E CE device with the same IPv4 address has to use a different TCP or UDP port. MAP-E provides IPv4 connectivity using shared IPv4 addresses in an IPv6-only network.

- Fixed-IPv4 configuration

  In a fixed-IPv4 configuration, one MAP-E CE device uses a fixed-IPv4 address.

MAP-E with TLOC

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.16.1a and Cisco Catalyst SD-WAN Manager Release 20.16.1

The IPoE MAP-E feature on Transport Locator (TLOC) interfaces enhances the Cisco Catalyst SD-WAN capabilities by providing reliable configurations for WAN services. TLOCs are identifiers representing the WAN edge router's physical or logical interfaces used for transport across the WAN. Each TLOC is characterized by three attributes: color (indicating the transport type, such as MPLS or Internet), IP address, and encapsulation type (such as IPsec or GRE).

By integrating MAP-E with TLOC, the Cisco Catalyst SD-WAN solution leverages MAP-E technology over TLOC interfaces to deliver WAN services. This integration allows efficient handling of IPv4 traffic over an IPv6 network by utilizing the TLOC's transport capabilities.

Components of a MAP-E configuration with NAT64

Each mapping of address and port using a MAP-E domain uses a different mapping rule.

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a

Each mapping of address and port using a MAP-E domain uses a different mapping rule. A MAP-E configuration contains the following:

- Basic mapping rule (BMR)

  A BMR configures the MAP-E IPv6 address or prefix. You can configure only one BMR per IPv6 prefix. The MAP-E CE device uses the BMR to configure itself with an IPv4 address, an IPv4 prefix, or a shared IPv4 address from an IPv6 prefix. You can also use a BMR for forwarding packets in use cases where an IPv4 source address and source port are mapped to an IPv6 address or prefix. Every MAP-E CE must be provisioned with a BMR.

  The BMR IPv6 prefix along with the port parameter is used as a tunnel source address.

- One default mapping rule (DMR)

  A DMR prefix that matches with the interface address is recognized as a host and a DMR prefix with a prefix length of 128 is recognized as the tunnel source address. A border router IPv6 address is the tunnel destination address.

- Port-set ID (PSID)

  The PSID identifies the allowed ports to use.

  The border router checks whether the PSID and the port set match. If the port-set ID and port set match, the DMR matches the packet destination of the IPv6 packet. Based on the BMR, the border router constructs the IPv4 source address and extracts the IPv4 destination address from the IPv6 destination address. The IPv6 packet uses the NAT64 IPv6-to-IPv4 translation engine to construct the IPv4 packet from the IPv6 packet.

Configure the MAP-E parameters automatically from the MAP-E rule server using HTTP when the MAP-E CE device starts or whenever an IPv6 address changes.

Note It is mandatory to configure the IPv6 WAN interface as the source interface for the HTTP client. For example:

```
ip http client source-interface GigabitEthernet0/0/0
```

To configure a MAP-E domain and MAP-E parameters, use the **nat64 provisioning** command. For more information on configuring a MAP-E domain and MAP-E parameters, see the Cisco IOS XE SD-WAN Qualified Command Reference Guide.

For information on the MAP-E rule REST API specifications, see the IP Addressing: NAT Configuration Guide.

Benefits of MAP-E with NAT64

Benefits of MAP-E with NAT64

- Supports IPv4 traffic flow over an IPv6-only network.
- Supports efficient traffic delivery with lower latency without requiring additional hardware at the border router.
- Supports an easy-to-use and scalable solution for migrating to IPv6.

Restrictions for MAP-E with NAT64

Restrictions for MAP-E with NAT64

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a

- Support for a single BMR per a MAP-E CE device. Configure different mapping rules for every address and port translation.
- No support for a BMR prefix length of 64, fragmentation, and local packet generation.
- The MAP-E with TLOC feature is supported for fixed IP mode only in Cisco IOS XE Catalyst SD-WAN Release 17.16.1a.
- The IOS-XE MAP-E solution works only when there is a single IPv6 interface connected to the service provider. Multiple WAN side IPv6 interfaces is not supported.

Workflow for MAP-E with NAT64

Summary

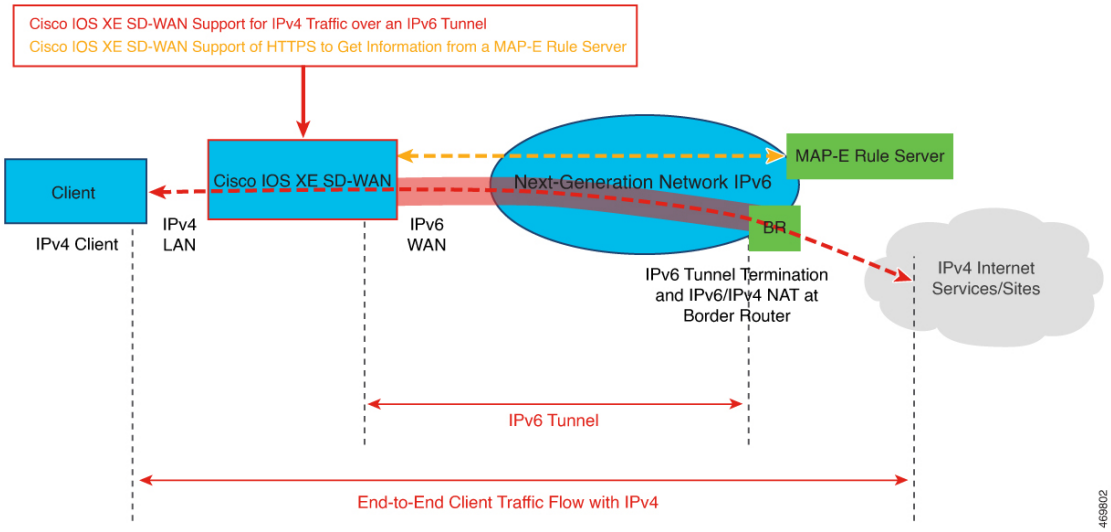
Workflow for MAP-E with NAT64

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a

The following diagram describes the end-to-end client traffic flow for an IPv4 client to reach an IPv4 server when using an IPv6-only network with MAP-E.

Workflow

Figure 8: Workflow for MAP-E with NAT64



MAP-E interactions between a MAP-E CE device and a MAP-E rule server

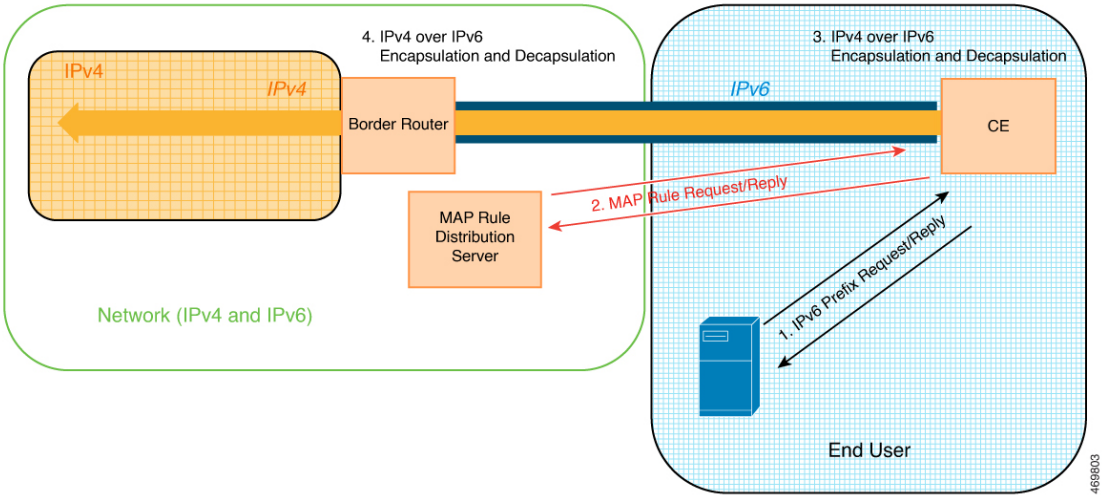
1. The MAP-E rule server acquires an IPv6 prefix from an IPv6-only network.

2. A MAP-E CE device sends an HTTP request to the MAP-E rule server and receives a response.

   MAP-E enables a Cisco IOS XE Catalyst SD-WAN device to function as a MAP-E CE device.

3. Per the MAP-E rule, a MAP-E CE device performs a translation of the incoming IPv4 packets.
4. The MAP-E CE device encapsulates the IPv4 packets into IPv6 packets and sends the IPv6 packets to the border router.
5. On receiving the encoded IPv6 packets, the IPv6 packets are decapsulated by the border router according to the MAP-E rule, and the IPv6 traffic is routed to the IPv4 public internet.

Figure 9: MAP-E workflow



Configure MAP-E with NAT64 using a CLI template

Configure MAP-E with NAT64 using a CLI template

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a

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 a MAP-E domain and MAP-E parameters.

Procedure

Step 1 Disable the NAT64 fragmentation header.

```
nat64 settings fragmentation header disable
```

Step 2 Configure a NAT64 DIA route.

```
nat64 route ip-address
                        interface-type-number
```

For more information, see Configure a NAT64 DIA Route.

Step 3 Specify the NAT64 MAP-E domain and enter MAP-E configuration mode.

```
nat64 provisioning mode jp01
```

Step 4 Configure the address resolution sever with a username and password.

```
address-resolution-server http://ipv6-prefix/directory-path
address-resolution-server 6 username encypted-user-name
address-resolution-server 6 password encypted-password
```

You can also specify an encryption type (2 or 6) for encrypting the address resolution server username and password.

Step 5 Configure a MAP-E rule server.

```
rule-server http://admin:admin@ipv6-prefix//directory-path
```

You can also specify an encryption type (2 or 6) for encrypting the rule server URL.

Step 6 (Optional) Configure a wait time in seconds for responses from the HTTP server.

```
rule-server request wait-time value-seconds
```

Step 7 Configure a host name.

Example:

```
hostname hostname
```

The host name is from the MAP-E rule server. In case you overwrite the host name, you can specify a new host name.

Step 8 Configure a tunnel interface.

```
tunnel interface Tunnelnumber
tunnel source interface-type-interface-number
```



Note Configure a tunnel interface and a tunnel source for a fixed-IPv4 configuration only.

Step 9 Configure a service prefix.

```
service-prefix ipv6-prefix
```



Note The IPv6 prefix of the MAP-E rule returned from the MAP-E rule server needs to match the IPv6 service prefix configured on the MAP-E CE device.

Note Configure a service prefix for either a fixed-IPv4 configuration or for a shared-IPv4 configuration.

The MAP-E domain and NAT64 parameters are configured.

Here is a complete configuration example for configuring a MAP-E domain and parameters.

```
nat64 settings fragmentation header disable
nat64 settings v4 tos ignore
interface GigabitEthernet1
!
nat64 settings mtu minimum 1500
nat64 provisioning mode jp01
 address-resolution-server http://2001:db8:b000:0:fe7f:6ee7:33db:5013/nic/update
 address-resolution-server password encypted-password
 address-resolution-server username encypted-username
 rule-server http://admin:admin@2001:DB8:A000::1//mape-rule.json
 rule-server request wait-time 180
 hostname hostname
 tunnel interface Tunnel1
 tunnel source GigabitEthernet2
 service-prefix 2001:DB8:b800::/48
!
nat64 route 0.0.0.0/0 GigabitEthernet1
```

What to do next

Verify MAP-E with NAT64 configuration. See Verify MAP-E with NAT64 configuration

Verify MAP-E with NAT64 configuration

Objective

Verify MAP-E with NAT64 configuration

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a

The following example is a sample output from the **show nat64 map-e** command:

```
Device# show nat64 map-e
MAP-E Domain 9126
   Mode MAP
   Border-relay-address
      Ip-v6-address 2001:DB8::9
   Basic-mapping-rule
      Ip-v6-prefix 2001:DB8:B001:80::/60
      Ip-v4-prefix 10.1.1.0/24
      Port-parameters
         Share-ratio 4   Contiguous-ports 256   Start-port 1024
         Share-ratio-bits 2   Contiguous-ports-bits 8   Port-offset-bits 6
      Port-set-id 0
```

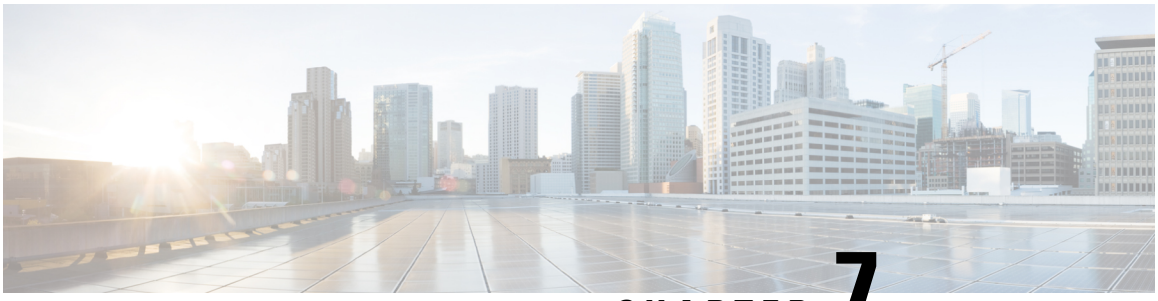
The output above is an example of a shared-IPv4 address configuration because the ports are shared across the MAP-E CE devices. The output displays the MAP-E parameters that were returned from the MAP-E rule server.

The following example is a sample output from the **show nat64 statistics** command:

```
Device# show nat64 statistics
NAT64 Statistics

Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Sessions found: 0
Sessions created: 0
Expired translations: 0
Global Stats:
   Packets translated (IPv4 -> IPv6)
      Stateless: 0
      Stateful: 0
      nat46: 0
      MAP-T: 0
      MAP-E: 5
   Packets translated (IPv6 -> IPv4)
      Stateless: 0
      Stateful: 0
      nat46: 0
      MAP-T: 0
      MAP-E: 4

Interface Statistics
   GigabitEthernet0/0/0 (IPv4 not configured, IPv6 configured):
      Packets translated (IPv4 -> IPv6)
         Stateless: 0
         Stateful: 0
         nat46: 0
         MAP-T: 0
         MAP-E: 0
      Packets translated (IPv6 -> IPv4)
         Stateless: 0
         Stateful: 0
         nat46: 0
         MAP-T: 0
         MAP-E: 4
      Packets dropped: 0
   GigabitEthernet0/0/1 (IPv4 configured, IPv6 not configured):
      Packets translated (IPv4 -> IPv6)
         Stateless: 0
         Stateful: 0
         nat46: 0
         MAP-T: 0
         MAP-E: 5
      Packets translated (IPv6 -> IPv4)
         Stateless: 0
         Stateful: 0
         nat46: 0
         MAP-T: 0
         MAP-E: 0
      Packets dropped: 0
Dynamic Mapping Statistics
   v6v4
Limit Statistics
```



CHAPTER 7

Configure NAT66

- Feature history: Configure NAT66, on page 145
- Configure NAT66 DIA and a DIA route, on page 153
- NAT66 DIA Route redistribution, on page 162
- Dialer interfaces with NAT66 DIA, on page 167

Feature history: Configure NAT66

Objective

This reference provides information about the features and enhancements that have been introduced for Configure NAT66 across different software releases.

Table 30: Feature History

Feature Name	Release Information	Description
Support for NAT66 DIA	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	The IPv6-to-IPv6 Network Address Translation (NAT66) Direct Internet Access (DIA) feature enables an IPv6 device to translate an inside source address prefix to an outside source address prefix in IPv6 packet headers. NAT66 DIA allows you to direct local IPv6 internet traffic to exit directly to the internet from the service-side VPN (VPN 1) through the transport VPN (VPN 0). You can configure NAT66 DIA using Cisco SD-WAN Manager, the CLI, or a device CLI template. This feature introduces new CLI commands. For more information on the new NAT commands, see the Cisco IOS XE Catalyst SD-WAN Qualified Command Reference Guide.

Feature Name	Release Information	Description
Support for Multiple WAN Links for NAT66 DIA	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	You can configure NAT66 to use multiple WAN links to direct local IPv6 traffic to exit directly to the internet.
Automatically Configure IPv6 Address on a WAN Interface by Using SLAAC	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	You can configure the Stateless Address Autoconfiguration (SLAAC) by using the Router Advertisement (RA) prefix to automatically assign IPv6 addresses for NAT66 prefix translations.
Support for Flow Stickiness	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	Flow stickiness records the flow level state of the NAT path and ensures that the application flows don't get reset due to a change in the NAT path. When the first packet match fails in deep packet inspection (DPI), the edge router ensures the first flow for this unknown application to stick to the original path, bypassing the policy to change the path when it is recognized by the DPI engine a few packets later.
Support for Centralized Data Policy for NAT66 DIA	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	You can configure the centralized data policy by using the **nat use-vpn 0** command, which ensures that matching traffic is sent to VPN 0 after the source IP is translated, based on the policy match criteria. This feature is supported from service and from tunnel. The fallback option ensures that the traffic falls back to routing and takes the overlay path when the DIA route is not available.
Support for Redistribution of NAT66 DIA Routes	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	You can configure the redistribution of NAT66 DIA routes into BGP or OSPFv3 protocols.
Support for NAT66 DIA Status Event.	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	You can monitor the NAT DIA status in the Cisco SD-WAN Manager logs. A new event called **nat-update** displays the status of NAT DIA on the **Events** page.
Support for Point-to-Point Protocol (PPP) Dialer Interfaces with NAT66 DIA	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	This feature adds support for two types of PPP dialer interfaces—PPP over Ethernet (PPPoE) and PPP over Asynchronous Transfer Mode (PPPoA). With this feature, you can configure PPP dialer interfaces for accessing IPv6 services and sites.

Information about NAT66 DIA

IPv6-IPv6 Network Prefix Translation (NPTv6) is a mechanism that converts an IPv6 address prefix to another IPv6 address prefix. The address translation method that is used is IPv6-IPv6 Network Address Translation (NAT66). A device that supports a NAT66 function is known as a NAT66 translator. A NAT66 translator provides source and destination address translation capability.

Additional NAT66 DIA information

Note NPTv6 functionality was already available on Cisco IOS XE platforms before it was introduced in Cisco Catalyst SD-WAN in the Cisco IOS XE Catalyst SD-WAN Release 17.7.1a. For more information, see the *IP Addressing: NAT Configuration Guide*.

NAT66 DIA allows you to redirect or forward packets from one network to another in an IPv6 environment. NAT66 DIA provides an algorithmic translation function with a 1:1 relationship between addresses within the inside network and the outside network. You can interconnect different networks and support multihoming, load balancing, and peer-to-peer networking.

NAT66 DIA supports prefixes longer than 64 bits and static IPv6 host-to-host translations. Only the prefix portion of an IPv6 address is translated.

Note To access Cisco SD-WAN Manager using an IPv6 address, specify port number 8443 in the URL.

Example:

```
https://[cisco-vmanage IPv6-address]:8443/
```

NAT66 DIA Flow Stickiness

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a.

When NAT66 DIA is configured with centralized data policy with application match, the application flows subject to NAT66 DIA policy may get reset due to path change. For example, when you have a data policy matching an application list and the action is NAT66 DIA, the first few packets may not be identified by deep packet inspection (DPI). So, the packets not matching NAT66 DIA application policy follow routing to the Cisco Catalyst SD-WAN overlay path. When the flow is identified, the later packets of the flow take the NAT66 DIA path as defined by the data policy. This path change results in a flow reset as different paths means different client source or port combination towards the server and the server resets the unknown TCP flows.

The NAT66 DIA flow stickiness feature records the flow level state of the NAT66 path. If the first packet of the flow is non-NAT66, it keeps the rest of the packets of this flow to non-NAT66 paths. If the first packet flow is via the NAT66 DIA path, it keeps the rest of the packets of this flow to the NAT66 DIA path. It is enabled by default with the NAT66 DIA data policy.

From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the NAT66 DIA flow stickiness feature is enabled by default. To disable flow stickiness, use the command **flow-stickiness-disable** under the localized policy using the CLI add-on template.

How NAT66 DIA works

Summary

High-level description of how NAT66 DIA works

Workflow

1. An IPv6 client in a branch site attempts to access Cisco SD-WAN Manager in a data center on the transport side of the network (VPN 0).
2. The Cisco IOS XE Catalyst SD-WAN device routes the IPv6 address from the service VPN (VPN 1) to the next-hop transport VPN (VPN 0), which is the WAN side of the network.
3. A NAT66 translator performs an IPv6-to-IPv6 prefix translation. Dynamic Host Configuration Protocol version 6 (DHCPv6) requires a source IPv6 prefix in the IPv6 prefix range for prefix delegation.

   NAT66 conversion occurs in the transport VPN interface.

   DHCPv6 prefix delegation allows an ISP to automate the process of assigning prefixes to a customer for use within the customer's network. Prefix delegation occurs between a provider edge (PE) device and customer premises equipment (CPE) using the DHCPv6 prefix delegation option. After an ISP has delegated prefixes to a customer, the customer can further divide the network and assign prefixes to the links in the customer's network.
4. When traffic is returned from Cisco SD-WAN Manager, the Cisco IOS XE Catalyst SD-WAN device looks up the NAT66 entry in the DIA route table and forwards the packet to the client's IPv6 address.

Configure NAT66 DIA Using Stateless DHCP

From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, you can autoconfigure an IPv6 address on a WAN interface by using Stateless Address Autoconfiguration (SLAAC) with a Router Advertisement (RA) prefix. Stateless DHCPv6 is a combination of SLAAC and DHCPv6. The device sends an RA with the O bit set but does not set the M bit. This is known as Stateless DHCPv6 because the DHCPv6 server does not have to track the client address bindings. The RA prefix is available for use with NAT66 for IPv6 DIA of the service side traffic. Once configured, the same source prefix can be matched with different outside interfaces.

Before you begin, ensure that you have configured DHCPv6 and SLAAC. For more information, see *Information About DHCPv6*.



Note Ensure that the RA prefix that are used in the SLAAC interface is different from the outside prefix that is used in the static NAT66 mapping rules.

When the mapping rule is configured and the flow match occurs, traffic flows from inside to outside. NAT66 maintains a bind table for sharing the RA prefix with service side hosts. When an IPv6 packet from the service side interface flows through the DIA path, a bind is created for the original source and the translated source address using the RA prefix. The same bind is used to translate back the packets. NAT66 maintains the bind entries for a specified time. The default timeout value is 5 minutes.

The prefix translation rule for an interface is effective only when the packet goes through that interface and there is no need to specify the egress interface when you've configured the prefix translation rule with RA.

When you configure the Translated Source Prefix as the system default, the SLAAC feature automatically provides the RA prefix (outside). Otherwise, you must configure the outside prefix in the translation rule.

You can configure NAT66 DIA Using Stateless DHCP by using the Cisco Catalyst SD-WAN Manager or the CLI:

- Configure NAT66 DIA Using Stateless DHCP Through Cisco Catalyst SD-WAN Manager
- Configure DIA Using Stateless DHCP using CLI

NAT66 DIA With centralized data policy

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1

NAT66 DIA centralized data policy

You can use the Cisco IOS XE Catalyst SD-WAN devices so that data traffic is NATed before entering the overlay tunnel that is located in the transport VPN. Based on the policy match criteria, matching IPv6 traffic is forwarded via DIA circuits after the source IP address is translated. The IPv6 traffic is forwarded after NAT66 on destination address via DIA circuits based on the centralized policy match criteria on source IPv6 prefix, prefix lists, or destination IPv6 prefix or Prefix-lists.`nat use-vpn 0` command to configure a NAT66 DIA route using a centralized data policy on

To configure NAT66 on the service-side of a device, you configure a NAT66 interface within a service VPN on the device, and then you configure a centralized data policy on the Cisco Catalyst SD-WAN Controller. The policy directs data traffic with the desired prefixes to the service-side NAT.

You can configure NAT for data that enters or exits the service-side of the network. The service-side NAT translates data traffic, of inside and outside host addresses, that match a configured centralized data policy.

If the DIA route is not available, traffic will drop if a fallback option is not configured. The NAT66 fallback feature provides a routing-based mechanism for all traffic that is sent to the DIA route to use an alternative route when required.This feature is supported this froms both service and from tunnel.

Configure NAT66 DIA through data policy using CLICisco SD-WAN Controller Using CLI

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

SUMMARY STEPS

1. Configure NAT66 DIA using CLI

DETAILED STEPS

Procedure

Configure NAT66 DIA using CLI

Here is the complete configuration example to configure NAT66 DIA Through Data Policy on Cisco SD-WAN Controller:

```
Device# policy
 data-policy policy-name
 vpn-list vpn_list
 sequence number
 match
 source-ipv6 ipv6-address
 !
 action accept
 nat use-vpn 0
 nat fallback
 set
 local-tloc-color lte
```

The CLI data policy configuration includes the NAT66 DIA action.

What to do next

To continue, see Verify dialer interface NAT66 DIA configuration.

Configure NAT66 DIA through data policy using Cisco Catalyst SD-WAN ManagerCisco Catalyst SD-WAN Manager

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1.

You can use the centralized data policy to configure IPv6 match and action conditions for NAT66 DIA along with fallback in Cisco SD-WAN Manager.

SUMMARY STEPS

1. Configure the centralized data policy for NAT fallback.
2. Configure the centralized data policy for NAT fallback.
3. To enable NAT fallback using Cisco SD-WAN Manager, create and configure a data policy by doing the following: Edit the existing centralized policy and import the policy:

DETAILED STEPS

Procedure

Step 1 Configure the centralized data policy for NAT fallback.

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
b) From the **Custom** options drop-down, under **Centralized Policy**, select **Traffic Data**.
c) From the **Add Policy** drop-down, click **Create New**.
d) Click **Sequence Type** and select **Custom**.
e) Click **(+) Sequence Rule** to create a new sequence rule.
f) Choose **IPv6** from the **Protocol** drop-down list.
g) After adding match conditions, click **Actions** and click **Accept**.
h) Click **NAT VPN** and select the **Fallback** checkbox.

Step 2 Configure the centralized data policy for NAT fallback.

a) Click **Save and Match Actions**.

b) Click **Save Data Policy**.

Step 3 To enable NAT fallback using Cisco SD-WAN Manager, create and configure a data policy by doing the following: Edit the existing centralized policy and import the policy:

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
b) From the **Custom** options drop-down, under **Centralized Policy**, select **Traffic Data**.
c) From the **Add Policy** drop-down, click **Create New**.
d) Click **Sequence Type** and select **Custom**.
e) Click **(+) Sequence Rule** to create a new sequence rule.
f) After adding match conditions, click **Actions** and click **Accept**.
g) Click **NAT VPN** and select the **Fallback** checkbox.
h) Click **Save and Match Actions**.
i) Click **Save Data Policy**.

The centralized data policy is configured to use NAT fallback for matching IPv6 traffic.

What to do next

To continue, see Verify dialer interface NAT66 DIA configuration.

Configure NAT66 DIA through data policy using policy groups

From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, you can use configuration groups to configure NAT66 DIA by using stateless DHCP in Cisco SD-WAN Manager.

Procedure

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

Step 2 Click **Application priority & SLA policy** to create a policy.

To edit an existing policy, click the ellipsis icon (**...**) next to the application priority and SLA policy under **Action** and click **Edit**

Step 3 Under **Internet Offload Traffic**, configure direct internet access by choosing an application from the **Application List** drop-down list and toggle on the **Fallback to Routing** option.

Step 4 Under **Apply Policy**, configure the direction, VPN, and interface.

Step 5 Click **Save**.

The policy group contains the NAT66 DIA data policy configuration.

What to do next

To continue, see Verify dialer interface NAT66 DIA configuration.

Benefits of NAT66 DIA

- Supports local IPv6 internet traffic to exit directly to the internet from the service-side VPN through the transport VPN

- Allows you to redirect or forward packets from one network to another in an IPv6 environment
- Enables good application performance
- Contributes to reduced bandwidth consumption and latency
- Contributes to lower bandwidth cost
- Enables improved branch office user experience by providing DIA at remote site locations
- Supports cellular and dialer interfaces from Cisco IOS XE Catalyst SD-WAN Release 17.14.x

Restrictions for NAT66 DIA

The following restrictions apply to NAT66 DIA:

- Firewall, AppNav-XE, and multicast are not supported.

  From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, NAT66 supports the use of a firewall.

- Only NAT66 DIA traffic flows are supported. There is no support for service-side traffic flows.
- Centralized data policy is not supported for NAT66 DIA.

  From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Centralized data policy is supported for NAT66 DIA.

- Combined NAT64 and NAT66 is not supported on the same interface.
- Only one single prefix translation is supported for each VRF.

  From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, multiple prefix translations are supported for each VRF.

- Use of multiple WAN links for NAT66 DIA is not supported.

  From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, multiple WAN links are supported for NAT66 DIA.

- NAT66 DIA route redistribution using the service IPv6 routing protocol is not supported.

  From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, you can configure NAT66 DIA route redistribution into BGP or OSPFv3 protocols.

- Real-time operational application programming interface (APIs) are not supported.
- You must include a default route in VPN 0 for successful NAT66 DIA route operations.
- Only physical Ethernet subinterfaces are supported.
- Router Advertisement (RA) prefix is not supported in NAT66 prefix translations.
- Multitenancy resource limits are not supported.
- IPv6 TLOC extension with NAT66 is not supported.

Configure NAT66 DIA and a DIA route

Summary

Configure NAT66 DIA and a DIA route.

Workflow

Configure NAT66 DIA and a DIA route.

Workflow for Enabling NAT66 DIA and a NAT66 DIA Route

1. Enable NAT66 DIA using a **Cisco VPN Interface Ethernet** feature template for IPv6.

   A **Cisco VPN Interface Ethernet** template is used as a transport (WAN) interface.

   For more information on enabling NAT66 DIA using a **Cisco VPN Interface Ethernet** template, see Configure NAT66 DIA.

2. Configure a NAT66 DIA IPv6 route using a **Cisco VPN** feature template, which is a service-side VPN (VPNs other than VPN 0).

   For more information on configuring a NAT66 DIA IPv6 route, see Configure a NAT66 DIA Route.

Configure NAT66 DIA

Procedure

Step 1 Configure NAT66 static translation.

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
b) Click **Feature Templates**.



Note In Cisco vManage Release 20.7.x release, **Feature Templates** is titled **Feature**.

c) Edit a **Cisco VPN Interface Ethernet** template by clicking **...** adjacent to it, and then choosing **Edit**.
d) Click **NAT** and choose **IPv6**.
e) In the **NAT** drop-down list, change the scope from **Default** to **Global**.

   Click **On** to enable NAT66.

f) In the **NAT Selection** field, choose **NAT66**.
g) Click **New Static NAT**.
h) In the **Source Prefix** field, specify the source IPv6 prefix.

Step 2 Configure NAT66 static translation.

a) In the **Translated Source Prefix** field, specify the translated source prefix.

b) In the **Source VPN ID** field, specify the source VPN ID.
c) Click **Update**.

The Cisco VPN Interface Ethernet template contains the NAT66 static translation settings.

What to do next

To continue, see Verify dialer interface NAT66 DIA configuration.

Enable DHCPv6 prefix delegation using a CLI add-on template

SUMMARY STEPS

1. Create a CLI add-on feature template for DHCPv6 prefix delegation.
2. To use the CLI add-on feature template, edit the device template as follows:

DETAILED STEPS

Procedure

Step 1 Create a CLI add-on feature template for DHCPv6 prefix delegation.

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
b) Click **Feature Templates**.
c) Click **Add Template**.
d) Under **Select Devices**, choose the device for which you are creating the template.
e) Under **Select Template**, scroll down to the **OTHER TEMPLATES** section, and click **CLI Add-On Template**.
f) In the **Template Name** field, enter a name for the feature template.
g) In the **Description** field, enter a description for the feature template.
h) In the **CLI CONFIGURATION** area, enter the DHCPv6 configuration.

```
interface GigabitEthernet1
ipv6 dhcp client pd prefix-from-provider
ipv6 dhcp client request vendor
```

i) Click **Save**.

The CLI add-on template is displayed in the **CLI CONFIGURATION** table.

Step 2 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**.

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

c) Click **. . .** adjacent to the device template for which you want to add the CLI add-on feature template, and choose **Edit**.
d) Scroll down to **Additional Templates**, and from the **CLI Add-On Template** drop-down list, choose the CLI add-on feature template that you previously created.
e) Click **Update**.

The CLI add-on feature template contains the DHCPv6 prefix delegation configuration.

What to do next

To continue, see Configure NAT66 DIA using CLI.

Configure a NAT66 DIA route

Enable an IPv6 route with NAT66 DIA in a **Cisco VPN** template.

Every service VPN, for example, VPN 1, routes packets into the transport VPN (VPN 0) for DIA traffic.

SUMMARY STEPS

1. Configure the IPv6 route and NAT settings.
2. Complete and save the NAT66 DIA route.

DETAILED STEPS

Procedure

Step 1 Configure the IPv6 route and NAT settings.

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
b) Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x release, **Feature Templates** is titled **Feature**.

c) Edit a **Cisco VPN** template by clicking **. . .** adjacent to it, and then choosing **Edit**.
d) Click **IPv6 Route**.
e) Click **New IPv6 Route**.

Step 2 Complete and save the NAT66 DIA route.

a) In the **Prefix** field, enter an IPv6 prefix for NAT66 translation.

Global inside and outside prefixes should be unique per virtual routing and forwarding (VRF).

IPv6-prefix delegation (PD) prefix length should be equal to or less than /56.

A global outside prefix should be unique per VRF.

The inside prefix length and an outside prefix length should be the same.

Up to 250 VRFs are supported with a PD prefix of /56.

b) In the **Gateway** field, click **VPN**.
c) In the **Enable VPN** drop-down list, change the scope from **Default** to **Global**, and click **On** to enable VPN.
d) In the **NAT** drop-down list, change the scope from **Default** to **Global**, and click **On** to enable NAT66.
e) Click **Update**.

The Cisco VPN feature template contains the IPv6 route used for NAT66 DIA.

What to do next

To continue, see Verify NAT66 DIA and DIA route configuration.

Configure NAT66 DIA using stateless DHCP through Cisco Catalyst SD-WAN Manager

From Cisco Catalyst SD-WAN Manager Release 20.13.1, you can use configuration groups to configure NAT66 DIA by using stateless DHCP in Cisco SD-WAN Manager.

Procedure

Step 1 Configure NAT66 and DHCP prefix delegation in the configuration group.

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
b) Click **Add Configuration Group** to create a new configuration group or click **Edit** under **Actions** to edit an existing configuration group.
c) To edit a configuration group, click **. . .** adjacent to it, and then choose **Edit**.
d) Click **Transport Profile**.
e) Click **. . .** adjacent to the VPN feature and choose **Add Sub-Feature**.
f) Select Ethernet Interface from the drop-down list.
g) Click **NAT** > **IPv6 Settings**.
h) In the **NAT** drop-down list, change the scope from **Default** to **Global**, and toggle on NAT66.

Step 2 Configure NAT66 and DHCP prefix delegation in the configuration group.

a) Under the **NAT66** option, click **Add Nat66** and configure the **Source Prefix** and **Source VPN ID**.
b) Leave the system default value in the **Translated Source** field.
c) In the **Egress Interface** drop-down list, change the scope from **Default** to **Global**, and toggle on egress interface.
d) Click **Add**.
e) Click **Save**.

The configuration group contains the NAT66 and stateless DHCP prefix delegation settings.

What to do next

To continue, see Verify dialer interface NAT66 DIA configuration.

Configure NAT66 DIA using stateless DHCP through a feature template

From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, you can use feature templates to configure NAT66 DIA by using stateless DHCP in Cisco SD-WAN Manager.

Procedure

Step 1 Configure NAT66 and DHCP prefix delegation in the feature template.

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
b) Click **Feature Templates**.
c) Click **Add Template**.
d) Under **Select Devices**, choose the device for which you are creating the template.
e) Under **Select Template**, scroll down to the **VPN** section, and click **Cisco VPN Interface Ethernet**
f) In the **Template Name** field, enter a name for the feature template.
g) In the **Description** field, enter a description for the feature template.
h) Click **NAT** > **IPv6**.

Step 2 Configure NAT66 and DHCP prefix delegation in the feature template.

a) In the **NAT** drop-down list, change the scope from **Default** to **Global**.
b) Click **ON** to enable NAT.
c) In the **NAT Selection** drop-down list, change the scope from **Default** to **Global** and choose **NAT66**.
d) Click **New Static NAT**.
e) Configure the **Source Prefix** and **Source VPN ID**.
f) Leave the system default value in the **Translated Source Prefix** field.
g) In the **Egress Interface** drop-down list, change the scope from **Default** to **Global**, and click **Yes**.
h) Click **Add**.

Step 3 Configure NAT66 and DHCP prefix delegation in the feature template.

a) Click **Save**.

The feature template contains the NAT66 and stateless DHCP prefix delegation settings.

What to do next

To continue, see Verify dialer interface NAT66 DIA configuration.

Configure NAT66 DIA using the CLI

SUMMARY STEPS

1. Configure Static NAT Prefix Translation for NAT66 DIA
2. Configure DIA Using Stateless DHCP using CLI
3. Configure multiple links for NAT66 DIA
4. Configure DHCPv6 Prefix Delegation for NAT66 DIA

DETAILED STEPS

Procedure

Step 1 Configure Static NAT Prefix Translation for NAT66 DIA

```
interface GigabitEthernet1
 ip address 10.1.15.15 255.0.0.0
 no ip redirects
 load-interval 30
 negotiation auto
 nat66 outside
 ipv6 address 2001:DB8:A1:F::F/64
 no ipv6 redirects
 service-policy output shape_GigabitEthernet1
!
nat66 prefix inside 2001:DB8:380:1::/80 outside 2001:DB8:A1:F:0:1::/80 vrf 1
nat66 prefix inside 2001:DB8:A14:18::/80 outside 2001:DB8:A1:F::/80 vrf 1
nat66 route vrf 1 2001:DB8:A14:19::/64 global
nat66 route vrf 1 2001:DB8:3D0:1::/64 global
```

Step 2 Configure DIA Using Stateless DHCP using CLI

```
interface GigabitEthernet1
 nat66 outside
 ip address 10.1.15.15 255.0.0.0
 ipv6 address autoconfig
 ipv6 enable
 ipv6 nd autoconfig default-route
 no ip redirects
 load-interval 30
 negotiation auto
 no ipv6 redirects
 service-policy output shape_GigabitEthernet1
!
nat66 prefix inside 2001:a14:18::/64 outside interface GigabitEthernet1 vrf 1
nat66 prefix inside 2001:a14:18::/64 outside interface GigabitEthernet1
```

Step 3 Configure multiple links for NAT66 DIA

From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, you can configure multiple egress interfaces for NAT66 DIA.

Here is an example of configuring NAT66 DIA with two interfaces, GigabitEthernet1 and GigabitEthernet4:

```
interface GigabitEthernet1
 no shutdown
 ipv6 address 2001:a1:f::f/64
 ipv6 nd ra suppress all
 no mop enabled
 no mop sysid
 negotiation auto
 nat66 outside
!
interface GigabitEthernet4
 no shutdown
 ipv6 address 2001:a0:14::f/64
 ipv6 enable
 ipv6 nd ra suppress all
 no mop enabled
 no mop sysid
 negotiation auto
 nat66 outside
```

```
!
nat66 prefix inside 2001:a14:18:0::/64 outside 2001:a1:f::/64 vrf 1 egress-interface GigabitEthernet1
nat66 prefix inside 2001:a14:18:0::/64 outside 2001:a0:14::/64 vrf 1 egress-interface GigabitEthernet4
nat66 prefix inside FC00:1:2:3::/80 outside 3001:a1:5::/80 vrf 100
nat66 route vrf 1 2001:a0:5::/64 global
nat66 route vrf 100 ::/0 global
```

For more information, see the nat66 prefix command in the Cisco IOS XE SD-WAN Qualified Command Reference Guide.

Step 4 Configure DHCPv6 Prefix Delegation for NAT66 DIA

```
interface GigabitEthernet1
ip address 10.1.15.15 255.0.0.0
no ip redirects
load-interval 30
negotiation auto
nat66 outside
ipv6 address dhcp
ipv6 address autoconfig
ipv6 enable
ipv6 nd autoconfig default-route
ipv6 dhcp client pd prefix-from-provider
ipv6 dhcp client request vendor
arp timeout 1200
no mop enabled
no mop sysid
service-policy output shape_GigabitEthernet1
!
nat66 prefix inside 2001:DB8:10:1::/64 outside prefix-from-provider vrf 1
nat66 prefix inside 2001:DB8:100:1::/64 outside prefix-from-provider vrf 100
nat66 prefix inside 2001:DB8:101:1::/64 outside prefix-from-provider vrf 101
nat66 route vrf 1 2001:DB8:A14:19::/64 global
nat66 route vrf 1 2001:DB8:3D0:1::/64 global
nat66 route vrf 100 ::/0 global
nat66 route vrf 101 ::/0 global
```

The CLI configuration includes NAT66 DIA static translation.

What to do next

To continue, see Verify dialer interface NAT66 DIA configuration.

Verify NAT66 DIA and DIA route configuration

Objective

Use the following commands and information to verify NAT66 DIA and DIA route configuration.

Display NAT66 Prefix Translation Entries

```
Device# show nat66 prefix
Prefixes configured: 2
NAT66 Prefixes
Id: 1 Inside 2001:DB8:380:1::/80 Outside 2001:DB8:A1:F:0:1::/80
Id: 2 Inside 22001:DB8:A14:18::/80 Outside 2001:DB8:A1:F::/80
```

Verify NAT66 DIA Routes

```
Device# show nat66 route-dia
Total interface NAT66 DIA enabled count [1]
route add [1] addr [2001:DB8:A14:19::] vrfid [2] prefix len [64]
route add [1] addr [2001:DB8:3D0:1::] vrfid [2] prefix len [64]
```

Display NAT66 Neighbor Discovery

```
Device# show nat66 nd
NAT66 Neighbor Discovery

ND prefix DB:
  2001:DB8:A1:F::/80
  2001:DB8:A1:F:0:1::/80
  2001:DB8:A1:F:1::/64
  2001:DB8:A1:F:2::/64
  2001:DB8:A1:F:3::/64

ipv6 ND entries:
  2001:DB8:A1:F::F
  2001:DB8:A1:F::11
```

Verify NAT66 Global Statistics for Translated Packets

```
Device# show nat66 statistics
NAT66 Statistics

Global Stats:
   Packets translated (In -> Out)
      : 7
   Packets translated (Out -> In)
      : 7
```

Verify NAT66 DIA Using Stateless DHCP

To view the binding entry:

```
Device# show platform hardware qfp active feature nat66 datapath bind-dump
bind 0xdf612cc0 v6outaddr 2001:A1:F::96 v6addr 2001:A14:18::96 vrfid 3 domain 0 create time
 513092 refcnt 0 flags 0x0 mapping 0xdf54ba40 last_use_ts 513186 output_ifhandle 0x1b
```

Display NAT66 Platform for Each Prefix Counter for Inside and Outside Translations

```
Device# show platform hardware qfp active feature nat66 datapath prefix
prefix hasht 0x89628400 max 2048 chunk 0x8c392bb0 hash_salt 719885386
NAT66 hash[1] id(1) len(64) vrf(0) in: 2001:db8:ab01:0000:0000:0000:0000:0000 out:
2001:db8:ab02:0000:0000:0000:0000:0000 in2out: 7 out2in: 7
```

Verify NAT66 Platform Global Counters

```
Device# show platform software nat66 fp active statistics
QFP Stats:
Interface:
    Add: 2, Ack: 2, Err: 0
    Mod: 0, Ack: 0, Err: 0
    Del: 0, Ack: 0, Err: 0
Prefix Trans:
    Add: 5, Ack: 5, Err: 0
    Mod: 0, Ack: 0, Err: 0
    Del: 0, Ack: 0, Err: 0
AOM Stats:
```

```
Interface:
    Add: 2, Err: 0
    Mod: 0, Err: 0
    Del: 0, Err: 0
    Free: 0, Err: 0
Prefix Translation:
    Add: 5, Err: 0
    Mod: 0, Err: 0
    Del: 0, Err: 0
    Free: 0, Err: 0
DB Stats:
  Interface:
    Add: 2, Err: 0
    Mod: 0, Err: 0
    Del: 0, Err: 0
  Prefix Translations:
    Add: 5, Err: 0
    Mod: 0, Err: 0
    Del: 0, Err: 0
Message RX Stats:
  Interface:
    Add: 2
```

Configuration example for NAT66 DIA

Objective

This reference provides configuration examples for NAT66 DIA.

The following is an end-to-end configuration example for NAT66 DIA:

End-to-end configuration example

```
interface GigabitEthernet1
ip address 10.1.15.15 255.0.0.0
no ip redirects
load-interval 30
negotiation auto
nat66 outside
ipv6 address dhcp
ipv6 address autoconfig
ipv6 enable
ipv6 nd autoconfig default-route
ipv6 dhcp client pd prefix-from-provider
ipv6 dhcp client request vendor
arp timeout 1200
no mop enabled
no mop sysid
service-policy output shape_GigabitEthernet1
!
nat66 prefix inside 2001:DB8:380:1::/80 outside 2001:DB8:A1:F:1::/80 vrf 1
nat66 prefix inside 2001:DB8:A14:18::/80 outside 2001:DB8:A1:F::/80 vrf 1
nat66 prefix inside 2001:DB8:10:1::/64 outside prefix-from-provider vrf 1
nat66 prefix inside 2001:DB8:100:1::/64 outside prefix-from-provider vrf 100
nat66 prefix inside 2001:DB8:101:1::/64 outside prefix-from-provider vrf 101
nat66 route vrf 1 2001:DB8:A14:19::/64 global
nat66 route vrf 1 2001:DB8:3D0:1::/64 global
nat66 route vrf 100 ::/0 global
nat66 route vrf 101 ::/0 global
```

End-to-end configuration example with multiple links

```
interface GigabitEthernet3
 no shutdown
 ipv6 address 2001:a1:f::f/64
 ipv6 nd ra suppress all
 no mop enabled
 no mop sysid
 negotiation auto
 nat66 outside
!
interface GigabitEthernet4
 no shutdown
 ipv6 address 2001:a0:14::f/64
 ipv6 enable
 ipv6 nd ra suppress all
 no mop enabled
 no mop sysid
 negotiation auto
 nat66 outside
!
nat66 prefix inside 2001:a14:18:0::/64 outside 2001:a1:f::/64 vrf 1 egress-interface
GigabitEthernet3
nat66 prefix inside 2001:a14:18:0::/64 outside 2001:a0:14::/64 vrf 1 egress-interface
GigabitEthernet4
nat66 prefix inside FC00:1:2:3::/80 outside 3001:a1:5::/80 vrf 100
nat66 route vrf 1 2001:a0:5::/64 global
nat66 route vrf 100 ::/0 global
```

NAT66 DIA Route redistribution

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

Information about NAT66 route redistribution

Route redistribution shares routing information between multiple domains running different routing protocols. When you configure NAT66 DIA route redistribution, you enable redistribution of the translated IPv6 addresses into Open Shortest Path First (OSPFv3) or the Border Gateway Protocol (BGP).

NAT66 route redistribution information

When the traffic from a remote site traverses the overlay network or tunnels, the NAT66 outside address translation service translates the remote host source IP address (outside host). The translation occurs before the traffic is sent to the LAN (VPN1) side of the network. If route redistribution is configured, the NAT outside pool address or routes are redistributed to the LAN side of the network through OSPFv3 or BGP protocols. Thus, the inside host from one network is aware of the path to reach remote hosts in another network running a different routing protocol.

NAT66 route redistribution applies to the following types of routes that it learns either locally or from its routing peers:

- BGP
- OSPFv3

You can configure NAT66 DIA route redistribution using CLI-based configuration groups or feature templates.

Configure NAT66 DIA route redistribution using a feature template

Feature template configuration

From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, you can use feature templates in Cisco SD-WAN Manager to configure NAT66 DIA route redistribution into BGP or OSPFv3 protocols.

Configure NAT66 DIA route redistribution into BGP using a feature template

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

Procedure

Step 1 Configure NAT route redistribution in the BGP feature template.

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
b) Click **Feature Templates**.
c) Click **Add Template**.
d) Under **Select Devices**, choose the device for which you are creating the template.
e) Under **Select Template**, scroll down to the **OTHER TEMPLATES** section, and click **Cisco BGP**.
f) In the **Template Name** field, enter a name for the feature template.
g) In the **Description** field, enter a description for the feature template.
h) Click **UNICAST ADDRESS FAMILY**.

Step 2 Configure NAT route redistribution in the BGP feature template.

a) Click **IPv6**.
b) Click **New Redistribute**.
c) In the **Protocol** drop-down list, choose **NAT**.
d) Click **Add**.
e) Click **Save**.

The BGP feature template includes the NAT route redistribution configuration.

What to do next

To continue, see Verify NAT66 DIA and DIA route configuration.

Configure NAT66 DIA route redistribution into OSPFv3 using a feature template

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

Procedure

Step 1 Configure NAT route redistribution in the OSPFv3 feature template.

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
b) Click **Feature Templates**.
c) Click **Add Template**.
d) Under **Select Devices**, choose the device for which you are creating the template.
e) Under **Select Template**, scroll down to the **OTHER TEMPLATES** section, and click **Cisco OSPFv3**.
f) In the **Template Name** field, enter a name for the feature template.
g) In the **Description** field, enter a description for the feature template.
h) Click **IPv6**.

Step 2 Configure NAT route redistribution in the OSPFv3 feature template.

a) In the **Redistribute** tab, click **New Redistribute**.
b) In the **Protocol** drop-down list, choose **nat-route**.
c) Click **Add**.
d) Click **Save**.

The OSPFv3 feature template includes the NAT route redistribution configuration.

What to do next

To continue, see Verify NAT66 DIA and DIA route configuration.

Configure NAT66 DIA route redistribution using CLI based configuration group

From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, you can use a CLI based configuration group in Cisco SD-WAN Manager to configure NAT66 DIA route redistribution into BGP or OSPFv3 protocols.

Configure NAT66 DIA route redistribution into BGP using CLI based configuration group

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

SUMMARY STEPS

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click **Add CLI based Configuration Group**.
3. Enter a name for the CLI based configuration group.
4. In the **Solution** drop-down list, choose **sdwan**.
5. In the **Description** field, enter a description for the CLI based configuration group.
6. Click **Next**.
7. Enter the CLI based configuration in the field.
8. Click **Save**.

DETAILED STEPS

Procedure

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

Step 2 Click **Add CLI based Configuration Group**.

Step 3 Enter a name for the CLI based configuration group.

Step 4 In the **Solution** drop-down list, choose **sdwan**.

Step 5 In the **Description** field, enter a description for the CLI based configuration group.

Step 6 Click **Next**.

Step 7 Enter the CLI based configuration in the field.

a) Configure a BGP routing process, and enter the router configuration mode for the specified routing process. Use the *autonomous-system-number* argument to specify an integer, from 0 and 65534, that identifies the device to other BGP speakers:

```
router bgp autonomous-system-number
```

b) Configure the router ID as the identifier of the local device running BGP. Use the *ip-address* argument to specify a router IP address within the network:

```
bgp router-id ip-address
```

c) Specify the IPv6 address family and enter the address family configuration mode:

```
address-family ipv6 unicast vrf vrf-name
```

d) Add the IP address of the neighbor in the specified AS to the IPv6 multiprotocol BGP neighbor table of the local device:

```
neighbor ip-address remote-as autonomous-system-number
```

e) Enable the neighbor to exchange prefixes for the IPv6 unicast address family with the local device:

```
neighbor ip-address activate
```

f) Redistribute NAT route:

```
redistribute nat-route
```

g) Exit address family configuration mode and return to privileged EXEC mode:

```
exit-address-family
```

Step 8 Click **Save**.

The CLI based configuration group contains the BGP route redistribution configuration for NAT66 DIA.

Here's an example to configure NAT66 DIA route redistribution into BGP:

```
router bgp 15
bgp router-id 10.1.1.1
address-family ipv6 unicast vrf 1
  neighbor 2001:a14:18::64 remote-as 2
  neighbor 2001:a14:18::64 activate
  redistribute nat-route
```

```
  exit-address-family
!
```

What to do next

To continue, see Verify NAT66 DIA and DIA route configuration.

Configure NAT66 DIA route redistribution into OSPFv3 using CLI based configuration group

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

SUMMARY STEPS

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click **Add CLI based Configuration Group**.
3. Enter a name for the CLI based configuration group.
4. In the **Solution** drop-down list, choose **sdwan**.
5. In the **Description** field, enter a description for the CLI based configuration group.
6. Click **Next**.
7. Create the CLI based configuration group.
8. Configure and save OSPFv3 route redistribution.
9. Click **Save**.

DETAILED STEPS

Procedure

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

Step 2 Click **Add CLI based Configuration Group**.

Step 3 Enter a name for the CLI based configuration group.

Step 4 In the **Solution** drop-down list, choose **sdwan**.

Step 5 In the **Description** field, enter a description for the CLI based configuration group.

Step 6 Click **Next**.

Step 7 Create the CLI based configuration group.

a) Configure an interface:

```
interface interface-name
```

b) Provide the OSPFv3 process ID, and specify **point-to-point** as the network type to which the interface is to connect:

```
ospfv3 process-id network point-to-point
```

c) Configure the OSPFv3 area for the IPv6 address family:

```
ospfv3 process-id ipv6 area area-id
```

d) Enter the router configuration mode and provide the OSPFv3 process ID:

```
router ospfv3 process-id
```

e) Configure the router ID as the identifier of the local device running OSPFv3. Use the *ip-address* argument to specify a router IP address within the network:

```
router-id ip-address
```

Step 8 Configure and save OSPFv3 route redistribution.

a) Specify the IPv6 address family and enter the address family configuration mode:

```
address-family ipv6 unicast
```

b) Configure the device to send a syslog message when an OSPFv3 neighbor goes up or down:

```
log-adjacency-changes
```

c) Redistribute the connected routes into OSPFv3:

```
redistribute connected
```

d) Redistribute NAT route:

```
redistribute nat-route
```

e) Exit address family configuration mode and return to privileged EXEC mode:

```
exit-address-family
```

Step 9 Click **Save**.

The CLI based configuration group contains the OSPFv3 route redistribution configuration for NAT66 DIA.

Here's an example to configure NAT66 DIA route redistribution into OSPFv3:

```
interface GigabitEthernet5
ospfv3 1 network point-to-point
ospfv3 1 ipv6 area 0
    router ospfv3 1
    router-id 10.1.1.1
address-family ipv6 unicast
  log-adjacency-changes
  redistribute connected
  redistribute nat-route
  exit-address-family
!
```

What to do next

To continue, see Verify NAT66 DIA and DIA route configuration.

Dialer interfaces with NAT66 DIA

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

Information about dialer interface with NAT66 DIA

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

Dialer interface information

A dialer interface specifies how to handle dialer traffic from clients, including default routing information, the encapsulation protocol, and the dialer pool to use. Dialer interfaces provide an abstraction layer from the physical interfaces that actually perform the dial-up. This feature provides support for Point-to-Point Protocol (PPP) dialer interfaces for the NAT66 DIA.

The following dialer interfaces are supported:

- Point-to-Point Protocol over Ethernet (PPPoE)
- Point-to-Point Protocol over Asynchronous Transfer Mode (PPPoA)
- Point-to-Point Protocol over Ethernet over Asynchronous Transfer Mode (PPPoEoA)

PPP connects multiple users over an ethernet local area network to a remote site through common customer premises equipment. PPP is commonly used in a broadband aggregation, such as by digital subscriber line (DSL). PPP provides authentication with the Challenge Handshake Authentication Protocol (CHAP) or password authentication protocol (PAP) while physical interfaces don't perform authentication.

For more information about configuring PPPoE, see the Configuring PPPoE section in the *Cisco Catalyst SD-WAN Systems and Interfaces Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x*.

Benefits of using a dialer interface with NAT66 DIA

- Allows physical interfaces to take on different characteristics based on incoming or outgoing call requirements
- Supports route-based as well as data-policy-based configuration with NAT66 DIA

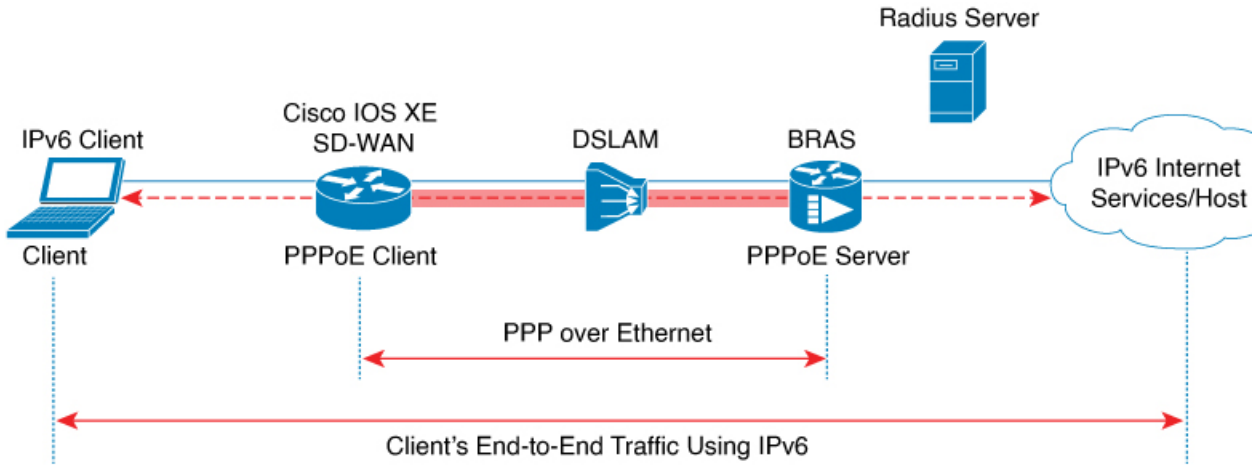
Workflow for IPv6 traffic through a NAT DIA dialer interface

Summary

The following diagram describes how IPv6 client traffic gets routed over a dialer interface for reaching IPv6 internet sites and services.

Workflow for NAT66 DIA Dialer Interface Support

Workflow



Restrictions for using a dialer interface with NAT66 DIA

The following restrictions apply to using a dialer interface with NAT66 DIA:

- DIA support:

  Only NAT66 DIA is supported with dialer interfaces.

- Service-side NAT66:

  No support for service-side NAT66 with dialer interfaces.

- PPPoE jumbo frames:

  PPPoE jumbo frames are limited to 1800 bytes when using a CLI add-on template.

- PPPoA dialer interface encapsulations:

  There is no support for configuring the following PPPoA dialer interface encapsulations: AAL5MUX, AAL5SNAP, AAL5NLPID, or bridge-dot1q using Cisco SD-WAN Manager feature templates. If you want to configure these PPPoA encapsulations, you need to configure the encapsulations using a CLI template.

- DIA tracker:

  NAT66 DIA tracker is not supported for a dialer interface with an IP unnumbered interface.

- DIA path preference:

  NAT66 DIA path preference is not supported with loopback on a WAN interface.

Configure a dialer interface with NAT66 DIA

Minimum support release: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

Configuration overview

You can configure a dialer interface with NAT66 DIA using configuration groups or by using a CLI template.

Configure a dialer interface with NAT66 DIA using configuration groups

Minimum support release: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

SUMMARY STEPS

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Under **Transport and Management Profile**, click **…** adjacent to an interface under the VPN 0 feature.
3. Click **Add Sub Feature** and select the one of the following dialer interfaces from the drop-down list:
4. Configure the options for DSL PPPoE or DSL PPPoA.
5. Click **Save**.

DETAILED STEPS

Procedure

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

For more information about creating a configuration group, see Configuration Group Workflows.

Step 2 Under **Transport and Management Profile**, click **…** adjacent to an interface under the VPN 0 feature.

Step 3 Click **Add Sub Feature** and select the one of the following dialer interfaces from the drop-down list:

- DSL PPPoE
- DSL PPPoA

Step 4 Configure the options for DSL PPPoE or DSL PPPoA.

For more information, see the sections DSL PPPoE or DSL PPPoA in Transport and Management Profile.

Step 5 Click **Save**.

The configuration group contains the dialer interface NAT66 DIA settings.

What to do next

To continue, see Verify dialer interface NAT66 DIA configuration.

Configure a dialer interface with NAT66 DIA using a CLI template

Minimum support release: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

For more information on using CLI templates, see CLI Templates and CLI Add-On Feature Templates.

SUMMARY STEPS

1. Configure a PPPoE dialer interface with NAT66 DIA enabled.
2. Enable **nat66 outside** over a dialer interface.
3. Configure a NAT66 DIA route for a service-side VPN.

DETAILED STEPS

Procedure

Step 1 Configure a PPPoE dialer interface with NAT66 DIA enabled.

```
                        interface interface-type-number
 pppoe enable group global
 pppoe-client dial-pool-number dialer-pool-number
!
interface Dialer dialer-number
 mtu bytes
 ipv6 address negotiated
 ipv6 mtu bytes
 nat66 outside
 encapsulation encapsulation-type
 ipv6 tcp adjust-mss bytes
 dialer pool dialer-pool-number
 dialer down-with-vInterface
 ppp chap hostname hostname
 ppp chap password password
 ppp authentication chap callin
 ppp ipcp route default
 service-policy output shape_Dialer dialer-number
```

Step 2 Enable **nat66 outside** over a dialer interface.

```
nat66 outside
nat66 prefix inside ipv6-address outside interface Dialer interface name vrf Sevice VPN number
nat66 prefix inside ipv6-address outside interface Dialer interface name
```

Step 3 Configure a NAT66 DIA route for a service-side VPN.

For more information on configuring a NAT DIA route for a service-side VPN, see Configure a NAT DIA Route.

or

Configure a NAT66 DIA route for a service-side VPN using a centralized data policy.

```
nat66 route vrf vrf-id
    route-prefix
    prefix-mask global
```

The CLI template contains the dialer interface NAT66 DIA configuration.

Note Deleting the dialer interface in the same transaction as NAT66 Mapping with Pool-overload-config, generates an extra no NAT66 configuration. Remove each NAT66 configuration separately using different transactions as folllows:

```
Device(config)# no nat66 inside source list global-list pool natpool-Dialer100-0 overload
egress-interface Dialer100
Device(config)# commit

Device(config)# no interface Dialer100
Device(config)# commit
```

Here's an example of configuring a PPPoE dialer interface with NAT66 DIA:

```
interface Dialer100
 mtu 1492
 ipv6 address negotiated
 nat66 outside
 encapsulation ppp
 ipv6 tcp adjust-mss 1452
 dialer pool 100
 dialer down-with-vInterface
 endpoint-tracker tracker-google
 ppp authentication chap callin
 ppp chap hostname branch1.ppp1
 ppp chap password 7 01100F175804
 ppp ipcp route default
 service-policy output shape_GigabitEthernet0/0/1
!
interface GigabitEthernet0/0/1
 no ipv6 redirects
 pppoe enable group global
 pppoe-client dial-pool-number 100
!
sdwan
 interface Dialer100
  tunnel-interface
   encapsulation ipsec weight 1
   color mpls restrict
  exit
 exit
nat66 prefix inside 2001:A14:18::/80 outside interface Dialer100 vrf 100
nat66 route vrf 100 ::/0 global
```

What to do next

To continue, see Verify dialer interface NAT66 DIA configuration.

Verify a dialer interface configuration for NAT66 DIA

Objective

Use the following commands and information to verify a dialer interface configuration for NAT66 DIA.

The following sections provide information on verifying a dialer interface configuration.

Verify NAT66 DIA Routes

```
Device# show nat66 route-dia
Total interface NAT66 DIA enabled count [1]
route add [1] addr [2001:A14:18::] vrfid [2] prefix len [64]
route add [1] addr [2001:A14:19::] vrfid [2] prefix len [64]
```

Display NAT66 Platform for Each Prefix Counter for Inside and Outside Translations

```
Device# show platform hardware qfp active feature nat66 datapath prefix
prefix hasht 0x89628400 max 2048 chunk 0x8c392bb0 hash_salt 719885386
NAT66 hash[1] id(1) len(64) vrf(0) in: 2001:0a14:0018:0000:0000:0000:0000:0000 out:
2001:db8:ab02:0000:0000:0000:0000:0000 in2out: 7 out2in: 7
```

Display Your PPPoE Sessions

In this sample output from the **show pppoe session** command, the PPPoE dialer interface displays as `UP`.

```
Device# show pppoe session
     1 client session

Uniq ID  PPPoE  RemMAC          Port                    VT  VA         State
           SID  LocMAC                                      VA-st      Type
    N/A    391  84b2.61cc.9903  Gi0/0/1.100          Di100 Vi2        UP
                c884.a1f4.b981  VLAN: 100                  UP
```

The following is a sample output from the **show ppp all** command:

```
Device# show ppp all
Interface/ID OPEN+ Nego* Fail-     Stage    Peer Address    Peer Name
------------ -------------------- -------- --------------- --------------------
Vi2          LCP+ IPV6CP+ CDPCP-   LocalT   0.0.0.0         SDWAN-AGGREGE
```

Verify PPP Negotiation Information

In this sample output from the **show interfaces Dialer** command, `Dialer100` is up and the line protocol is up.

```
Device# show ipv6 interface Dialer100
Dialer100 is up, line protocol is up
 IPv6 is enabled, link-local address is FE80::72EA:1AFF:FE1E:C800
  No Virtual link-local address(es):
  Global unicast address(es):
2001:a0:14:0:8132:C37E:1172:A9C7, subnet is 2001:a0:14:0::/64
valid lifetime 2587577 preferred lifetime 600377
Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
    FF02::1:FF78:5E00
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

Configuration example for using a dialer interface with NAT66 DIA

Objective

This reference provides configuration examples for using a dialer interface with NAT66 DIA.

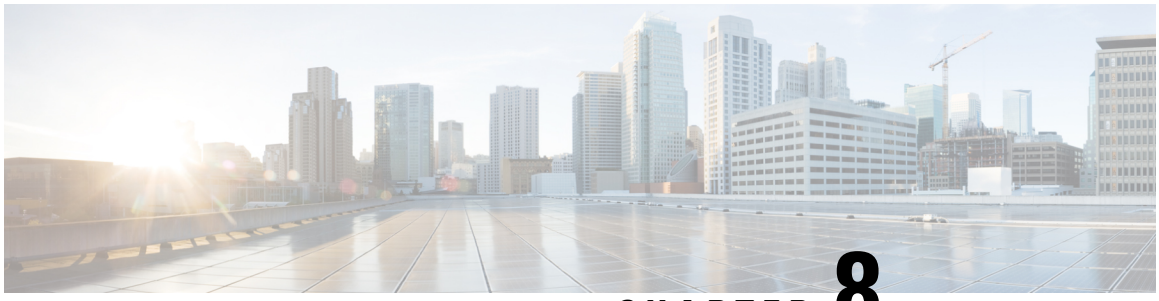
This example shows the configuration of a dialer interface.

Configure Static NAT Prefix Translation for NAT66 DIA

```
interface Dialer100
    nat66 outside
!
nat66 prefix inside 2001:DB8:380:1::/80 outside 2001:DB8:A1:F:0:1::/80 vrf 1
nat66 prefix inside 2001:DB8:A14:18::/80 outside 2001:DB8:A1:F::/80 vrf 1
nat66 route vrf 1 2001:DB8:A14:19::/64 global
nat66 route vrf 1 2001:DB8:3D0:1::/64 global
```

Configure DIA Using Stateless DHCP using CLI

```
interface Dialer100
     nat66 outside
!
nat66 prefix inside 2001:a14:18::/64 outside interface Dialer100 vrf 1
nat66 prefix inside 2001:a14:18::/64 outside interface Dialer100
```



CHAPTER 8

Feature history: Site-local failover for NAT DIA

This reference provides information about the features and enhancements that have been introduced for Site-local failover for NAT DIA across different software releases.

Site-Local Failover for NAT DIA

Table 31: Feature History

Feature Name	Release Information	Description
Support for Site-Local Failover for NAT DIA	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	Support for NAT DIA traffic failover in sites with more than one edge device. The support for same-site NAT DIA local failover works with NAT44 and NAT66 by tunneling the traffic from one edge device to another edge device that has NAT DIA access within a site.

- Information About Site-Local Failover for NAT DIA, on page 175
- Benefits of Site-Local Failover for NAT DIA, on page 177
- Restrictions for Site-Local Failover for NAT DIA, on page 177
- Configure Site-local failover for NAT DIA, on page 177
- Verify Site Local Failover For NAT DIA, on page 179

Information About Site-Local Failover for NAT DIA

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.16.1a, site-local failover for NAT DIA introduces a method for NAT (NAT44 and NAT66) DIA traffic to failover to other edges within the same site that are configured for NAT DIA in the event that the primary NAT DIA circuit goes down. This feature supports NAT DIA traffic failover in sites with multiple edge devices using dedicated Layer 3 standard GRE tunnels.

Details

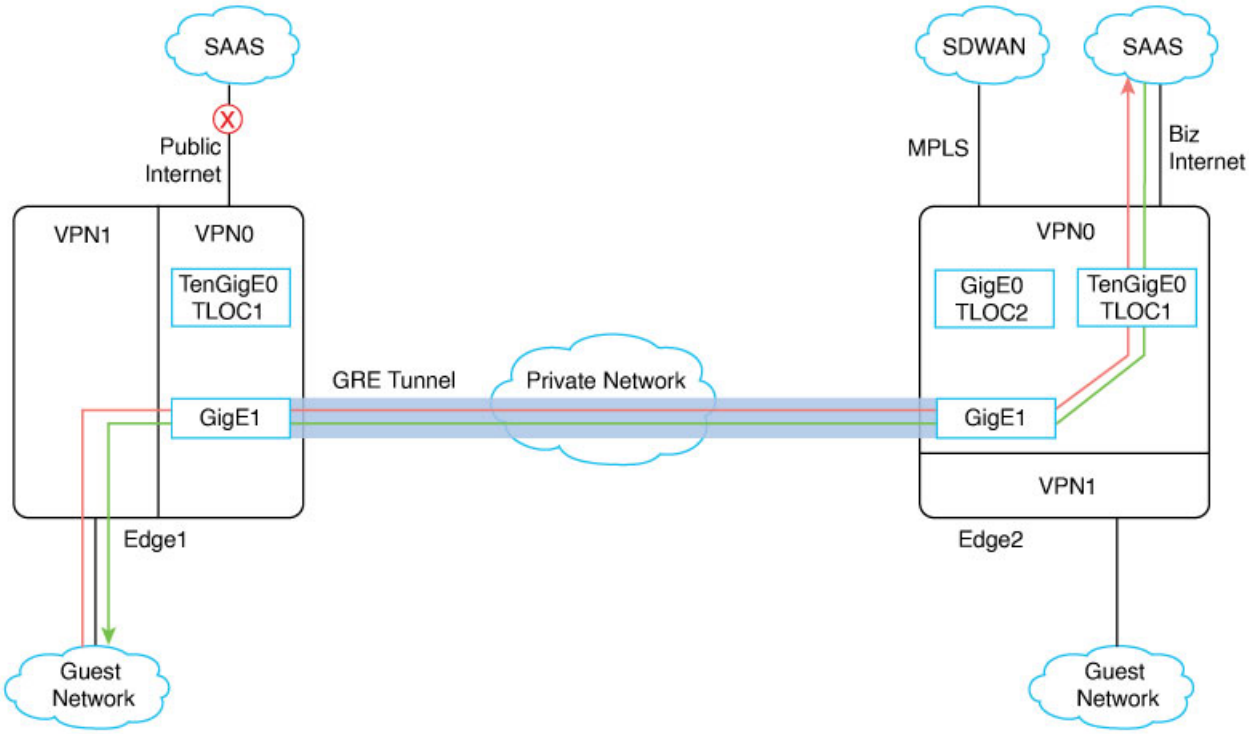
Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.16.1a and Cisco Catalyst SD-WAN Manager Release 20.16.1

In Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and earlier, NAT DIA was managed by directing specific types of network traffic directly to the internet from a local branch or site through configured exit DIA interfaces. In the absence of a local exit DIA interface, the NAT DIA traffic was routed through a central data center.

With this release, you can enable site-local redundancy for NAT DIA, which also works with existing Layer 2 and Layer 3 TLOC extension-based deployments. The DIA traffic initially fails over via a GRE Tunnel interface to the site-local redundant router to check for an available TLOC that is capable of DIA. If TLOC is not available, the DIA traffic uses NAT fallback as backup. The edge device detects the existence of a DIA interface based on endpoint trackers.

To enable the NAT-DIA site-local redundancy solution, use a standard dedicated GRE tunnel interface, which carries only the NAT DIA traffic to the site-local redundant Cisco Catalyst SD-WAN edge devices. The source interface of the tunnel on either edge device can be a physical interface or a subinterface on the transport VPN. NAT DIA traffic is routed between the two edges in the same site. We recommend that you use port-channels as the traffic is diverted via the GRE tunnel even for flows redirected to hub sites. Consider the link bandwidth while choosing the underlay interface for the GRE Tunnel. Routing is not required in the GRE tunnel overlay.

Figure 10: Workflow of Site-Local Failover for NAT DIA



For example, when NAT DIA from Edge1 is unavailable, the traffic is transported over the Layer 3 standard GRE tunnel interface to Edge2. Edge2, which is configured as the router for site-local failover, decapsulates the incoming traffic and forwards it to the interface enabled with NAT DIA, *TenGigE0 TLOC1*. Similarly, return traffic from *TenGigE0 TLOC1* which is identified as the NAT DIA traffic which arrived over the GRE tunnel, is translated and forwarded, over the Layer 3 standard GRE tunnel interface to Edge1. Edge1 then decapsulates the incoming traffic and forwards it to the source interface in service VPN.

Benefits of Site-Local Failover for NAT DIA

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.16.1a, site-local failover for NAT DIA introduces a method for NAT (NAT44 and NAT66) DIA traffic to failover to other edges within the same site that are configured for NAT DIA in the event that the primary NAT DIA circuit goes down. This feature supports NAT DIA traffic failover in sites with multiple edge devices using dedicated Layer 3 standard GRE tunnels.

Benefits

- Site-local failover for NAT DIA with TLOC extension: You can configure site-local failover for NAT DIA with existing Layer 2 and Layer 3 TLOC extension-based deployments.
- Improved performance in application SLAs: Implementing site-local failover for NAT DIA leads to reduced latency, jitter, drops, and decreased cost.

Restrictions for Site-Local Failover for NAT DIA

Restrictions for site-local failover for NAT DIA.

- Overlapping subnets: Subnets originating from different VPNs during failover must be unique and cannot have the same host IP.
- GRE tunnel: In Cisco IOS XE Catalyst SD-WAN Release 17.16.1a, only one GRE tunnel is supported currently irrespective of number of TLOC extensions between the edges devices in the same site.
- Packets from transport VPN 0: Site-local failover does not support packets originating from transport VPN 0.
- Centralized data policy: Site-local failover is supported only with NAT DIA centralized data policy.

Configure Site-local failover for NAT DIA

Before you begin

- Create a GRE tunnel interface between the edge devices. For information about configuring GRE tunnels, see GRE Over IPsec Tunnels.
- Configure the centralized data policy to enable NAT DIA. For more information, see NAT Fallback on Cisco IOS XE Catalyst SD-WAN Devices.

You can configure site-local failover for NAT DIA by using the **site-local-redundancy** command in the centralized data policy by using CLI commands.

For more information about using CLI templates, see CLI Templates.

Note By default, CLI templates execute commands in global config mode.

This section provides example CLI configurations to configure site-local failover for NAT DIA:

Procedure

Step 1 Configure the GRE Tunnel interface using the site-local-redundancy command.

For more information about this command, see the action (centralized policy) command in the Cisco Catalyst SD-WAN Qualified Command Reference guide.

a) Configure Edge1 for site-local redundancy. To configure NAT DIA failover for NAT44, use an IPv4 address, and for NAT66, use an IPv6 address.

```
interface GRE-tunnel-name
 description variable-name
 ip address ip-address-of-edge1
 ip mtu mtu-size
 site-local-redundancy
 keepalive keepalive-value
 tunnel source source-interface-name
 tunnel destination interface-ip-address-of-edge2
end
!
```

b) Configure Edge2 for site-local redundancy. To configure NAT DIA failover for NAT44, use an IPv4 address, or for NAT66, use an IPv6 address.

```
interface GRE-tunnel-name
 description variable-name
 ip address ip-address-of-edge2
 ip mtu mtu-size
 site-local-redundancy
 keepalive keepalive-value
 tunnel source source-interface-name
 tunnel destination interface-ip-address-of-edge1
end
!
```

Step 2 Configure the centralized data policy for NAT DIA by using the site-local-redundancy command

```
policy
 data-policy data-policy-name
  vpn-list list-name
   sequence sequence-number
    match source-data-prefix-list data-prefix list-name
    !
    action accept
     count vpn-list-name
     nat use-vpn 0
     nat fallback
     nat site-local-redundancy     !
   !
   default-action accept
```

```
 !
!
```

Here's the complete example to configure the edge devices in the same site and the centralized data policy for NAT44:

Configure Edge1. To configure NAT DIA failover for NAT44, use an IPv4 address, or for NAT66, use an IPv6 address.

```
interface Tunnel15000561
 description GRE Tunnel Interface for NAT-DIA fallback
 ip address 192.0.2.1
 ip mtu 1500
 site-local-redundancy
 keepalive 6 3
 tunnel source GigabitEthernet6
 tunnel destination 192.0.2.2
end
!
```

Configure Edge2. To configure NAT DIA failover for NAT44, use an IPv4 address, and for NAT66, use an IPv6 address.

```
interface Tunnel15000561
 ip address 192.0.2.2
 ip mtu 1500
 site-local-redundancy
 keepalive 6 3
 tunnel source GigabitEthernet6
 tunnel destination 192.0.2.1
end
!
```

Configure the centralized data policy to enable site-local failover by using the **site-local-redundancy** command.

```
policy
 data-policy same-site-nat-dia-fallback-site-1
  vpn-list nat-dia-vpn-1
   sequence 1
    match
     source-data-prefix-list same-site-nat-dia-site-1
    !
    action accept
     count ss-nat-dia-s1
     nat use-vpn 0
     nat fallback
     nat site-local-redundancy
    !
   !default-action accept
  !
 !
```

Verify Site Local Failover For NAT DIA

Verify the site-local failover for NAT DIA.

Verify NAT DIA and Site-Local Failover Status

```
#show platform hardware qfp active feature nat datapath basecfg | inc DIA

NAT DIA enabled
NAT DIA mutliple methods disabled
#show platform software sdwan slr database
Status : True
------------------------------------------------------------
Index Ifname Ifindex Valid Status
------------------------------------------------------------
0 Tunnel15000561 26 True True
```

Verify Configuration for Edge1

```
#show platform hardware qfp active feature nat datapath basecfg | inc DIA
NAT DIA enabled
NAT DIA mutliple methods disabled

#show platform software sdwan slr database
Status : True
------------------------------------------------------------
Index  Ifname          Ifindex   Valid   Status
------------------------------------------------------------
0     Tunnel15000561    26      True    True

#show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
tcp  172.25.12.1:5062      172.25.12.1:48670     4.2.2.2:80            4.2.2.2:80
icmp 172.25.12.1:197       198.51.100.4:197         8.8.8.8:197           8.8.8.8:197
Total number of translations: 2
```

After the local breakout from edge1 device goes down:

```
#show ip nat translations
Total number of translations: 0

#show platform software sdwan slr database
Status : True
------------------------------------------------------------
Index  Ifname          Ifindex   Valid   Status
------------------------------------------------------------
0     Tunnel15000561    25      True    True
```

Verify Configuration for Edge2 (Site-Local Failover Device)

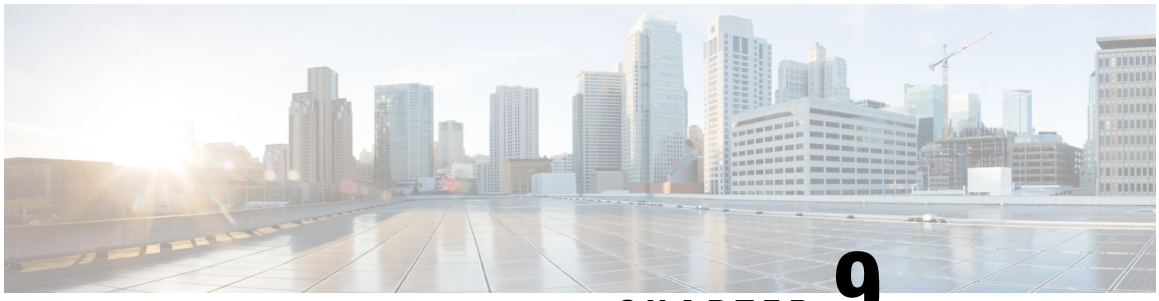
```
#show platform hardware qfp active feature sdwan datapath slr table hosts
VPN_IDX Host_IP Flags Tun_idx IFNAME Tx_encap_Pr Rx_decap_Pr Tx_encap_Sec Rx_decap_Sec
-------------------------------------------------------------------------------------------------------
1        198.51.100.3          0x0     65519      Tunnel15000561   0          0
0          0
1        198.51.100.4          0x1     65519      Tunnel15000561   0          0
0          0


#show ip nat translations
Pro Inside global         Inside local          Outside local         Outside global
<snip>
udp  172.21.11.1:5062      10.10.92.1:12346      172.21.20.1:12346     172.21.20.1:12346
icmp 172.21.11.1:199       10.10.1.4:199         8.8.8.8:199           8.8.8.8:199
<snip>Total number of translations: 10

#show ip nat translations
Pro Inside global         Inside local          Outside local         Outside global
<snip>
```

```
udp  172.21.11.1:5062      10.10.92.1:12346      172.21.20.1:12346     172.21.20.1:12346
icmp 172.21.11.1:199       198.51.100.4:199         8.8.8.8:199           8.8.8.8:199
<snip>
Total number of translations: 10
```

```
#show platform hardware qfp active feature sdwan datapath statistics | sec SLR
SDWAN SLR:
Total SLR policy : 0
Total SLR policy fail : 0
Total SLR Down : 0
Total SLR Tunnel adj not found : 0
Total SLR SB not Init : 0
Total SLR Host mem req : 0
Total SLR Host mem req : 0
Total SLR Dst Changed : 0
Total SLR Dia Down Fallback : 0
Total SLR Dia Down Restrict Drop Pkt : 0
Total SLR v4 Host Entry add failed : 0
Total SLR v6 Host Entry add failed : 0
Total SLR mdata encap        : 20
Total SLR mdata decap        : 44
```



CHAPTER 9

Support document links

A support document link is a resource that

- provides access to documents authored by Cisco subject matter experts
- helps resolve technical issues without requiring a support ticket, and
- offers guidance about the data to collect and add to a support ticket if escalation is needed.

Community and support escalation information

This section describes additional resources for resolving technical issues and guidance for support escalation.

- If the documents do not resolve your issue, visit the applicable Cisco Community for information and advice from fellow Cisco customers.
- If you cannot find a resolution on the Community, raise a support ticket at Cisco Support.
- When raising a support ticket, specify the support document you referred to so TAC can create an improvement request with the document owner.

- Support articles, on page 183
- Submit feedback for a support document, on page 184
- Disclaimer and caution, on page 184

Support articles

The documents in this section were created using specific software and hardware listed in the Components Used section of each article. However, this does not mean that they are limited to what is listed in Components Used, and generally remain relevant for later versions of software and hardware. Note that there could be some changes in the software or hardware that can cause commands to stop working, the syntax to change, or GUIs and CLIs to look different from one release to another.

The following support article is associated with this technology:

Document	Description
Configure Service to Transport Static NAT on a Cisco IOS XE Catalyst SD-WAN device	This document describes the configuration to perform a static NAT from the service side VRF to the transport VRF on a Cisco IOS XE Catalyst SD-WAN device.

Document	Description
Configure Service-Side Static NAT on a Cisco IOS XE Catalyst SD-WAN device	This document describes the configuration to perform a static NAT to and from service side VRF on a Cisco IOS-XE® SD-WAN Router.
Implement Direct Internet Access (DIA) for Cisco Catalyst SD-WAN	This document describes how to implement Cisco Catalyst SD-WAN DIA. It refers to the configuration when Internet traffic breaks out directly from branch router.

Submit feedback for a support document

Procedure

Step 1 Provide feedback using the **Feedback** button located at the right panel of the corresponding article.

The document owner will be notified and will either update the article or flag it for removal.

Step 2 Include information regarding the section, area, or issue you had with the document and what could be improved.

Provide as much detail as possible to help the document owner understand and address your feedback.

After submitting feedback, the document owner will review your input and may update the article or flag it for removal based on your suggestions.

Disclaimer and caution

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.