

Cisco IOS IP Addressing Services Command Reference

First Published: 2018-01-11

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)

© 2018 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **accounting DHCP through clear ip route** 1

accounting (DHCP) 3

accounting (DHCP for IPv6) 5

address client-id 6

address hardware-address 7

address prefix 8

address range 9

application redundancy 10

alg sip blacklist 11

alg sip processor 13

alg sip timer 14

arp (global) 15

arp (interface) 17

arp access-list 19

arp authorized 22

arp log threshold entries 23

arp packet-priority enable 25

arp probe interval 26

arp timeout 27

asymmetric-routing 28

authentication 30

authorization method (DHCP) 32

authorization shared-password 33

authorization username (DHCP) 34

auto-ip-ring 37

auto-ip-ring ipv4-auto 39

auto-ip-ring ipv4-seed 41
auto-ip-ring server 42
basic-mapping-rule 43
bootfile 44
cache-memory-max 45
class (DHCP) 46
clear arp interface 47
clear arp-cache 48
clear arp-cache counters ha 51
clear host 52
clear ip arp inspection log 54
clear ip arp inspection statistics 55
clear ip arp poll statistics 56
clear ip dhcp binding 57
clear ip dhcp conflict 59
clear ip dhcp limit lease 61
clear ip dhcp server statistics 62
clear ip dhcp snooping binding 63
clear ip dhcp snooping database statistics 64
clear ip dhcp snooping statistics 65
clear ip dhcp subnet 66
clear ip interface 68
clear ip nat translation 69
clear ip nat translation redundancy 72
clear ip nhrp 73
clear ip route 75

CHAPTER 2 **clear ip route dhcp through ip arp entry learn** 77

clear ip route dhcp 79
clear ip snat sessions 80
clear ip snat translation distributed 81
clear ip snat translation peer 82
clear ip dhcp snooping database statistics 83
clear ip translation peer 84

clear ipv6 dhcp 85
clear ipv6 dhcp binding 86
clear ipv6 dhcp client 88
clear ipv6 dhcp conflict 89
clear ipv6 dhcp-ldra statistics 90
clear ipv6 dhcp relay binding 92
clear ipv6 dhcp route 94
clear ipv6 nat translation 95
clear logging ip access-list cache 96
clear mdns cache 97
clear mdns service-types 98
clear mdns statistics 99
clear nat64 ha statistics 101
clear nat64 statistics 102
clear nat64 translations 104
client-identifier 105
client-name 107
control 108
data 110
ddns (DDNS-update-method) 111
default-mapping-rule 112
default-router 113
designated-gateway 114
device-role (DHCPv6 Guard) 116
dns forwarder 117
dns forwarding 119
dns forwarding source-interface 121
dns-server 123
dns-server (config-dhcp-global-options) 124
dns-server (IPv6) 125
domain list 126
domain lookup 128
domain multicast 130
domain name 131

domain-name (IPv6) 133
domain name-server 134
domain name-server interface 136
domain resolver source-interface 139
domain retry 140
domain round-robin 141
domain timeout 143
domain-name (DHCP) 144
designated-gateway 145
group (firewall) 147
hardware-address 148
host 151
host (host-list) 153
http (DDNS-update-method) 155
import all 159
import dns-server 160
import domain-name 161
import information refresh 162
import nis address 163
import nis domain-name 164
import nisp address 165
import nisp domain-name 166
import sip address 167
import sip domain-name 168
import sntp address 169
information refresh 171
internal (DDNS-update-method) 173
interval maximum 174
interval minimum 175
ip address 177
ip address dhcp 180
ip address pool (DHCP) 183
ip arp entry learn 184

CHAPTER 3 **ip arp gratuitous through ip dhcp ping packets** 187

ip arp gratuitous 189
ip arp incomplete 190
ip arp inspection filter vlan 191
ip arp inspection limit (interface configuration) 193
ip arp inspection log-buffer 195
ip arp inspection trust 197
ip arp inspection validate 198
ip arp inspection vlan 200
ip arp inspection vlan logging 201
ip arp nat-garp-retry 203
ip arp poll 205
ip arp proxy disable 206
ip arp queue 207
ip classless 208
ip ddns update hostname 209
ip ddns update method 210
ip default-gateway 211
ip dhcp aaa default username 212
ip dhcp auto-broadcast 214
ip dhcp bootp ignore 215
ip dhcp class 216
ip dhcp client 218
ip dhcp client authentication key-chain 219
ip dhcp client authentication mode 220
ip dhcp client broadcast-flag (interface) 222
ip dhcp client class-id 223
ip dhcp client client-id 224
ip dhcp client default-router distance 226
ip dhcp client hostname 227
ip dhcp client lease 228
ip dhcp client mobile renew 230
ip dhcp client request 231

ip dhcp client route 233
ip dhcp client update dns 234
ip dhcp compatibility lease-query client 236
ip dhcp compatibility suboption link-selection 238
ip dhcp conflict logging 239
ip dhcp conflict resolution 240
ip dhcp database 241
ip dhcp debug ascii-client-id 243
ip dhcp excluded-address 244
ip dhcp global-options 246
ip dhcp limit lease log 247
ip dhcp limit lease per interface 248
ip dhcp limited-broadcast-address 249
ip dhcp ping packets 250

CHAPTER 4 **ip dhcp ping timeout through ip dhcp-client forcerenew** 251

ip dhcp ping timeout 253
ip dhcp pool 254
ip dhcp relay bootp ignore 256
ip dhcp relay prefer known-good-server 257
ip dhcp relay forward spanning-tree 258
ip dhcp relay information check 259
ip dhcp relay information check-reply 260
ip dhcp relay information option 262
ip dhcp relay information option server-id-override 265
ip dhcp relay information option subscriber-id 267
ip dhcp relay information option vpn-id 269
ip dhcp relay information option-insert 271
ip dhcp relay information policy 273
ip dhcp relay information policy-action 275
ip dhcp relay information trust-all 277
ip dhcp relay information trusted 278
ip dhcp-relay source-interface 279
ip dhcp route connected 280

ip dhcp server use subscriber-id client-id 281
ip dhcp smart-relay 282
ip dhcp snooping 283
ip dhcp snooping binding 284
ip dhcp snooping database 285
ip dhcp snooping detect spurious 287
ip dhcp snooping detect spurious interval 289
ip dhcp snooping detect spurious vlan 290
ip dhcp snooping glean 291
ip dhcp snooping information option 292
ip dhcp snooping limit rate 294
ip dhcp snooping packets 296
ip dhcp snooping verify mac-address 297
ip dhcp snooping vlan 298
ip dhcp subscriber-id interface-name 299
ip dhcp support option55-override 300
ip dhcp support tunnel unicast 301
ip dhcp update dns 302
ip dhcp use 303
ip dhcp use subscriber-id client-id 305
ip dhcp-client broadcast-flag 306
ip dhcp-client default-router distance 307
ip dhcp-client forcerenew 308

CHAPTER 5 **ip dhcp-client network-discovery through ip nat sip-sbc** 309
ip dhcp-client network-discovery 311
ip dhcp-client update dns 313
ip dhcp drop-inform 315
ip dhcp-relay information option server-override 316
ip dhcp-relay source-interface 318
ip dhcp-server 319
ip dhcp-server query lease 321
ip dns name-list 322
ip dns primary 324

ip dns server 326
ip dns server queue limit 327
ip dns server view-group 328
ip dns spoofing 330
ip dns view 331
ip dns view-group 335
ip dns view-list 337
ip domain list 340
ip domain lookup 342
ip domain multicast 344
ip domain name 345
ip domain recursive 347
ip domain retry 348
ip domain round-robin 349
ip domain timeout 350
ip gratuitous-arps 351
ip host 352
ip host-list 357
ip hostname strict 358
ip local-proxy-arp 360
ip mobile arp 361
ip name-server 363
ip nat 365
ip nat create flow-entries 367
ip nat enable 369
ip nat inside destination 370
ip nat inside source 372
ip nat log translations flow-export 378
ip nat log translations syslog 380
ip nat outside source 381
ip nat piggyback-support 385
ip nat pool 386
ip nat service 389
ip nat service dns-reset-ttl 394

ip nat service enable-sym-port 396
ip nat service gatekeeper 398
ip nat service ipsec-esp enable 399
ip nat service pptp 400
ip nat settings gatekeeper-size 401
ip nat settings mode 402
ip nat settings pap 403
ip nat settings pool watermark 406
ip nat settings redundancy optimized-data-sync 407
ip nat settings scale bind 409
ip nat settings support mapping outside 410
ip nat sip-sbc 411

CHAPTER 6 **ip nat source through iterate-ip-addrs 415**

ip nat settings gatekeeper-size 417
ip nat settings high-performance 418
ip nat settings nonpatdrop 420
ip nat source 421
ip nat stateful id 423
ip nat switchover replication http 425
ip nat translation 426
ip nat translation (timeout) 427
ip nat translation max-entries 430
ip nat translation max-entries cpu 433
ip netmask-format 434
ip nhrp authentication 435
ip nhrp group 436
ip nhrp holdtime 438
ip nhrp interest 439
ip nhrp map 440
ip nhrp map group 442
ip nhrp map multicast 444
ip nhrp map multicast dynamic 445
ip nhrp max-send 447

ip nhrp multicast 449
ip nhrp network-id 450
ip nhrp nhs 451
ip nhrp record 454
ip nhrp redirect 455
ip nhrp registration 457
ip nhrp registration no-unique 459
ip nhrp responder 460
ip nhrp resolution refresh base 461
ip nhrp send-routed 463
ip nhrp server-only 464
ip nhrp shortcut 465
ip nhrp trigger-svc 466
ip nhrp use 467
ip options 469
ip proxy-arp 471
ip route 472
ip route vrf 477
ip routing 481
ip source binding 482
ip source-route 484
ip sticky-arp (global configuration) 485
ip sticky-arp (interface configuration) 487
ip subnet-zero 488
ip unnumbered 489
IP Unnumbered Ethernet Polling Support 492
ip verify source vlan dhcp-snooping 493
ipv4-prefix 494
ipv6 address autoconfig 495
ipv6 address dhcp 497
ipv6 address dhcp client request 498
ipv6 dhcp binding track ppp 499
ipv6 dhcp client information refresh minimum 500
ipv6 dhcp client pd 501

ipv6 dhcp database 503
ipv6 dhcp debug redundancy 505
ipv6 dhcp framed password 506
ipv6 dhcp guard attach-policy 507
ipv6 dhcp guard policy 509
ipv6 dhcp iana-route-add 510
ipv6 dhcp iapd-route-add 511
ipv6 dhcp-ldra 512
ipv6 dhcp-ldra attach-policy 513
ipv6 dhcp ldra attach-policy (VLAN) 515
ipv6 dhcp ping packets 516
ipv6 dhcp pool 517
ipv6 dhcp relay destination 520
ipv6 dhcp-relay source-interface 523
ipv6 dhcp-relay bulk-lease 524
ipv6 dhcp-relay option vpn 525
ipv6 dhcp-relay show bindings 526
ipv6 dhcp-relay source-interface 527
ipv6 dhcp server 528
ipv6 dhcp server vrf enable 530
ipv6 inspect tcp finwait-time 531
ipv6 nd managed-config-flag 532
ipv6 nd other-config-flag 534
ipv6-prefix 536
iterate-ip-addrs 537

CHAPTER 7 **lease through renew dhcp 541**

lease 544
local-ip (IPC transport-SCTP local) 546
local-port 548
logging (cfg-dns-view) 549
logging (DNS) 550
logging server-arp 551
mac packet-classify 553

mac packet-classify use vlan 555
match learnt-interface 556
match location 558
match message-type 560
match reply prefix-list 561
match server access-list 562
match service-instance 563
match service-type 564
mode (nat64) 565
name 566
nat64 enable 567
nat64 logging 568
nat64 logging translations flow-export 569
nat64 map-t 571
nat64 prefix stateful 572
nat64 prefix stateless 574
nat64 route 576
nat64 service ftp 577
nat64 settings 578
nat64 settings eif 579
nat64 settings flow-entries disable 580
nat64 settings mtu minimum 582
nat64 switchover replicate http 583
nat64 translation 584
nat64 v4 585
nat64 v4v6 586
nat64 v6v4 588
nat66 inside 590
nat66 outside 591
nat66 prefix 592
netbios-name-server 593
netbios-node-type 594
network (DHCP) 595
next-server 597

nhrp cache limit 598
nhrp group 600
nhrp map group 602
nis address 604
nis domain-name 605
nisp domain-name 606
nisp address 607
odap client 608
odap server 609
option 610
option hex 612
option ext 614
origin 616
override default-router 618
override utilization high 620
override utilization low 621
port-parameters 622
preempt 623
preference (DHCPv6 Guard) 624
prefix-delegation 625
prefix-delegation aaa 627
prefix-delegation pool 630
priority (firewall) 632
protocol 633
rate-limit (mDNS) 634
rbe nasip 636
redistribute mdns-sd 638
redundancy 640
redundancy asymmetric-routing enable 645
redundancy group 646
redundancy group (interface) 647
relay agent information 649
relay destination 650
relay source 651

relay target 652
relay-information hex 654
release dhcp 656
remote command 658
remote login 660
remote-ip (IPC transport-SCTP remote) 662
remote-port 664
remote-span 665
renew deny unknown 666
renew dhcp 668

CHAPTER 8 **reserved-only through show ip irdp 671**

reserved-only 673
restrict authenticated 674
restrict name-group 676
restrict source access-group 678
service dhcp 680
service-instance mdns-sd 682
service-list mdns-sd 684
service-policy 686
service-policy-proximity 687
service-policy-query 689
service-policy-query (interface) 690
service-routing mdns-sd 692
service-type-enumeration period 694
set ip next-hop dynamic dhcp 695
set platform software trace forwarding-manager alg 696
show alg sip 698
show arp 700
show arp application 705
show arp ha 708
show arp summary 712
show auto-ip-ring 715
show hosts 718

show ip aliases 721
show ip arp 723
show ip arp inspection 725
show ip arp inspection log 728
show ip arp poll 729
show ip ddns update 730
show ip ddns update method 731
show ip dhcp binding 732
show ip dhcp conflict 735
show ip dhcp database 737
show ip dhcp import 739
show ip dhcp limit lease 740
show ip dhcp pool 741
show ip dhcp relay information trusted-sources 743
show ip dhcp server statistics 744
show ip dhcp snooping 746
show ip dhcp snooping binding 748
show ip dhcp snooping database 751
show ip dhcp vrf 753
show ip dns name-list 755
show ip dns primary 757
show ip dns statistics 759
show ip dns view 761
show ip dns view-list 764
show ip host-list 766
show ip interface 768
show ip interface unnumbered 777
show ip irdp 779

CHAPTER 9 **show ip masks through vrf DHCP pool** 781

show ip masks 784
show ip nat limits all-host 785
show ip nat limits all-vrf 787
show ip nat nvi statistics 789

show ip nat nvi translations 791
show ip nat redundancy 793
show ip nat statistics 795
show ip nat statistics platform 797
show ip nat translations 799
show ip nat translation entry-id platform 803
show ip nat translations redundancy 804
show ip nhrp 805
show ip nhrp group-map 816
show ip nhrp multicast 818
show ip nhrp multicast stats 821
show ip nhrp nhs 822
show ip nhrp redirect 825
show ip nhrp summary 827
show ip nhrp traffic 828
show ip route dhcp 830
show ip snat 832
show ip source binding 833
show ip verify source 835
show ipv6 dhcp 838
show ipv6 dhcp binding 839
show ipv6 dhcp conflict 842
show ipv6 dhcp database 843
show ipv6 dhcp guard policy 845
show ipv6 dhcp-ldra 847
show ipv6 dhcp pool 850
show ipv6 dhcp interface 852
show ipv6 dhcp relay binding 855
show ipv6 dhcp route 857
show ip nat pool platform 858
show ip nat pool name platform 859
show ipv6 nat statistics 860
show ipv6 nat translations 861
show logging ip access-list 863

show mdns cache 865
show mdns cache mac 867
show mdns cache static 869
show mdns requests 871
show mdns service-types 873
show mdns statistics 875
show nat64 877
show nat64 adjacency 881
show nat64 aliases 883
show nat64 ha status 885
show nat64 limits 887
show nat64 map-t 889
show nat64 mappings dynamic 890
show nat64 pools 892
show nat64 prefix stateful 894
show nat64 prefix stateless 896
show nat64 routes 898
show nat64 services 900
show nat64 statistics 902
show nat64 timeouts 904
show nat64 translations 905
show nat64 translations entry-type 908
show nat64 translations redundancy 910
show nat64 translations time 912
show nat64 translations total 914
show nat64 translations v4 916
show nat64 translations v6 918
show nat64 translations verbose 920
show nhrp debug-condition 923
show nhrp group-map 924
show platform hardware qfp feature 926
show platform hardware qfp feature alg statistics sip 930
show platform software trace message 933
show redundancy application control-interface group 936

show redundancy application data-interface 937
show redundancy application faults group 938
show redundancy application group 939
show redundancy application if-mgr 943
show redundancy application protocol 945
show redundancy application transport 947
show running-config mdns-sd policy 948
show running-config mdns-sd service-instance 950
show running-config mdns-sd service-list 952
show running-config vrf 954
show tech nat 957
sip address 959
sip domain-name 960
snmp-server enable traps dhcp 961
source-interface (mDNS) 962
subnet prefix-length 964
term ip netmask-format 967
timers hellotime 968
trusted-port (DHCPv6 Guard) 970
update arp 971
update dns 973
utilization mark high 975
utilization mark low 977
view (DNS) 978
vrf (DHCP pool) 981
vrf (DHCPv6 pool) 982



accounting DHCP through clear ip route

- accounting (DHCP), on page 3
- accounting (DHCP for IPv6), on page 5
- address client-id, on page 6
- address hardware-address, on page 7
- address prefix, on page 8
- address range, on page 9
- application redundancy, on page 10
- alg sip blacklist, on page 11
- alg sip processor, on page 13
- alg sip timer, on page 14
- arp (global), on page 15
- arp (interface), on page 17
- arp access-list, on page 19
- arp authorized, on page 22
- arp log threshold entries, on page 23
- arp packet-priority enable, on page 25
- arp probe interval, on page 26
- arp timeout, on page 27
- asymmetric-routing, on page 28
- authentication, on page 30
- authorization method (DHCP), on page 32
- authorization shared-password, on page 33
- authorization username (DHCP), on page 34
- auto-ip-ring, on page 37
- auto-ip-ring ipv4-auto, on page 39
- auto-ip-ring ipv4-seed, on page 41
- auto-ip-ring server, on page 42
- basic-mapping-rule, on page 43
- bootfile, on page 44
- cache-memory-max , on page 45
- class (DHCP), on page 46
- clear arp interface, on page 47
- clear arp-cache, on page 48

- clear arp-cache counters ha, on page 51
- clear host, on page 52
- clear ip arp inspection log, on page 54
- clear ip arp inspection statistics, on page 55
- clear ip arp poll statistics, on page 56
- clear ip dhcp binding, on page 57
- clear ip dhcp conflict, on page 59
- clear ip dhcp limit lease, on page 61
- clear ip dhcp server statistics, on page 62
- clear ip dhcp snooping binding, on page 63
- clear ip dhcp snooping database statistics, on page 64
- clear ip dhcp snooping statistics, on page 65
- clear ip dhcp subnet, on page 66
- clear ip interface, on page 68
- clear ip nat translation, on page 69
- clear ip nat translation redundancy, on page 72
- clear ip nhrp, on page 73
- clear ip route, on page 75

accounting (DHCP)

To enable Dynamic Host Configuration Protocol (DHCP) accounting, use the **accounting**command in DHCP pool configuration mode. To disable DHCP accounting for the specified server group, use the **no** form of this command.

accounting *server-group-name*
no accounting *server-group-name*

Syntax Description

server-group-name	Name of a server group to apply DHCP accounting. • The server group can have one or more members. The server group is defined in the configuration of the **aaa group server** and **aaa accounting** commands.

Command Default

DHCP accounting is not enabled by default.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

The **accounting**command is used to enable the DHCP accounting feature by sending secure DHCP START accounting messages when IP addresses are assigned to DHCP clients, and secure DHCP STOP accounting messages when DHCP leases are terminated. A DHCP lease is terminated when the client explicitly releases the lease, when the session times out, and when the DHCP bindings are cleared from the DHCP database. DHCP accounting is configured on a per-client or per-lease basis. Separate DHCP accounting processes can be configured on a per-pool basis.

The **accounting**command can be used only to network pools in which bindings are created automatically and destroyed upon lease termination (or when the client sends a DHCP RELEASE message). DHCP bindings are also destroyed when the **clear ip dhcp binding** or **no service dhcp** command is issued. These commands should be used with caution if an address pool is configured with DHCP accounting.

Authentication, authorization, and accounting (AAA) and RADIUS must be configured before this command can be used to enable DHCP accounting. A server group must be defined with the **aaa group server** command. START and STOP message generation is configured with the **aaa accounting**command. The **aaa accounting**command can be configured to enable the DHCP accounting to send both START and STOP messages or STOP messages only.

Examples

The following example shows how to configure DHCP accounting start and stop messages to be sent if RADIUS-GROUP1 is configured as a start-stop group. Stop messages will be sent only if RADIUS-GROUP1 is configured as a stop-only group.

```
Router(config)# ip dhcp pool pool1
```

```
Router(dhcp-config)# accounting group1
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
aaa group serve r	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
aaa session-id	Specifies whether the same session ID will be used for each AAA accounting service type within a call or whether a different session ID will be assigned to each accounting service type.
clear arp-cache	Deletes all dynamic entries from the ARP cache.
clear ip dhcp binding	Deletes an automatic address binding from the Cisco IOS DHCP server database.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.
ip radius source-interface	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.
radius-server hos t	Specifies a RADIUS server host.
radius-server retransmit	Specifies the number of times that Cisco IOS will look for RADIUS server hosts.
service dhcp	Enables the Cisco IOS DHCP server and relay agent features.
show ip dhcp binding	Displays address bindings on the Cisco IOS DHCP server.
show ip dhcp server statistics	Displays Cisco IOS DHCP server statistics.
update arp	Secures the MAC address of the authorized client interface to the DHCP binding.

accounting (DHCP for IPv6)

To enable sending of accounting start and stop messages, use the **accounting** command in DHCP for IPv6 pool configuration mode. To remove configuration for these messages, use the **no** form of this command.

accounting *mlist*
no accounting *mlist*

Syntax Description

mlist	Accounting list to which start and stop messages are sent.

Command Default

Accounting start and stop messages are not configured.

Command Modes

DHCP for IPv6 pool configuration (config-dhcp)

Command History

Release	Modification
Cisco IOS Release XE 2.5	This command was introduced.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

The **accounting** command allows users to configure and send accounting start and stop messages to a named accounting list. When accounting is configured for a DHCPv6 pool, accounting interim packets are sent to broadband sessions after binding is provided from the pool.

Examples

The following example configures accounting start and stop messages to be sent to an accounting list called list1:

```
Router(config)# ipv6 dhcp pool pool1
Router(config-dhcp)# accounting list1
```

address client-id

To reserve an IP address for a Dynamic Host Configuration Protocol (DHCP) client identified by a client identifier, use the **address client-id** command in DHCP pool configuration mode. To remove the reserved address, use the **no** form of this command.

address *ip-address* **client-id** *string* [**ascii**]
no address *ip-address*

Syntax Description

ip-address	IP address reserved for the client.
string	A unique ASCII string or hexadecimal string.
ascii	(Optional) Specifies that the client ID is in ASCII string form.

Command Default

IP addresses are not reserved.

Command Modes

DCHP pool configuration (dhcp-config)

Command History

Release	Modification
12.2(46)SE	This command was introduced.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

The **address client-id** command can be used to create reserved addresses in pools for any DHCP client identified by the client identifier option in the DHCP packet. You can also reserve an IP address for a DHCP client that is configured to use the port-based address allocation feature. For port-based address allocation, the *string* argument must be the short name of the interface (port) and the **ascii** keyword must be specified.

Examples

In the following example, a subscriber ID will be automatically generated based on the short name of the interface (port) specified by the **address client-id**command. The DHCP server will ignore any client identifier fields in the DHCP messages and use this subscriber ID as the client identifier. The DHCP client is preassigned IP address 10.1.1.7.

```
Router(config)# ip dhcp use subscriber-id client-id
Router(config)# ip dhcp subscriber-id interface-name
Router(config)# ip dhcp excluded-address 10.1.1.1 10.1.1.3
Router(config)# ip dhcp pool dhcppool
Router(dhcp-config)# network 10.1.1.0 255.255.255.0
Router(dhcp-config)# address 10.1.1.7 client-id ethernet 1/0 ascii
```

Related Commands

Command	Description
address hardware address	Reserves an IP address for a client identified by hardware address.

address hardware-address

To reserve an IP address for a client identified by hardware address, use the **address hardware-address** command in DHCP pool configuration mode. To remove the reserved address, use the **no** form of this command.

address *ip-address* **hardware-address** *mac-address* [*hardware-number*]
no address *ip-address*

Syntax Description

ip-address	IP address reserved for the client.
mac-address	Hardware address of the client.
hardware-number	(Optional) Address Resolution Protocol (ARP) hardware specified in an online database at http://www.iana.org/assignments/arp-parameters. The range is from 0 to 255.

Command Default

IP addresses are not reserved.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

Release	Modification
12.2(46)SE	This command was introduced.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

This command is used to reserve an IP address for clients identified by the hardware address included in the fixed-size header of the Dynamic Host Configuration Protocol (DHCP) message.

Examples

In the following example, an IP address is reserved for a client that is identified by its hardware address:

```
Router(config)# ip dhcp pool dhcppool
Router(dhcp-config)# address 10.10.10.3 hardware-address b708.1388.f166
```

Related Commands

Command	Description
address client-id	Reserves an IP address for a DHCP client identified by the client identifier.

address prefix

To specify an address prefix for address assignment, use the **address prefix** command in interface configuration mode. To remove the address prefix, use the **no** form of this command.

address prefix ipv6-prefix [**lifetime** {**valid-lifetime preferred-lifetime** | **infinite**}]
no address prefix

Syntax Description

ipv6-prefix	IPv6 address prefix.
lifetime {valid-lifetime preferred-lifetime | infinite}]	(Optional) Specifies a time interval (in seconds) that an IPv6 address prefix remains in the valid state. If the **infinite** keyword is specified, the time interval does not expire.

Command Default

No IPv6 address prefix is assigned.

Command Modes

DHCP pool configuration (config-dhcpv6)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

You can use the **address prefix** command to configure one or several address prefixes in an IPv6 DHCP pool configuration. Each time the IPv6 DHCP address pool is used, an address will be allocated from each of the address prefixes associated with the IPv6 DHCP pool.

Examples

The following example shows how to configure a pool called engineering with an IPv6 address prefix:

```
Router(config)# ipv6 dhcp pool engineering
Router(config-dhcpv6)# address prefix 2001:1000::0/64 lifetime infinite
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCPv6 server configuration information pool and enters DHCPv6 pool configuration mode.

address range

To set an address range for a Dynamic Host Configuration Protocol (DHCP) class in a DHCP server address pool, use the **address range**command in DHCP pool class configuration mode. To remove the address range, use the **no** form of this command.

address range *start-ip end-ip*
no address range *start-ip end-ip*

Syntax Description

start-ip	Starting IP address that defines the range of addresses in the address pool.
end-ip	Ending IP address that defines the range of addresses in the address pool.

Command Default

No DHCP address range is set.

Command Modes

DHCP pool class configuration (config-dhcp-pool-class)

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

If the **address range** command is not configured for a DHCP class in a DHCP server address pool, the default value is the entire subnet of the address pool.

Examples

The following example shows how to set the available address range for class 1 from 10.0.20.1 through 10.0.20.100:

```
Router(config)# ip dhcp pool pool1
Router(dhcp-config)# network 10.0.20.0 255.255.255.0
Router(dhcp-config)# class class1
Router(config-dhcp-pool-class)# address range 10.0.20.1 10.0.20.100
```

Related Commands

Command	Description
ip dhcp class	Defines a DHCP class and enters DHCP class configuration mode.

application redundancy

To enter redundancy application configuration mode, use the **application redundancy** command in redundancy configuration mode.

application redundancy

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Redundancy configuration (config-red)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Examples

The following example shows how to enter redundancy application configuration mode:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)#
```

Related Commands

Command	Description
group (firewall)	Enters redundancy application group configuration mode.

alg sip blacklist

To configure a dynamic Session Initiation Protocol (SIP) application layer gateway (ALG) blocked list for destinations, use the **alg sip blacklist** command in global configuration mode. To remove a blocked list, use the **no** form of this command.

alg sip blacklist trigger-period *seconds* **trigger-size** *number-of-events* [**block-time** *block-time*] [**destination** *ipv4-address*]
no alg sip blacklist trigger-period *seconds* **trigger-size** *number-of-events* [**block-time** *block-time*] [**destination** *ipv4-address*]

Syntax Description

trigger-period *seconds*	Specifies the time period, in seconds, during which events are monitored before a blocked list is triggered. Valid values are from 10 to 60000.
trigger-size *number-of-events*	Specifies the number of events that are allowed from a source before the blocked list is triggered and all packets from that source are blocked. Valid values are from 1 to 65535.
block-time *block-time*	(Optional) Specifies the time period, in seconds, when packets from a source are blocked if the configured limit is exceeded. Valid values are from 0 to 2000000. The default is 30.
destination *ipv4-address*	(Optional) Specifies the destination IP address to be monitored.

Command Default

A blocked list is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.11S	This command was introduced.

Usage Guidelines

If the configured block time is zero, it means that a blocked list is not configured for the source. If no destination is specified, all destinations are monitored for denial of service (DoS) attacks.

The following events trigger a blocked list:

- In the configured period of time if a source sends multiple requests to a destination and receives non-2xx (as per RFC 3261, any response with a status code between 200 and 299 is a "2xx response") final responses from the destination.
- In the configured period of time if a source sends multiple requests to a destination and does not receive any response from the destination.

Examples

The following example shows how to configure a blocked list for the destination IP address 10.2.2.23:

```
Device(config)# alg sip blacklist trigger-period 100 trigger-size 10 destination 10.2.2.23
```

Related Commands

show alg sip	Displays all SIP ALG information.

alg sip processor

To configure the maximum number of backlog messages that wait for shared processor resources, use the **alg sip processor** command in global configuration mode. To disable the configuration, use the **no** form of this command.

alg sip processor {**global** | **session**} **max-backlog** *concurrent-usage*
no alg sip processor {**global** | **session**} **max-backlog** *concurrent-usage*

Syntax Description

global	Sets the maximum number of backlog messages that are waiting for shared resources for all Session Initiation Protocol (SIP) sessions. The default is 100.
session	Sets a per session limit for the number of backlog messages waiting for shared resources. The default is 10.
max-backlog	Specifies the maximum backlog for all sessions or for a single session.
concurrent-usage	Maximum number of backlog messages waiting for concurrent processor usage. Valid values are from 1 to 200 for the **global** keyword and from 1 to 20 for the **session** keyword.

Command Default

Blocked list messages are enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.11S	This command was introduced.

Usage Guidelines

Use this command to configure parameters against distributed denial of service (DoS) attacks.

Examples

The following example shows set the per session limit for the number of backlog messages:

```
Device(config)# alg sip processor session max-backlog 5
```

Related Commands

show alg sip	Displays all SIP ALG information.

alg sip timer

To configure a timer that the Session Initiation Protocol (SIP) application layer gateway (ALG) uses to manage SIP calls, use the **alg sip timer** command in global configuration mode. To remove the configured timer, use the **no** form of this command.

alg sip timer {**call-proceeding-timeout** *call-proceeding-time* | **max-call-duration** *call-duration*}
no alg sip timer {**call-proceeding-timeout** *call-proceeding-time* | **max-call-duration** *call-duration*}

Syntax Description

call-proceeding-timeout *call-proceeding-time*	Sets the call proceeding time interval, in seconds, for SIP calls that do not receive a response. The range is from 30 to 1800. The default is 180.
max-call-duration *call-duration*	Sets the maximum call duration, in seconds, for a successful SIP call. The range is from 0 to 65535. The default is 3600.

Command Default

A timer is not configured for SIP ALG calls.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.11S	This command was introduced.

Usage Guidelines

The timer that you configure with the **alg sip timer call-proceeding-timeout** command is similar to the number of times a phone rings for a call; the SIP ALG releases the SIP call if the call is not connected after the final ring.

When you configure the **alg sip timer max-call-duration** command, all SIP calls whose duration exceeds the configured value is released. The SIP ALG only releases resources that are used by the calls; and the SIP ALG is not torn down.

Examples

The following example shows how to configure a maximum time interval after which an unsuccessful SIP call is released:

```
Device(config)# alg sip timer call-proceeding-timeout 200
```

The following example shows how to configure a call duration time for a successful SIP call:

```
Device(config)# alg sip timer max-call-duration 180
```

Related Commands

show alg sip	Displays all SIP ALG information.

arp (global)

To add a permanent entry in the Address Resolution Protocol (ARP) cache, use the **arp** command in global configuration mode. To remove an entry from the ARP cache, use the **no** form of this command.

arp {*ip-address* | **vrf** *vrf-name*} *hardware-address encap-type* [*interface-type*] [**alias**]
no arp {*ip-address* | **vrf** *vrf-name*} *hardware-address encap-type* [*interface-type*] [**alias**]

Cisco IOS 12.2(33)SXI Release and Later Releases
arp {*ip-address* | **vrf** *vrf-name* | **access-list** *name* | **clear retry** *count*} *hardware-address encap-type* [*interface-type*] [**alias**]
no arp {*ip-address* | **vrf** *vrf-name* | **access-list** *name* | **clear retry** *count*} *hardware-address encap-type* [*interface-type*] [**alias**]

Syntax Description

ip-address	IP address in four-part dotted decimal format corresponding to the local data-link address.
vrf *vrf-name*	Virtual routing and forwarding (VRF) instance. The *vrf-name* argument is the name of the VRF table.
access-list	Specifies the named access-list.
name	Access-list name.
clear	Clears ARP command parameter.
retry	Specifies the number of retries.
count	Retry attempts. The range is from 1 to 50.
hardware-address	Local data-link address (a 48-bit address).
encap-type	Encapsulation description. The keywords are as follows: • **arpa** --For Ethernet interfaces. • **sap** --For Hewlett Packard interfaces. • **smds** --For Switched Multimegabit Data Service (SMDS) interfaces. • **snap** --For FDDI and Token Ring interfaces. • **srp-a** --Switch Route Processor, side A (SRP-A) interfaces. • **srp-b** --Switch Route Processor, side B (SRP-B) interfaces.

interface-type	(Optional) Interface type. For more information, use the question mark (?) online help. The keywords are as follows: • **ethernet** --IEEE 802.3 interface. • **loopback** --Loopback interface. • **null** --No interface. • **serial** --Serial interface.
alias	Responds to ARP requests for the IP address.

Command Default

No entries are permanently installed in the ARP cache.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SXI	This command was modified in a release earlier than Cisco IOS Release 12.2(33)SXI. The **clear** and **retry** keywords were added. The *count* argument was added.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S

Usage Guidelines

The Cisco IOS software uses ARP cache entries to translate 32-bit IP addresses into 48-bit hardware addresses. Because most hosts support dynamic resolution, you generally need not specify static ARP cache entries.

To remove all nonstatic entries from the ARP cache, use the **clear arp-cache**privileged EXEC command.

Examples

The following is an example of a static ARP entry for a typical Ethernet host:

```
arp 10.31.7.19 0800.0900.1834 arpa
```

Related Commands

Command	Description
clear arp-cache	Deletes all dynamic entries from the ARP cache.

arp (interface)

To support a type of encapsulation for a specific network, such as Ethernet, Fiber Distributed Data Interface (FDDI), Frame Relay, and Token Ring, so that the 48-bit Media Access Control (MAC) address can be matched to a corresponding 32-bit IP address for address resolution, use the **arp** command in interface configuration mode. To disable an encapsulation type, use the **no** form of this command.

arp {**arpa** | **frame-relay** | **snap**}
no arp {**arpa** | **frame-relay** | **snap**}

Syntax Description

arpa	Standard Ethernet-style Address Resolution Protocol (ARP) (RFC 826).
frame-relay	Enables ARP over a Frame Relay encapsulated interface.
snap	ARP packets conforming to RFC 1042.

Command Default

Standard Ethernet-style ARP

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(13)T	The **probe** keyword was removed because the HP Probe feature is no longer available in Cisco IOS software.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.0(33)S	Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers.

Usage Guidelines

Unlike most commands that have multiple arguments, the **arp** command has arguments that are not mutually exclusive. Each command enables or disables a specific type of encapsulation.

Given a network protocol address (IP address), the **arp frame-relay** command determines the corresponding hardware address, which would be a data-link connection identifier (DLCI) for Frame Relay.

The **show interfaces** command displays the type of encapsulation being used on a particular interface. To remove all nonstatic entries from the ARP cache, use the **clear arp-cache** command.

Examples

The following example enables Frame Relay services:

```
interface ethernet 0
 arp frame-relay
```

Related Commands

Command	Description
clear arp-cache	Deletes all dynamic entries from the ARP cache.
show interfaces	Displays statistics for all interfaces configured on the router or access server.

arp access-list

To configure an Address Resolution Protocol access control list (ARP ACL) for ARP inspection and QoS filtering and enter the ARP ACL configuration submode, use the **arp access-list** command in global configuration mode. To remove the ARP ACL, use the **no** form of this command.

arp access-list *name*
no arp access-list *name*

Syntax Description

name	Name of the access list.

Command Default

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXE	This command was changed to support DAI on the Supervisor Engine 720. See the "Usage Guidelines" section for the syntax description.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Once you are in the ARP ACL configuration submode, you can add **permit** or **deny** clauses to permit or deny QoS to the flows. The following syntax is available in the ARP QoS ACL configuration submode for QoS filtering; all other configurations will be rejected at the time of the policy-map attachment to the interfaces:

{**permit** | **deny**} **ip** {**any** | **host** *sender-ip* [*sender-ip-mask*]} **mac any**
no {**permit** | **deny**} **ip** {**any** | **host** *sender-ip* [*sender-ip-mask*]} **mac any**

permit	Specifies to apply QoS to the flows.
deny	Skips the QoS action that is configured for traffic matching this ACE.
ip	Specifies the IP ARP packets.
any	Specifies any IP ARP packets.
host *sender-ip*	Specifies the IP address of the host sender.
sender-ip-mask	(Optional) Subnet mask of the host sender.
mac any	Specifies MAC-layer ARP traffic.
no	Deletes an ACE from an ARP ACL.

Once you are in the ARP ACL configuration submode, the following configuration commands are available for ARP inspection:

- **default** --Sets a command to its defaults. You can use the **deny** and **permit**keywords and arguments to configure the default settings.
- **deny** --Specifies the packets to reject.
- **exit** --Exits the ACL configuration mode.
- **no** --Negates a command or set its defaults.
- **permit** -- Specifies the packets to forward.

You can enter the **permit** or **deny** keywords to configure the permit or deny clauses to forward or drop ARP packets based on some matching criteria. The syntax for the **permit** and **deny** keywords are as follows:

{**permit** | **deny**} **ip** {**any** | **host** *sender-ip* [*sender-ip sender-ip-mask*]} **mac** {**any** | **host** *sender-mac* [*sender-mac-mask*]} [**log**]
{**permit** | **deny**} **request ip** {**any** | **host sender-ip** [**sender-ip-mask**]} **mac** {**any** | **host sender-mac** [**sender-mac-mask**]} [**log**]
{**permit** | **deny**} **response ip** {**any** | **host sender-ip** [**sender-ip-mask**]} [**any** | **host target-ip** [**target-ip-mask**]] **mac** {**any** | **host sender-mac** [**sender-mac-mask**]} [**any** | **host target-mac** [**target-mac-mask**]] [**log**]

permit	Specifies packets to forward.
deny	Specifies packets to reject.
ip	Specifies the sender IP address.
any	Specifies any sender IP address.
host	Specifies a single sender host.
sender-ip	IP address of the host sender.
sender-ip-mask	Subnet mask of the host sender.
mac any	Specifies any MAC address.
mac host	Specifies a single sender host MAC address.
sender-mac	MAC address of the host sender.
sender-mac-mask	Subnet mask of the host sender.
log	(Optional) Specifies log on match.
request	Specifies ARP requests.
response	Specifies ARP responses.
any	(Optional) Specifies any target address.
host	(Optional) Specifies a single target host.
target-ip	IP address of the target host.

target-ip-mask	Subnet mask of the target host.
target-mac	MAC address of the target host.
target-mac-mask	Subnet mask of the target host.

If you enter the **ip** keyword without the **request** or **response** keywords, the configuration applies to both requests and responses.

Once you define an ARP ACL, you can apply it to VLANs using the **ip arp inspection filter** command for ARP inspection.

Incoming ARP packets are compared against the ARP access list, and packets are permitted only if the access list permits them. If access lists deny packets because of explicit denies, they are dropped. If packets get denied because of the implicit deny, they are matched against the list of DHCP bindings, unless the access list is static or the packets are not compared against the bindings.

When a ARP access list is applied to a VLAN for dynamic ARP inspection, the ARP packets containing only IP-to-Ethernet MAC bindings are compared against the ACLs. All other type of packets are bridged in the incoming VLAN without any validation.

ACL entries are scanned in the order that you enter them. The first matching entry is used. To improve performance, place the most commonly used entries near the beginning of the ACL.

An implicit **deny ip any mac any** entry exists at the end of an ACL unless you include an explicit **permit ip any mac any** entry at the end of the list.

All new entries to an existing list are placed at the end of the list. You cannot add entries to the middle of a list.

Examples

This example shows how to create a new ARP ACL or enter the submode of an existing ARP ACL:

```
Router(config)# arp access-list arpacl22
Router(config-arp-nacl)#
```

This example shows how to create an ARP ACL named arp_filtering that denies QoS but permits MAC-layer ARP traffic:

```
Router(config)# arp access-list arp_filtering

Router(config-arp-nacl)# permit ip host 10.1.1.1 mac any
Router(config-arp-nacl)# deny ip any mac any
Router(config-arp-nacl)#
```

Related Commands

Command	Description
show arp	Displays information about the ARP table.

arp authorized

To disable dynamic Address Resolution Protocol (ARP) learning on an interface, use the **arp authorized** command in interface configuration mode. To reenable dynamic ARP learning, use the **no** form of this command.

arp authorized
no arp authorized

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The **arp authorized** command disables dynamic ARP learning on an interface. This command enhances security in public wireless LANs (PWLANs) by limiting the leasing of IP addresses to mobile users and authorized users. The mapping of IP address to MAC address for an interface can be installed only by the authorized subsystem. Unauthorized clients cannot respond to ARP requests.

If both static and authorized ARP are installing the same ARP entry, the static configuration overrides the authorized ARP entry. To install a static ARP entry use the **arp** (global) command. A nondynamic ARP entry can only be removed by using the same method by which it was installed.

The **arp authorized** command can only be specified on Ethernet interfaces and for Dynamic Host Configuration Protocol (DHCP) networks.

Examples

The following example disables dynamic ARP learning on interface Ethernet 0:

```
interface Ethernet0
 ip address 10.0.0.1 255.255.255.0
 arp authorized
```

Related Commands

Command	Description
arp (global)	Adds a permanent entry in the ARP cache.
update arp	Secures dynamic ARP entries in the ARP table to their corresponding DHCP bindings.

arp log threshold entries

To enable an Address Resolution Protocol (ARP) trap so that the ARP log is triggered when a specific number of dynamically learned entries is reached on the router interface, use the **arp log threshold entries** command in interface configuration mode. To disable the ARP trap for the interface, use the **no** form of this command.

arp log threshold entries *entry-count*
no arp log threshold entries

Syntax Description

entry-count	Triggers the ARP log service when the number of dynamically learned entries on the interface reaches this threshold. The range is from 1 to 2147483647.

Command Default

ARP trap is disabled for the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

This command enables an ARP trap for the router interface. When the number of dynamically learned entries on the interface exceeds the preconfigured amount, an ARP event message is written to system message logging (syslog) output.

A high number of learned entries on the interface might indicate anomalies such as an attempt to breach security through an ARP attack on the router. The threshold at which to configure the ARP log service trigger should be determined heuristically, based on the expected number of nodes the router will serve and the number of hosts on the interface.

To display information about the setting configured by the **arp log threshold entries** command, use the **show running-config** command. If an ARP trap is enabled for a given interface, the information for that **interface** command includes the **arp log threshold entries** command, followed by the threshold value.

To display the syslog history statistics and buffer contents, use the **show logging** command.

Examples

The following example shows how to enable an ARP trap so that the ARP log is triggered when 50 dynamically learned entries is reached on the Ethernet interface at slot 2, port 1:

```
Router(config)# interface ethernet2/1

Router(config-if)# arp log threshold entries 50
```

The following sample output from the **show logging** command shows that the ARP trap entry was triggered when 50 dynamic ARP entries was reached on the Ethernet interface at slot 2, port 1:

```
Router# show logging
```

```
Syslog logging: enabled (0 messages dropped, 39 messages rate-limited, 0 flushes, 0 overruns,
 xml disabled, filtering disabled)
    Console logging: disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging: level debugging, 309 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (8192 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled
No active filter modules.
    Trap logging: level informational, 312 message lines logged
Log Buffer (65536 bytes):
Jan 27 18:27:32.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 10:27:31 PST
Fri Jan 27 2006 to 10:27:32 PST Fri Jan 27 2006, configured from console by console.
Jan 27 18:27:32.431: %SYS-5-CONFIG_I: Configured from console by console
Jan 27 18:27:34.051: %ARP-4-TRAPENTRY: 50 dynamic ARP entries on Ethernet2/1 installed in
the ARP table
```

Related Commands

Command	Description
interface	Selects an interface to configure and enters interface configuration mode.
show logging	Displays the contents of logging buffers.
show running-config	Displays the contents of the currently running configuration file of your routing device.

arp packet-priority enable

To enable Address Resolution Protocol (ARP) packet priority on an interface, use the **arp packet-priority enable**command in interface configuration mode. To disable ARP packet priority, use the **no** form of this command.

arp packet-priority enable
no arp packet-priority enable

Syntax Description

This command has no arguments or keywords.

Command Default

By default, ARP packet priority is not enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)T	This command was introduced.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.

Usage Guidelines

Use the **arp packet-priority enable** command when a network congestion causes ARP packets to drop. Enabling ARP packet priority significantly reduces the number of ARP packet drops.

Before you configure the **arp packet-priority enable** command, you must configure an IP address for the interface and ensure that the interface is enabled. If the interface is disabled, use the **no shutdown** command to enable the interface.

Examples

The following example shows how to enable packet priority on a Fast Ethernet interface:

```
Router(config)# interface FastEthernet0/1
Router(config-if)# no shutdown
Router(config-if)# ip address
 198.51.100.253 255.255.255.0
Router(config-if)# arp packet-priority enable
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
ip address	Sets a primary or secondary IP address for an interface.
shutdown (interface)	Disables an interface.

arp probe interval

To control the the p robing of authorized peers, use the **arp probe interval**command in interface configuration mode. To disable the probe, use the **no**form of this command.

arp probe interval *seconds* **count** *count-number*
no arp probe

Syntax Description

seconds	Interval in seconds after which the next probe will be sent to see if the peer is still present. The range is from 1 to 10.
count *count-number*	Number of probe retries. If no response, the peer has logged off. The range is from 1 to 60.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.3(8)XX	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Usage Guidelines

Once you configure the **arp probe interval** command, probing continues until you disable it using the **no** form of the command on all interfaces.

Examples

The following example shows a 2 second interval with a probe of the peer occurring 5 times:

```
interface ethernet 0
 arp probe interval 2 count 5
```

Related Commands

Command	Description
arp (interface)	Controls the interface-specific handling of IP address resolution.
clear arp-cache	Deletes all dynamic entries from the ARP cache.
show interfaces	Displays statistics for all interfaces configured on the router or access server.

arp timeout

To configure how long a dynamically learned IP address and its corresponding Media Control Access (MAC) address remain in the Address Resolution Protocol (ARP) cache, use the **arp timeout** command in interface configuration mode. To restore the default value, use the **no** form of this command.

arp timeout *seconds*
no arp timeout

Syntax Description

seconds	Time (in seconds) that an entry remains in the ARP cache. The general recommended value for ARP timeout is the configured default value, which is 4 hours. If the network has frequent changes to cache entries, change the default to a shorter time period. As you reduce the ARP timeout, your network traffic increases. A low ARP timeout value might lead to network outage, and a value less than an hour (or 3600 seconds) will generate significantly increased traffic across the network. **Caution** We recommend that you set an ARP timeout value greater than 60 seconds.

Command Default

14400 seconds (4 hours)

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is ignored when issued on interfaces that do not use ARP. The **show interfaces** EXEC command displays the ARP timeout value. The value is displayed in hours, as shown below:

```
ARP type: ARPA, ARP Timeout 02:00:00
```

Examples

The following example sets the ARP timeout to 7200 seconds (or 2 hours) to allow entries to time out more quickly than the default:

```
interface ethernet 0
 arp timeout 7200
```

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router or access server.

asymmetric-routing

To set up an asymmetric routing link interface and to enable applications to divert packets received on the standby redundancy group to the active, use the **asymmetric-routing** command in redundancy application group configuration mode. To disable the configuration, use the **no** form of this command.

asymmetric-routing {**always-divert enable** | **interface** *type number*}
no asymmetric-routing {**always-divert enable** | **interface**}

Syntax Description

always-divert enable	Always diverts packets from the standby redundancy group (RG) to the active RG.
interface *type number*	Specifies the asymmetric routing interface that is used by the RG.

Command Default

Asymmetric routing is disabled.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

Asymmetric routing occurs when packets from TCP or UDP connections flow in different directions through different routes. In asymmetric routing, packets that belong to a single connection are forwarded through one router, but return packets of the connection return through another router in the same RG. When you configure the **asymmetric routing always-divert enable** command, the packets received on the standby RG are redirected to the active RG for processing. If the **asymmetric routing always-divert enable** command is disabled, the packets received on the standby RG may be dropped.

When you configure the **asymmetric-routing interface** command, the asymmetric routing feature is enabled. After enabling the feature, configure the **asymmetric-routing always-divert enable** command to enable Network Address Translation (NAT) to divert packets that are received on the standby RG to the active RG.

Note The zone-based policy firewall does not support the **asymmetric-routing always-divert enable** command that diverts packets received on the standby RG to the active RG. The firewall forces all packet flows to be diverted to the active RG.

Examples

The following example shows how to configure asymmetric routing on a Gigabit Ethernet interface:

```
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 2
Router(config-red-app-grp)# asymmetric-routing interface gigabitethernet 0/0/0
Router(config-red-app-grp)# end
```

Related Commands

Command	Description
application redundancy	Configures application redundancy.
group	Configures a redundancy group.
redundancy	Enters redundancy configuration mode.
redundancy asymmetric-routing enable	Establishes an asymmetric flow diversion tunnel for each redundancy group.

authentication

To configure clear text authentication and MD5 authentication under a redundancy group protocol, use the **authentication**command in redundancy application protocol configuration mode. To disable the authentication settings in the redundancy group, use the **no** form of this command.

authentication {**text** *string* | **md5 key-string** [**0** | **7**] *key* | **md5 key-chain** *key-chain-name*}
no authentication {**text** *string* | **md5 key-string** [**0** | **7**] *key* | **md5 key-chain** *key-chain-name*}

Syntax Description

text *string*	Uses clear text authentication.
md5 key-string	Uses MD5 key authentication. The *key* argument can be up to 64 characters in length (at least 16 characters is recommended). Specifying 7 means the key will be encrypted.
0	(Optional) Specifies that the text following immediately is not encrypted.
7	(Optional) Specifies that the text is encrypted using a Cisco-defined encryption algorithm.
md5 key-chain *key-chain-name*	Uses MD5 key-chain authentication.

Command Default

The key is not encrypted.

Command Modes

Redundancy application protocol configuration (config-red-app-prtcl)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Examples

The following example shows how to configure clear text authentication for a redundancy group:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# protocol 1
Router(config-red-app-prtcl)# authentication text name1
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
group	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.
protocol	Defines a protocol instance in a redundancy group.

Command	Description
timers hellotime	Configures timers for hellotime and holdtime messages for a redundancy group.

authorization method (DHCP)

To specify a method list to be used for address allocation using RADIUS for Dynamic Host Control Protocol (DHCP), use the **authorization method**command in DHCP pool configuration mode. To disable the authorization method list, use the **no** form of this command.

authorization method *method-list-name*
no authorization method *method-list-name*

Syntax Description

method-list-name	An authorization method list of the network type to be used for this DHCP pool.

Command Default

The authorization network default method list is used for authorization.

Command Modes

DHCP pool configuration (config-dhcp)

Command History

Release	Modification
12.2(31)ZV1	This command was modified for the DHCP server RADIUS proxy feature on the Cisco 10000 series router and integrated into Cisco IOS Release 12.2(31)ZV1.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

The method list must be defined during initial authentication setup.

Examples

The following example shows how to set an authorization method of auth1 to download DHCP information from DHCP or a RADIUS server for DHCP clients when pool_common is used:

```
Router(config)# aaa authorization network auth1 group radius
Router(config)# ip dhcp pool pool_common
Router(config-dhcp)# authorization method auth1
```

Related Commands

Command	Description
authorization list	Specifies the AAA authorization list.
authorization username (dhcp)	Specifies the parameters that RADIUS sends to a DHCP server when downloading information for a DHCP client.
authorization shared-password	Specifies the password that RADIUS sends to a DHCP or RADIUS server when downloading configuration information for a DHCP client.

authorization shared-password

To specify the password that RADIUS sends to a Dynamic Host Control Protocol (DHCP) or RADIUS server when downloading configuration information for a DHCP client, use the **authorization shared-password** command in DHCP pool configuration mode. To remove the password used for downloading DHCP client configuration, use the **no** form of this command.

authorization shared-password *password*
no authorization shared-password *password*

Syntax Description

password	The password configured in the RADIUS user profile.

Command Default

No password is sent in the RADIUS requests.

Command Modes

DHCP pool configuration (config-dhcp)

Command History

Release	Modification
12.2(31)ZV1	This command was modified for the DHCP server RADIUS proxy feature on the Cisco 10000 series router and integrated into Cisco IOS Release 12.2(31)ZV1.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

This command is used to enter the password that matches the password configured in a RADIUS user profile, at a RADIUS server, for the username matching the string.

Examples

The following example shows how to set the password to cisco:

```
Router(config)# ip dhcp pool pool_common
Router(config-dhcp)# authorization method auth1
Router(config-dhcp)# authorization shared-password cisco
```

Related Commands

Command	Description
authorization list	Specifies the AAA authorization list.
authorization method (dhcp)	Specifies the method list to be used for address allocation information.
authorization username (dhcp)	Specifies the parameters that RADIUS sends to a DHCP server when downloading information for a DHCP client.

authorization username (DHCP)

To specify the parameters that RADIUS sends to a Dynamic Host Control Protocol (DHCP) server when downloading configuration information for a DHCP client, use the **authorization username** command in DHCP pool configuration mode. To disable the parameters, use the **no** form of this command.

authorization username *string*
no authorization username *string*

Syntax Description

string	A string that RADIUS sends to the DHCP server when downloading an IP address and other configuration information for a client's DHCP responses. The string must contain the following formatting characters to insert information associated with the DHCP client: • **%%** --Transmits the percent sign (%) character in the string sent to the RADIUS server • **%c** --Ethernet address of the DHCP client (chaddr field) in ASCII format • **%C** --Ethernet address of the DHCP client in hexadecimal format • **%g** --Gateway address of the DHCP relay agent (giaddr field) • **%i** --Inner VLAN ID from the DHCP relay information (option 82) in ASCII format • **%I** --Inner VLAN ID from the DHCP relay information in hexadecimal format • **%o** --Outer VLAN ID from the DHCP relay information (option 82) in ASCII format • **%O** --Outer VLAN ID from the DHCP relay information (option 82) in hexadecimal format • **%p** --Port number from the DHCP relay information (option 82) in ASCII format • **%P** --Port number from the DHCP relay information (option 82) in hexadecimal format • **%u** --Circuit ID from the DHCP relay information in ASCII format • **%U** --Circuit ID from the DHCP relay information in hexadecimal format • **%r** --Remote ID from the DHCP relay information in ASCII format • **%R** --Remote ID from the DHCP relay information in hexadecimal format **Note** The percent (%) is a marker to insert the DHCP client information associated with the specified character. The % is not sent to the RADIUS server unless you specify the %% character.

Command Default

No parameters are specified.

Command Modes

DHCP pool configuration (config-dhcp)

Command History

Release	Modification
12.2(31)ZV1	This command was modified for the DHCP server RADIUS proxy feature on the Cisco 10000 series router and integrated into Cisco IOS Release 12.2(31)ZV1.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

When a DHCP server sends an access request to the authentication, authorization, and accounting (AAA) server, the **%** and character specified in the username are format characters that is replaced by one of the following values based on the characters specified:

- Hardware address
- Inner VLAN ID
- Outer VLAN ID
- Port number
- Circuit ID
- Remote ID

The **%** and character specified in the **authorization username** command configure the DHCP server to send the username in ASCII format or the hexadecimal format based on the case (uppercase or lowercase) of the character used.

For example, if you specify **%C** with the **authorization username** command and the hardware address of the client is aabb.ccdd.eeff, then the DHCP server sends the username as "dhcp-AABBCCDDEEFF" in ASCII format. If you specify **%c** with the **authorization username** command, then the DHCP server sends the username as "646863702daabbccddeeff" in hexadecimal format. The server sends 11 bytes of data when the format is hexadecimal and 19 bytes when the format is ASCII.

Examples

The following example shows how to configure RADIUS to send the Ethernet address of the DHCP client (chaddr field) to the DHCP server when downloading configuration information for a DHCP client:

```
Router(config)# ip dhcp pool pool_common
Router(config-dhcp)# authorization method auth1
Router(config-dhcp)# authorization shared-password cisco
Router(config-dhcp)# authorization username %c-user1
```

Related Commands

Command	Description
authorization list	Specifies the AAA authorization list.
authorization method (dhcp)	Specifies the method list to be used for address allocation information.

Command	Description
authorization shared-password	Specifies the password that RADIUS sends to a DHCP or RADIUS server when downloading configuration information for a DHCP client.

auto-ip-ring

To enable the auto-IP functionality on the interfaces of a device, use the **auto-ip-ring** command in interface configuration mode. To disable the auto-IP functionality, use the **no** form of this command.

auto-ip-ring *ring-id* **ipv4-address** *auto-ip-address*
no auto-ip-ring *ring-id* **ipv4-address** *auto-ip-address*

Syntax Description

ring-id	Auto-IP ring identification number. The ring ID must be the same for the two network-to-network interfaces (NNIs) of the node. **Note** A device in a ring is called a node.
ipv4-address *auto-ip-address*	Specifies the auto-IP address configured on a node interface.

Command Default

The auto-IP functionality is not enabled on a node interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.10S	This command was introduced.
15.3(3)S	This command was integrated into Cisco IOS Release15.3(3)S

Usage Guidelines

1. Link Layer Discovery Protocol (LLDP) must be enabled on the device before configuring the auto-IP address on the node interfaces. Use the **lldp run** command in global configuration mode to enable LLDP.
2. You must configure the same auto-IP address on both the node interfaces on a device using the **auto-ip-ring** command. The auto-IP configuration can be enabled on node interfaces in an existing ring or auto-IP configured node interfaces can be inserted into an auto-IP ring.

Note If you are configuring a seed device, you must use the auto-IP address to configure the IP address on one of the node interfaces, with the mask /31. For example, if 10.1.1.1 is the auto-IP address for the 2 node interfaces, then one of the interfaces must be configured with the IP address 10.1.1.1 255.255.255.254.

3. Auto-IP addresses should contain an odd number in the last octet (such as 10.1.1.1, where the number in the last octet is 1). When a device is inserted into an auto-IP ring, IP address allocation takes place automatically by subtracting 1 from the last octet of R1's auto-IP address (10.1.1.0 is allocated to the neighbor node interface).

An auto-IP address must not be configured on an interface which belongs to a Virtual routing and forwarding (VRF) other than the global or default VRF since the auto-IP feature is not supported on a VRF.

Examples

The following example shows how to enable the auto-IP functionality on the interfaces of a device and configure a seed device:

Note You must configure at least one seed device in an auto-IP ring. In this example, the auto-IP address is being configured on one of the node interfaces with the mask /31 to designate the device as a seed device.

```
Device> enable
Device# configure terminal
Device(config)# lldp run
Device(config)# interface ethernet 0/0
Device(config-if)# auto-ip-ring 4 ipv4-address 10.1.1.1
Device(config-if)# exit
Device(config)# interface ethernet 1/0
Device(config-if)# auto-ip-ring 4 ipv4-address 10.1.1.1
Device(config-if)# ip address 10.1.1.1 255.255.255.254
Device(config-if)# end
```

The following example shows how to enable the auto-IP functionality on the interfaces of a device:

Note This configuration example applies to a device which is not being configured a seed device:

```
Device> enable
Device# configure terminal
Device(config)# lldp run
Device(config)# interface ethernet 0/1
Device(config-if)# auto-ip-ring 4 ipv4-address 10.1.1.3
Device(config-if)# exit
Device(config)# interface ethernet 1/1
Device(config-if)# auto-ip-ring 4 ipv4-address 10.1.1.3
Device(config-if)# end
```

Related Commands

Command	Description
debug auto-ip-ring	Debugs errors or events specific to an auto-IP ring.
show auto-ip-ring	Displays auto-IP ring information.

auto-ip-ring ipv4-auto

To enable automatic IP address configuration on an Auto-IP ring port from a pool of IP addresses, use the **auto-ip-ring ipv4-auto** command in interface configuration mode. To disable automatic IP address configuration on an Auto-IP ring port from a previously reserved pool of IP addresses, use the **no** form of this command.

auto-ip-ring *ring-id* **ipv4-auto**
no auto-ip-ring *ring-id* **ipv4-auto**

Syntax Description

ring-id	Auto-IP ring identification number. The ring ID must be the same for the two network-to-network interfaces (NNIs) of the node.
ipv4-auto	Automatically configures an IP address from a pool of IP addresses. **Remember** You must enable the **auto-ip-ring ipv4-auto** command on all Auto-IP ring ports for Zero touch Auto-IP functionality configuration.

Command Default

The automatic mode is disabled on an Auto-IP port.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.5(2)S	This command was introduced.
Cisco IOS XE Release 3.15S	This command was integrated into Cisco IOS XE Release 3.15S.

Usage Guidelines

The process of automatically configuring an IP address on an Auto-IP ring port from a pool of addresses forms a part of implementing the Zero touch Auto-IP functionality. Use the **auto-ip-ring server** (to implement a device as the Auto-IP server) and **auto-ip-ring ipv4-seed** (to create a port as seed port and initiate the automatic IP address configuration process) commands for other configurations of the Zero touch Auto-IP functionality.

Examples

The following example shows how to enable automatic IP address configuration on an Auto-IP ring port:

```
Device> enable
Device# configure terminal
Device(config)# lldp run
Device(config)# interface ethernet 0/0
Device(config-if)# auto-ip-ring 1 ipv4-auto
Device(config-if)# exit
Device(config)# end
```

Related Commands

Command	Description
debug auto-ip-ring	Debugs errors or events specific to an auto-IP ring.
show auto-ip-ring	Displays auto-IP ring information.

auto-ip-ring ipv4-seed

To configure an Auto-IP ring port as a seed port, use the **auto-ip-ring ipv4-seed** command in interface configuration mode. To remove the seed port status on an Auto-IP ring port, use the **no** form of this command.

auto-ip-ring *ring-id* **ipv4-seed**
no auto-ip-ring *ring-id* **ipv4-seed**

Syntax Description

ring-id	Auto-IP ring identification number.
ipv4-seed	Specifies the port as the seed port. An Auto-IP ring can have only one seed port.

Command Default

A seed port is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.5(2)S	This command was introduced.
Cisco IOS XE Release 3.15S	This command was integrated into Cisco IOS XE Release 3.15S.

Usage Guidelines

A seed port is an Auto-IP port that initiates the address allocation process. The priority of the seed port is set to 2 (priority of an owner port), an IP address is taken from the pool of IP addresses that is reserved in the Auto-IP server, and automatically configured for the port. The owner port assigns an IP address to its neighbor, a non-owner port. In a similar way, each owner port derives an IP address from the Auto-IP server for itself and also assigns an IP address to the neighbor, a non-owner port.

Examples

The following example shows how to configure an Auto-IP ring port as a seed port:

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 0/0
Device(config-if)# auto-ip-ring 1 ipv4-seed
Device(config-if)# exit
```

Related Commands

Command	Description
auto-ip-ring ipv4-auto	Enables automatic IP address configuration on an Auto-IP ring port from a pool of IP addresses.
auto-ip-ring server	Configures a device in an Auto-IP ring as the Auto-IP server.
show auto-ip-ring	Displays auto-IP ring information.

auto-ip-ring server

To configure a device in an Auto-IP ring as the Auto-IP server, use the **auto-ip-ring server** command in global configuration mode. To remove Auto-IP server status on a device, use the **no** form of this command.

auto-ip-ring server
no auto-ip-ring server

Syntax Description

This command has no arguments or keywords.

Command Default

No device in an Auto-IP ring is configured as an Auto-IP server.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.5(2)S	This command was introduced.
Cisco IOS XE Release 3.15S	This command was integrated into Cisco IOS XE Release 3.15S.

Usage Guidelines

One device in an Auto-IP ring has to be configured as the Auto-IP server. After configuration, you have to reserve a pool of IP addresses for automatic assignment of IP addresses. A sample configuration of the Auto-IP server and reserving of a pool of IP addresses is given below:

```
!
Device(config)# auto-ip-ring server
Device(config-auto-ip-server)# ipv4-address-pool 10.1.1.10 6
!
```

The Auto-IP server allocates IP addresses to the owner ports of the ring and each non-owner port derives its IP address from the owner port through LLDP.

Examples

The following example shows how to configure a device in an Auto-IP ring as the Auto-IP server:

```
Device> enable
Device# configure terminal
Device(config)# auto-ip-ring server
Device(config-auto-ip-server)#
```

Related Commands

Command	Description
debug auto-ip-ring	Debugs errors or events specific to an Auto-IP ring.
ipv4-address-pool	Reserves a pool of IP addresses on the Auto-IP server.
show auto-ip-ring	Displays Auto-IP ring information.

basic-mapping-rule

To configure a basic mapping rule for the mapping of addresses and ports translation (MAP-T), use the **basic-mapping-rule** command in NAT64 MAP-T configuration mode. To remove the basic mapping rule, use the **no** form of this command.

basic-mapping-rule
no basic-mapping-rule

Syntax Description

This command has no arguments or keywords.

Command Default

Mapping rules are not enabled.

Command Modes

NAT64 MAP-T configuration (config-nat64-mapt)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.
Cisco IOS Release 15.5(2)T	This command was integrated into Cisco IOS Release 15.5(2)T.

Usage Guidelines

MAP-T or Mapping of addresses and ports (MAP) double stateless translation-based solution (MAP-T) provides IPv4 hosts connectivity to and across an IPv6 domain.

Examples

The following example shows how to configure the basic mapping rule mode:

```
Device(config)# nat64 map-t domain 3
Device(config-nat64-mapt)# basic-mapping-rule
Device(config-nat64-mapt-bmr)#
```

Related Commands

Command	Description
nat64 map-t	Configures NAT64 MAP-T settings.

bootfile

To specify the name of the default boot image for a Dynamic Host Configuration Protocol (DHCP) client, use the **bootfile** command in DHCP pool configuration mode. To delete the boot image name, use the **no** form of this command.

bootfile *filename*
no bootfile

Syntax Description

filename	Specifies the name of the file that is used as a boot image.

Command Default

No default behavior or values.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies xllboot as the name of the boot file:

```
bootfile xllboot
```

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP Server and enters DHCP pool configuration mode.
next-server	Configures the next server in the boot process of a DHCP client.

cache-memory-max

To allocate a portion of the system memory for cache, use the **cache-memory-max** command in multicast Domain Name System (mDNS) configuration mode. To remove the allocation of a portion of the system memory for cache, use the **no** form of this command.

cache-memory-max *cache-config-percentage*
no cache-memory-max *cache-config-percentage*

Syntax Description

cache-config-percentage	Portion of the system memory, in percentage, that is allocated for cache. **Note** By default, 10 % system memory is allocated for cache. You must use the **cache-memory-max** command to increase the cache memory allocation.

Command Default

10 % system memory is allocated for cache.

Command Modes

Multicast DNS configuration (config-mdns)

Command History

Release	Modification
15.2(1)E	This command was introduced.

Usage Guidelines

You must specify the system memory portion that you want to reserve for cache as a number, without the percentage symbol (%). For 20% allocation for cache memory, you must enter the value 20.

Examples

The following example shows system memory allocation for cache being increased to 20 %:

```
Device> enable
Device# configure terminal
Device(config)# service-routing mdns-sd
Device(config-mdns)# cache-memory-max 20
Device(config-mdns)# exit
```

Related Commands

Command	Description
service-routing mdns-sd	Enables mDNS gateway functionality for a device.

class (DHCP)

To associate a class with a Dynamic Host Configuration Protocol (DHCP) address pool and enter DHCP pool class configuration mode, use the **class** command in DHCP pool configuration mode. To remove the class association, use the **no** form of this command.

class *class-name*
no class *class-name*

Syntax Description

class-name	Name of the DHCP class.

Command Default

No class is associated with the DHCP address pool.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

You must first define the class using the **ip dhcp class** command available in global configuration command. If a nonexistent class is named by the **class** command, the class will be automatically created. Each class in the DHCP pool will be examined for a match in the order configured.

Examples

The following example shows how to associate DHCP class 1 and class 2 with a DHCP pool named pool1:

```
Router(config)# ip dhcp pool pool1
Router(dhcp-config)# network 10.0.20.0 255.255.255.0
Router(dhcp-config)# class class1
Router(config-dhcp-pool-class)# address range 10.0.20.1 10.0.20.100
Router(config-dhcp-pool-class)# exit
Router(dhcp-config)# class class2
Router(config-dhcp-pool-class)# address range 10.0.20.101 10.0.20.200
```

Related Commands

Command	Description
ip dhcp class	Defines a DHCP class and enters DHCP class configuration mode.

clear arp interface

To clear the entire Address Resolution Protocol (ARP) cache on an interface, use the **clear arp interface** command in privileged or user EXEC mode.

clear arp interface *type number*

Syntax Description

type	Interface type.
number	Interface number.

Command Default

No default behavior or values.

Command Modes

Privileged or User EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **clear arp interface** command to clean up ARP entries associated with an interface.

Examples

The following example clears the ARP cache from Ethernet interface 0:

```
Router# clear arp interface ethernet 0
```

clear arp-cache

To refresh dynamically created entries from the Address Resolution Protocol (ARP) cache, use the **clear arp-cache** command in privileged EXEC mode.

clear arp-cache [**interface** *type number* | [**vrf** *vrf-name*] *ip-address*]

Syntax Description

interface *type number*	(Optional) Refreshes only the ARP table entries associated with this interface.
vrf *vrf-name*	(Optional) Refreshes only the ARP table entries for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance and the IP address specified by the *ip-address* argument.
ip-address	(Optional) Refreshes only the ARP table entries for the specified IP address.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.4(11)T	The **interface** keyword and the *type* and *number* arguments were made optional to support refreshing of entries for a single router interface. The **vrf** keyword, the *vrf-name* argument, and the *ip-address* argument were added to support refreshing of entries of a specified address and an optionally specified VRF.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command updates the dynamically learned IP address and MAC address mapping information in the ARP table to ensure the validity of those entries. If the refresh operation encounters any stale entries (dynamic ARP entries that have expired but have not yet been aged out by an internal, timer-driven process), those entries are aged out of the ARP table immediately as opposed to at the next refresh interval.



Note By default, dynamically learned ARP entries remain in the ARP table for four hours.

The **clear arp-cache** command can be entered multiple times to refresh dynamically created entries from the ARP cache using different selection criteria.

- Use this command without any arguments or keywords to refresh all ARP cache entries for all enabled interfaces.
- To refresh ARP cache entries for a specific interface, use this command with the **interface** keyword and *type* and *number* arguments.



Tip The valid interface types and numbers can vary according to the router and the interfaces on the router. To list all the interfaces configured on a particular router, use the **show interfaces** command with the **summary** keyword. Use the appropriate interface specification, typed exactly as it is displayed under the Interface column of the **show interfaces** command output, to replace the *type* and *number* arguments in the **clear arp-cache interface** command.

- To refresh ARP cache entries from the global VRF and for a specific host, use this command with the *ip-address* argument.
- To refresh ARP cache entries from a named VRF and for a specific host, use this command with the **vrf** keyword and the *vrf-name* and *ip-address* arguments.

To display ARP table entries, use the **show arp** command.

This command does not affect permanent entries in the ARP cache, and it does not affect the ARP HA statistics:

- To remove static ARP entries from the ARP cache, use the **no** form of the **arp** command.
- To remove alias ARP entries from the ARP cache, use the **no** form of the **arp** command with the **alias** keyword.
- To reset the ARP HA status and statistics, use the **clear arp-cache counters ha** command.

Examples

The following example shows how to refresh all dynamically learned ARP cache entries for all enabled interfaces:

```
Router# clear arp-cache
```

The following example shows how to refresh dynamically learned ARP cache entries for the Ethernet interface at slot 1, port 2:

```
Router# clear arp-cache interface ethernet 1/2
```

The following example shows how to refresh dynamically learned ARP cache entries for the host at 192.0.2.140:

```
Router# clear arp-cache 192.0.2.140
```

The following example shows how to refresh dynamically learned ARP cache entries from the VRF named vpn3 and for the host at 192.0.2.151:

```
Router# clear arp-cache vrf vpn3 192.0.2.151
```

Related Commands

Command	Description
arp (global)	Configures a permanent entry in the ARP cache.
arp timeout	Configures how long a dynamically learned IP address and its corresponding MAC address remain in the ARP cache.
clear arp-cache counters ha	Resets the ARP HA statistics.
show arp	Displays ARP table entries.
show interfaces	Displays statistics for all interfaces configured on the router or access server.

clear arp-cache counters ha

To reset the Address Resolution Protocol (ARP) high availability (HA) statistics, use the **clear arp-cache counters ha** command in privileged EXEC mode.

clear arp-cache counters ha

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

Use the **clear arp-cache counters ha** command to reset all ARP high availability statistics for all enabled interfaces.

To display the ARP HA status and statistics, use the **show arp ha** command.



Note The **clear arp-cache counters ha** command and the **show arp ha** command are available only on HA-capable platforms (that is, Cisco networking devices that support dual Route Processors [RPs]).

Examples

The following example shows how to reset the ARP HA statistics:

```
Router# clear arp-cache counters ha
```

Related Commands

Command	Description
clear arp-cache	Refreshes dynamically learned entries in the ARP cache.
show arp ha	Displays the ARP HA status and statistics.

clear host

To delete hostname-to-address mapping entries from one or more hostname caches, use the **clear host** command in privileged EXEC mode.

clear host [**view** *view-name* | **vrf** *vrf-name* | **all**] {*hostname* | *****}

Syntax Description

view *view-name*	(Optional) The *view-name* argument specifies the name of the Domain Name System (DNS) view whose hostname cache is to be cleared. Default is the default DNS view associated with the specified or global Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf *vrf-name*	(Optional) The *vrf-name* argument specifies the name of the VRF associated with the DNS view whose hostname cache is to be cleared. Default is the global VRF (that is, the VRF whose name is a NULL string) with the specified or default DNS view.
all	(Optional) Specifies that hostname-to-address mappings are to be deleted from the hostname cache of every configured DNS view.
hostname	Name of the host for which hostname-to-address mappings are to be deleted from the specified hostname cache.
*****	Specifies that all the hostname-to-address mappings are to be deleted from the specified hostname cache.

Command Default

No hostname-to-address mapping entries are deleted from any hostname cache.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.4(4)T	The **vrf** keyword, *vrf-name* argument, and **all** keyword were added.
12.4(9)T	The **view** keyword and *view-name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command clears the specified hostname cache entries in running memory, but it does not remove the entries from NVRAM.

Entries can be removed from the hostname caches for a DNS view name, from the hostname caches for a VRF, or from all configured hostname caches. To remove entries from hostname caches for a particular DNS view name, use the **view** keyword and *view-name* argument. To remove entries from the hostname caches for a particular VRF, use the **vrf** keyword and *vrf-name* argument. To remove entries from all configured hostname caches, use the **all** keyword.

To remove entries that provide mapping information for a single hostname, use the *hostname* argument. To remove all entries, use the ***** keyword.

To display the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views, use the **show hosts** command.

To define static hostname-to-address mappings in the DNS hostname cache for a DNS view, use the **ip host** command.

Examples

The following example shows how to clear all entries from the hostname cache for the default view in the global address space:

```
Router# clear host all *
```

The following example shows how to clear entries for the hostname www.example.com from the hostname cache for the default view associated with the VPN named vpn101:

```
Router# clear host vrf vpn101 www.example.com
```

The following example shows how to clear all entries from the hostname cache for the view named user2 in the global address space:

```
Router# clear host view user2 *
```

Related Commands

Command	Description
ip host	Defines static hostname-to-address mappings in the DNS hostname cache for a DNS view.
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views.

clear ip arp inspection log

To clear the status of the log buffer, use the **clear ip arp inspection log**command in privileged EXEC mode.

clear ip arp inspection log

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to clear the contents of the log buffer:

```
Router#
clear ip arp inspection log
```

Related Commands

Command	Description
arp access-list	Configures an ARP ACL for ARP inspection and QoS filtering and enter the ARP ACL configuration submode.
show ip arp inspection log	Displays the status of the log buffer.

clear ip arp inspection statistics

To clear the dynamic ARP inspection statistics, use the **clear ip arp inspection statistics**command in privileged EXEC mode.

clear ip arp inspection statistics [**vlan** *vlan-range*]

Syntax Description

vlan *vlan-range*	(Optional) Specifies the VLAN range.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to clear the DAI statistics from VLAN 1:

```
Router# clear ip arp inspection statistics vlan 1
```

Related Commands

Command	Description
arp access-list	Configures an ARP ACL for ARP inspection and QoS filtering and enter the ARP ACL configuration submode.
clear ip arp inspection log	Clears the status of the log buffer.
show ip arp inspection log	Displays the status of the log buffer.

clear ip arp poll statistics

To clear the IP Address Resolution Protocol (ARP) host polling information, use the **clear ip arp poll statistics** command in privileged EXEC mode.

clear ip arp poll statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)SY	This command was introduced.

Examples

The following example shows how to clear the IP ARP host polling information:

```
Device# clear ip arp poll statistics
```

Related Commands

Command	Description
ip arp poll	Configures IP ARP polling for unnumbered interfaces.
show ip arp poll	Displays the IP ARP host polling status.

clear ip dhcp binding

To delete an automatic address binding from the Dynamic Host Configuration Protocol (DHCP) server database, use the **clear ip dhcp binding** command in privileged EXEC mode.

clear ip dhcp [**pool** *name*] **binding** [**vrf** *vrf-name*] {***address**}

Syntax Description

pool *name*	(Optional) Specifies the name of the DHCP pool.
vrf	(Optional) Clears virtual routing and forwarding (VRF) information from the DHCP database.
vrf-name	(Optional) The VRF name.
*	Clears all automatic bindings.
address	The address of the binding you want to clear.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(8)T	The **pool** keyword and *name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.6	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

Typically, the address denotes the IP address of the client. If the asterisk (*) character is used as the address parameter, DHCP clears all automatic bindings.

Use the **no ip dhcp binding** command in global configuration mode to delete a manual binding.

Note the following behavior for the **clear ip dhcp binding**command:

- If you do not specify the **pool** *name* option and an IP address is specified, it is assumed that the IP address is an address in the global address space and will look among all the nonvirtual VRF DHCP pools for the specified binding.
- If you do not specify the **pool** *name* option and the * option is specified, it is assumed that all automatic or on-demand bindings in all VRF and non-VRF pools are to be deleted.
- If you specify both the **pool** *name* option and the * option, all automatic or on-demand bindings in the specified pool only will be cleared.

- If you specify the **pool** *name* option and an IP address, the specified binding will be deleted from the specified pool.

Examples

The following example shows how to delete the address binding 10.12.1.99 from a DHCP server database:

```
Router# clear ip dhcp binding 10.12.1.99
```

The following example shows how to delete all bindings from all pools:

```
Router# clear ip dhcp binding *
```

The following example shows how to delete all bindings from the address pool named pool1:

```
Router# clear ip dhcp pool pool1 binding *
```

The following example shows how to delete address binding 10.13.2.99 from the address pool named pool2:

```
Router# clear ip dhcp pool pool2 binding 10.13.2.99
```

The following example shows how to delete VRF vrf1 from the DHCP database:

```
Router# clear ip dhcp binding vrf vrf1 10.13.2.99
```

Related Commands

Command	Description
show ip dhcp binding	Displays address bindings on the Cisco IOS DHCP server.

clear ip dhcp conflict

To clear an address conflict from the Dynamic Host Configuration Protocol (DHCP) server database, use the **clear ip dhcp conflict** command in privileged EXEC mode.

clear ip dhcp [**pool** *name*] **conflict** [**vrf** *vrf-name*] {***address**}

Syntax Description

pool *name*	(Optional) Specifies the name of the DHCP pool.
vrf	(Optional) Clears DHCP virtual routing and forwarding (VRF) conflicts.
vrf-name	(Optional) The VRF name.
*	Clears all address conflicts.
address	The IP address of the host that contains the conflicting address you want to clear.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(8)T	The **pool** keyword and *name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.6	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

The server detects conflicts using a ping session. The client detects conflicts using gratuitous Address Resolution Protocol (ARP). If the asterisk (*) character is used as the address parameter, DHCP clears all conflicts.

Note the following behavior for the **clear ip dhcp conflict** command:

- If you do not specify the **pool** *name* option and an IP address is specified, it is assumed that the IP address is an address in the global address space and will look among all the nonvirtual VRF DHCP pools for the specified conflict.
- If you do not specify the **pool** *name* option and the * option is specified, it is assumed that all automatic/or on-demand conflicts in all VRF and non-VRF pools are to be deleted.
- If you specify both the **pool** *name* option and the * option, all automatic or on-demand conflicts in the specified pool only will be cleared.
- If you specify the **pool** *name* option and an IP address, the specified conflict will be deleted from the specified pool.

Examples

The following example shows how to delete an address conflict of 10.12.1.99 from the DHCP server database:

```
Router# clear ip dhcp conflict 10.12.1.99
```

The following example shows how to delete all address conflicts from all pools:

```
Router# clear ip dhcp conflict *
```

The following example shows how to delete all address conflicts from the address pool named pool1:

```
Router# clear ip dhcp pool pool1
conflict *
```

The following example shows how to delete address conflict 10.13.2.99 from the address pool named pool2:

```
Router# clear ip dhcp pool pool2 conflict 10.13.2.99
```

The following example shows how to delete VRF vrf1 from the DHCP database:

```
Router# clear ip dhcp conflict vrf vrf1 10.13.2.99
```

Related Commands

Command	Description
show ip dhcp conflict	Displays address conflicts found by a Cisco IOS DHCP server when addresses are offered to the client.

clear ip dhcp limit lease

To clear lease limit violation entries, use the **clear ip dhcp limit lease**command in privileged EXEC mode.

clear ip dhcp limit lease [*type number*]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (?) online help function.
number	(Optional) Interface or subinterface number. For more information about the numbering system for your networking device, use the question mark (?) online help function.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.

Usage Guidelines

The **show ip dhcp limit lease** command displays the number of lease limit violations. You can control the number of subscribers at the global level by using the **ip dhcp limit lease per interface** command and at the interface level by using the **ip dhcp limit lease**command.

Examples

In the following example, the number of lease violations is displayed and then cleared:

```
Router# show ip dhcp limit lease
Interface        Count
Serial0/0.1      5
Serial1          3
Router# clear ip dhcp limit lease
Router# show ip dhcp limit lease
```

Related Commands

Command	Description
ip dhcp limit lease	Limits the number of leases offered to DHCP clients per interface.
ip dhcp limit lease per interface	Limits the number of DHCP leases offered to DHCP clients behind an ATM RBE unnumbered or serial unnumbered interface.
show ip dhcp limit lease	Displays the number of times the lease limit threshold has been violated on an interface.

clear ip dhcp server statistics

To reset all Dynamic Host Configuration Protocol (DHCP) server counters, use the **clear ip dhcp server statistics** command in privileged EXEC mode.

clear ip dhcp server statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show ip dhcp server statistics** command displays DHCP counters. All counters are cumulative. The counters will be initialized, or set to zero, with the **clear ip dhcp server statistics** command.

Examples

The following example resets all DHCP counters to zero:

```
Router# clear ip dhcp server statistics
```

Related Commands

Command	Description
show ip dhcp server statistics	Displays Cisco IOS DHCP server statistics.

clear ip dhcp snooping binding

To clear the DHCP-snooping binding-entry table without disabling DHCP snooping, use the **clear ip dhcp snooping binding** command in privileged EXEC mode.

clear ip dhcp snooping binding

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to clear the DHCP-snooping binding-entry table:

```
Router# clear ip dhcp snooping binding
```

clear ip dhcp snooping database statistics

To clear the DHCP binding database statistics, use the **clear ip dhcp snooping database statistics**command in privileged EXEC mode.

clear ip dhcp snooping database statistics

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example shows how to clear the statistics from the DHCP binding database:

```
Router# clear ip dhcp snooping database statistics
```

clear ip dhcp snooping statistics

To clear the DHCP snooping statistics, use the **clear ip dhcp snooping statistics** command in privileged EXEC mode.

clear ip dhcp snooping statistics

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to clear the DHCP snooping statistics:

```
Router# clear ip dhcp snooping statistics
```

clear ip dhcp subnet

To clear all currently leased subnets in the Dynamic Host Configuration Protocol (DHCP) pool, use the **clear ip dhcp subnet**command in privileged EXEC configuration mode.

clear ip dhcp [**pool** *name*] **subnet** {***address**}

Syntax Description

pool *name*	(Optional) Name of the DHCP pool.
*	Clears all leased subnets.
address	Clears a subnet containing the specified IP address.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

A PPP session that is allocated an IP address from the released subnet will be reset.

Note the following behavior for the **clear ip dhcp subnet** command:

- If you do not specify the **pool** *name* option and an IP address is specified, it is assumed that the IP address is an address in the global address space and will look among all the non-virtual routing and forwarding (VRF) DHCP pools for the specified subnet.
- If you do not specify the **pool** *name* option and the * option is specified, it is assumed that all automatic or on-demand subnets in all VRF and non-VRF pools are to be deleted.
- If you specify both the **pool** *name* option and the * option, all automatic or on-demand subnets in the specified pool only will be cleared.
- If you specify the **pool** *name* option and an IP address, the subnet containing the specified IP address will be deleted from the specified pool.



Caution Use this command with caution to prevent undesired termination of active PPP sessions.

Examples

The following example releases the subnet containing 10.0.0.2 from any non-VRF on-demand address pools:

```
Router# clear ip dhcp subnet 10.0.0.2
```

The following example clears all leased subnets from all pools:

```
Router# clear ip dhcp subnet *
```

The following example clears all leased subnets from the address pool named pool3:

```
Router# clear ip dhcp pool pool3 subnet *
```

The following example clears the address 10.0.0.2 from the address pool named pool2:

```
Router# clear ip dhcp pool pool2 subnet 10.0.0.2
```

Related Commands

Command	Description
show ip dhcp pool	Displays information about the DHCP address pools.

clear ip interface

To clear the IP interface statistics, use the **clear ip interface** command in privileged EXEC mode.

clear ip interface *type number* [**stats** | **topology** {*instance-name* | **all** | **base**} **stats**]

Syntax Description

type number	Interface type and number.
stats	(Optional) Clears the statistics summary.
topology	(Optional) Clears topology statistics.
instance-name	(Optional) Name of the instance for which topology statistics are to be cleared.
all	(Optional) Clears all topology statistics.
base	(Optional) Clears base topology statistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)SY	This command was introduced.

Usage Guidelines

The interface that borrows its address from one of the device's other functional interfaces is called the *unnumbered interface*. The IP unnumbered interfaces help in conserving network and address space. Use the **clear ip interface** command to clear the IP interface statistics for IP numbered and unnumbered interfaces.

Examples

The following example shows how to clear all topology statistics for a loopback interface:

```
Device(#)clear ip interface loopback0 topology all stats
```

Related Commands

Command	Description
show ip interface	Displays the usability status of interfaces configured for IP.
show ip interface unnumbered	Displays the status of unnumbered interface support on specific interfaces.

clear ip nat translation

To clear dynamic Network Address Translation (NAT) translations from the translation table, use the **clear ip nat translation**commandinEXEC mode.

clear ip nat translation {***** | **forced** | [**piggyback-internal** | **esp** | **tcp** | **udp**] [**inside** *global-ip* [*global-port*] *local-ip* [*local-port*] **outside** *local-ip global-ip*] | [**inside** *global-ip local-ip* [**forced**]] | [**outside** *local-ip global-ip* [**forced**]]}

Syntax Description

*****	Clears all dynamic translations.
forced	(Optional) Forces the clearing of either: • all dynamic entries, whether or not there are any child translations. • a single dynamic half-entry and any existing child translations, whether or not there are any child translations.
piggyback-internal	(Optional) Clears translations created off of piggyback data.
esp	(Optional) Clears Encapsulating Security Payload (ESP) entries from the translation table.
tcp	(Optional) Clears the TCP entries from the translation table.
udp	(Optional) Clears the User Datagram Protocol (UDP) entries from the translation table.
inside	(Optional) Clears the inside translations containing the specified *global-ip* and *local-ip* addresses. If used without the **forced** keyword, clears only those entries that do not have child translations.
global-ip	(Optional) Global IP address.
global-port	(Optional) Global port.
local-ip	(Optional) Local IP address.
local-port	(Optional) Local port.
outside	(Optional) Clears the outside translations containing the specified *local-ip* and *global-ip* addresses. If used without the **forced** keyword, clears only those entries that do not have child translations.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(15)T	The **esp** keyword was added.

Release	Modification
12.2 (33) XND	The **forced** keyword was extended to support the removal of a half entry regardless of whether it has any child translations.
12.4(2)T	The **piggyback-internal** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
XE 2.4.2	The **forced** keyword was extended to support the removal of a half entry regardless of whether it has any child translations.

Usage Guidelines

Use this command to clear entries from the translation table before they time out.

Examples

The following example shows the NAT entries before and after the User Datagram Protocol (UDP) entry is cleared:

```
Router> show ip nat translations
Pro Inside global        Inside local       Outside local      Outside global
udp 10.69.233.209:1220  10.168.1.95:1220   10.69.2.132:53     10.69.2.132:53
tcp     10.69.233.208       10.168.1.94
tcp 10.69.233.209:11012 10.168.1.89:11012  10.69.1.220:23     10.69.1.220:23
tcp 10.69.233.209:1067  10.168.1.95:1067   10.69.1.161:23     10.69.1.161:23
Router# clear ip nat translation udp inside 10.69.233.209 1220 10.168.1.95 1220
outside 10.69.2.132 53 10.69.2.132 53
Router# show ip nat translations

Pro     Inside global       Inside local       Outside local      Outside global
tcp     10.69.233.208       10.168.1.94
tcp     10.69.233.209:11012 10.168.1.89:11012  10.69.1.220:23     10.69.1.220:23
tcp     10.69.233.209:1067  10.168.1.95:1067   10.69.1.161:23     10.69.1.161:23
Router# clear ip nat translation inside 10.69.233.208 10.168.1.94 forced
Router# show ip nat translations

Pro     Inside global       Inside local       Outside local      Outside global
tcp     10.69.233.209:11012 10.168.1.89:11012  10.69.1.220:23     10.69.1.220:23
tcp     10.69.233.209:1067  10.168.1.95:1067   10.69.1.161:23     10.69.1.161:23
```

Related Commands

Command	Description
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Changes the amount of time after which NAT translations time out.

Command	Description
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

clear ip nat translation redundancy

To clear IP Network Address Translation (NAT) redundancy translations, use the **clear ip nat translation redundancy** command in privileged EXEC mode.

clear ip nat translation redundancy *RG-id* {***** | **forced**}

Syntax Description

*****	Clears all dynamic translations.
forced	Clears all dynamics forcefully.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.3(2)T	This command was introduced.

Usage Guidelines

Use the **clear ip nat translation redundancy** command to clear IP NAT redundancy translations. It is not recommended to execute this command on a device which is currently in the standby redundancy state.

Example

The following example shows how to all clear IP NAT redundancy translations.

```
Device# clear ip nat translation redundancy *
```

Related Commands

Command	Description
show ip nat redundancy	Displays NAT redundancy information
show ip nat translations redundancy	Displays active NAT translations.

clear ip nhrp

To clear all dynamic entries from the Next Hop Resolution Protocol (NHRP) cache, use the **clear ip nhrp** command in user EXEC or privileged EXEC mode.

clear ip nhrp[*dest-ip-address* [*dest-mask*]][**counters** | [**interface** | {**tunnel** *number* | **Virtual-Access** *number*} | **vrf** *vrf-name*]][**shortcut** | [**interface** | {**tunnel** *number* | **Virtual-Access** *number*}]]

Syntax Description

dest-ip-address	(Optional) Destination IP address. Specifying this argument clears NHRP mapping entries for the specified destination IP address.
dest-mask	(Optional) Destination network mask.
counters	(Optional) Clears the NHRP counters.
interface	(Optional) Clears the NHRP mapping entries for all interfaces.
tunnel *number*	Removes the specified interface name from the NHRP cache that all entries learned using this tunnel interface.
Virtual-Access *number*	Removes the specified interface name from the NHRP cache that all entries learned using this virtual access interface.
vrf	(Optional) Deletes entries from the NHRP cache for the specified VPN Routing and Forwarding (VRF) and Front VRF (FVRF).
vrf-name	Name of the VRF address family to which the command is applied.
shortcut	(Optional) Deletes shortcut entries from the NHRP cache.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.5	This command was modified. The **shortcut** keyword was added.
15.3(2)T	This command was modified. The behavior of the **interface** keyword was updated to clear NHRP mapping entries for all interfaces. The **Virtual-Access** *number* keyword-argument pair was added.

Usage Guidelines

The **clear ip nhrp** command does not clear any static (configured) IP-to-NBMA address mappings from the NHRP cache. The **clear ip nhrp shortcut** command clears NHRP cache entries that have associated NHRP routes or next-hop overrides in the Routing Information Base (RIB).

The **clear ip nhrp** command clears Front VRF (FVRF) counters. It does not clear Internal VRF (IVRF) counters.

Replacing **ip** in the command name with **ipv6** clears IPv6-specific cache.

Examples

The following example shows how to clear all dynamic entries from the NHRP cache for an interface:

```
Device# clear ip nhrp
```

The following example shows how to clear the NHRP cache entries that have associated NHRP routes or next-hop overrides in the RIB:

```
Device# clear ip nhrp shortcut
```

Related Commands

Command	Description
show ip nhrp	Displays NHRP mapping information.

clear ip route

To delete routes from the IP routing table, use the **clear ip route** command in EXEC mode.

clear ip route {*network* [*mask*] | ***}

Syntax Description

network	Network or subnet address to remove.
mask	(Optional) Subnet address to remove.
*	Removes all routing table entries.

Command Default

All entries are removed.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example removes a route to network 10.5.0.0 from the IP routing table:

```
Router> clear ip route 10.5.0.0
```



clear ip route dhcp through ip arp entry learn

- clear ip route dhcp, on page 79
- clear ip snat sessions, on page 80
- clear ip snat translation distributed, on page 81
- clear ip snat translation peer, on page 82
- clear ip dhcp snooping database statistics, on page 83
- clear ip translation peer, on page 84
- clear ipv6 dhcp, on page 85
- clear ipv6 dhcp binding, on page 86
- clear ipv6 dhcp client, on page 88
- clear ipv6 dhcp conflict, on page 89
- **clear ipv6 dhcp-ldra statistics** , on page 90
- clear ipv6 dhcp relay binding, on page 92
- clear ipv6 dhcp route, on page 94
- clear ipv6 nat translation, on page 95
- clear logging ip access-list cache, on page 96
- clear mdns cache, on page 97
- clear mdns service-types, on page 98
- clear mdns statistics, on page 99
- clear nat64 ha statistics, on page 101
- clear nat64 statistics, on page 102
- clear nat64 translations, on page 104
- client-identifier, on page 105
- client-name, on page 107
- control, on page 108
- data, on page 110
- ddns (DDNS-update-method), on page 111
- default-mapping-rule, on page 112
- default-router, on page 113
- designated-gateway, on page 114
- device-role (DHCPv6 Guard), on page 116
- dns forwarder, on page 117
- dns forwarding, on page 119
- dns forwarding source-interface, on page 121

- dns-server, on page 123
- dns-server (config-dhcp-global-options), on page 124
- dns-server (IPv6), on page 125
- domain list, on page 126
- domain lookup, on page 128
- domain multicast, on page 130
- domain name, on page 131
- domain-name (IPv6), on page 133
- domain name-server, on page 134
- domain name-server interface, on page 136
- domain resolver source-interface, on page 139
- domain retry, on page 140
- domain round-robin, on page 141
- domain timeout, on page 143
- domain-name (DHCP), on page 144
- designated-gateway, on page 145
- group (firewall), on page 147
- hardware-address, on page 148
- host, on page 151
- host (host-list), on page 153
- http (DDNS-update-method), on page 155
- import all, on page 159
- import dns-server, on page 160
- import domain-name, on page 161
- import information refresh, on page 162
- import nis address, on page 163
- import nis domain-name, on page 164
- import nisp address, on page 165
- import nisp domain-name, on page 166
- import sip address, on page 167
- import sip domain-name, on page 168
- import sntp address, on page 169
- information refresh, on page 171
- internal (DDNS-update-method), on page 173
- interval maximum, on page 174
- interval minimum, on page 175
- ip address, on page 177
- ip address dhcp, on page 180
- ip address pool (DHCP), on page 183
- ip arp entry learn, on page 184

clear ip route dhcp

To remove routes from the routing table added by the Cisco IOS Dynamic Host Configuration Protocol (DHCP) server and relay agent for the DHCP clients on unnumbered interfaces, use the **clear ip route dhcp**command in EXEC mode.

clear ip route [**vrf** *vrf-name*] **dhcp** [*ip-address*]

Syntax Description

vrf	(Optional) VPN routing and forwarding instance (VRF).
vrf-name	(Optional) Name of the VRF.
ip-address	(Optional) Address about which routing information should be removed.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To remove information about global routes in the routing table, use the **clear ip route dhcp** command. To remove routes in the VRF routing table, use the **clear ip route vrf** *vrf-name* **dhcp** command.

Examples

The following example removes a route to network 10.5.5.217 from the routing table:

```
Router# clear ip route dhcp 10.5.5.217
```

Related Commands

Command	Description
show ip route dhcp	Displays the routes added to the routing table by the Cisco IOS DHCP server and relay agent.

clear ip snat sessions

To clear dynamic Stateful Network Address Translation (SNAT) sessions from the translation table, use the **clear ip snat sessions**command in EXEC mode.

clear ip snat sessions * [**ip-address-peer**]

Syntax Description

*	Removes all dynamic entries.
ip-address-peer	(Optional) Removes SNAT entries of the peer translator.

Command Modes

EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Use this command to clear entries from the translation table before they time out.

Examples

The following example shows the SNAT entries before and after using the **clear ip snat sessions** command:

```
Router> show ip snat distributed
SNAT:Mode PRIMARY
    :State READY
    :Local Address 10.168.123.2
    :Local NAT id 100
    :Peer Address 10.168.123.3
    :Peer NAT id 200
    :Mapping List 10
Router> clear ip snat sessions *
Closing TCP session to peer:10.168.123.3
Router> show ip snat distributed
```

clear ip snat translation distributed

To clear dynamic Stateful Network Address Translation (SNAT) translations from the translation table, use the **clear ip snat translation distributed**command in EXEC mode.

clear ip snat translation distributed *

Syntax Description

*	Removes all dynamic SNAT entries.

Command Modes

EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Use this command to clear entries from the translation table before they time out.

Examples

The following example clears all dynamic SNAT translations from the translation table:

```
Router# clear ip snat translation distributed *
```

clear ip snat translation peer

To clear peer Stateful Network Address Translation (SNAT) translations from the translation table, use the **clear ip snat translation peer**command in EXEC mode.

clear ip snat translation peer ip-address-peer [**refresh**]

Syntax Description

ip-address-peer	IP address of the peer translator.
refresh	(Optional) Provides a fresh dump of the NAT table from the peer.

Command Modes

EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Use this command to clear peer entries from the translation table before they time out.

Examples

The following example shows the SNAT entries before and after the peer entry is cleared:

```
Router# show ip snat peer
Pro Inside global      Inside local       Outside local      Outside global
--- 192.168.25.20      192.168.122.20     ---                ---
tcp 192.168.25.20:33528 192.168.122.20:33528 192.168.24.2:21 192.168.24.2:21
Router# clear ip snat translation peer 192.168.122.20
```

clear ip dhcp snooping database statistics

To clear the DHCP binding database statistics, use the **clear ip dhcp snooping database statistics** command in privileged EXEC mode.

clear ip dhcp snooping database statistics

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to clear the statistics from the DHCP binding database:

```
Router# clear ip dhcp snooping database statistics
```

clear ip translation peer

To clear or reset the Network Address Translation (NAT) entries created by the Stateful Failover of Network Address Translation (SNAT) peer router and retreive a list of NAT entries, use the **clear ip translation peer** command in privileged EXEC mode.

clear ip translation peer *ip-address* **refresh**

Syntax Description

ip-address	IP address of the SNAT peer router.
refresh	Retrieves a list of NAT entries from the SNAT peer router.

Command Default

The NAT entries created by the SNAT peer router are recorded.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows how to retrieve a list of NAT entries and clear the NAT entries created by the SNAT peer router:

```
Router# clear ip translation peer 10.1.1.1 refresh
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.

clear ipv6 dhcp

To clear IPv6 Dynamic Host Configuration Protocol (DHCP) information, use the **clear ipv6 dhcp**command in privileged EXEC mode:

clear ipv6 dhcp

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

The **clear ipv6 dhcp** command deletes DHCP for IPv6 information.

Examples

The following example :

```
Router# clear ipv6 dhcp
```

clear ipv6 dhcp binding

To delete automatic client bindings from the Dynamic Host Configuration Protocol (DHCP) for IPv6 server binding table, use the **clear ipv6 dhcp binding** command in privileged EXEC mode.

clear ipv6 dhcp binding [*ipv6-address*] [**vrf** *vrf-name*]

Syntax Description

ipv6-address	(Optional) The address of a DHCP for IPv6 client. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4(24)T	This command was modified. It was updated to allow for clearing all address bindings associated with a client.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Routers.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)SXE.
15.1(2)S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
Cisco IOS XE Release 3.3S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Usage Guidelines

The **clear ipv6 dhcp binding** command is used as a server function.

A binding table entry on the DHCP for IPv6 server is automatically:

- Created whenever a prefix is delegated to a client from the configuration pool.
- Updated when the client renews, rebinds, or confirms the prefix delegation.
- Deleted when the client releases all the prefixes in the binding voluntarily, all prefixes' valid lifetimes have expired, or an administrator runs the **clear ipv6 dhcp binding** command.

If the **clear ipv6 dhcp binding** command is used with the optional *ipv6-address* argument specified, only the binding for the specified client is deleted. If the **clear ipv6 dhcp binding** command is used without the *ipv6-address* argument, then all automatic client bindings are deleted from the DHCP for IPv6 binding table. If the optional **vrf** *vrf-name* keyword and argument combination is used, only the bindings for the specified VRF are cleared.

Examples

The following example deletes all automatic client bindings from the DHCP for IPv6 server binding table:

```
Router# clear ipv6 dhcp binding
```

Related Commands

Command	Description
show ipv6 dhcp binding	Displays automatic client bindings from the DHCP for IPv6 server binding table.

clear ipv6 dhcp client

To restart the Dynamic Host Configuration Protocol (DHCP) for IPv6 client on an interface, use the **clear ipv6 dhcp client** command in privileged EXEC mode.

clear ipv6 dhcp client *interface-type interface-number*

Syntax Description

interface-type interface-number	Interface type and number. For more information, use the question mark (**?**) online help function.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SXE.

Usage Guidelines

The **clear ipv6 dhcp client** command restarts the DHCP for IPv6 client on specified interface after first releasing and unconfiguring previously acquired prefixes and other configuration options (for example, Domain Name System [DNS] servers).

Examples

The following example restarts the DHCP for IPv6 client for Ethernet interface 1/0:

```
Router# clear ipv6 dhcp client Ethernet 1/0
```

Related Commands

Command	Description
show ipv6 dhcp interface	Displays DHCP for IPv6 interface information.

clear ipv6 dhcp conflict

To clear an address conflict from the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server database, use the **clear ipv6 dhcp conflict** command in privileged EXEC mode.

clear ipv6 dhcp conflict {***** *ipv6-address* | **vrf** *vrf-name*}

Syntax Description

*	Clears all address conflicts.
ipv6-address	Clears the host IPv6 address that contains the conflicting address.
vrf *vrf-name*	Specifies a virtual routing and forwarding (VRF) name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced.
15.1(2)S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
Cisco IOS XE Release 3.3S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Usage Guidelines

When you configure the DHCPv6 server to detect conflicts, it uses ping. The client uses neighbor discovery to detect clients and reports to the server through a DECLINE message. If an address conflict is detected, the address is removed from the pool, and the address is not assigned until the administrator removes the address from the conflict list.

If you use the asterisk (*) character as the address parameter, DHCP clears all conflicts.

If the **vrf** *vrf-name* keyword and argument are specified, only the address conflicts that belong to the specified VRF will be cleared.

Examples

The following example shows how to clear all address conflicts from the DHCPv6 server database:

```
Router# clear ipv6 dhcp conflict *
```

Related Commands

Command	Description
show ipv6 dhcp conflict	Displays address conflicts found by a DHCPv6 server when addresses are offered to the client.

clear ipv6 dhcp-ldra statistics

To clear Lightweight DHCPv6 Relay Agent (LDRA) related statistics, use the **clear ipv6 dhcp-ldra statistics** command in user EXEC or privileged EXEC mode.

clear ipv6 dhcp-ldra statistics [*interface-type number*]

Syntax Description

interface-type	(Optional) Interface type. For more information, use the question mark (?) online help function.
number	(Optional) Interface number.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)SG	This command was introduced.
Cisco IOS XE Release 3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.

Usage Guidelines

The following interfaces are allowed and can be used for the *interface-type* argument:

- FastEthernet
- GigabitEthernet
- Loopback
- Lspvif
- null
- Port-channel
- TenGigabitEthernet
- Tunnel

Example

The following clears LDRA-related statistics for the GigabitEthernet 0/1 interface:

```
Device> enable
Device# clear ipv6 dhcp-ldra statistics GigabitEthernet 0/1
Device# exit
```

Related Commands

Command	Description
ipv6 dhcp-ldra	Enables LDRA functionality on an access node.

Command	Description
ipv6 dhcp ldra attach-policy	Enables LDRA functionality on a VLAN.
ipv6 dhcp-ldra attach-policy	Enables LDRA functionality on an interface.

clear ipv6 dhcp relay binding

To clear an IPv6 address or IPv6 prefix of a Dynamic Host Configuration Protocol (DHCP) for IPv6 relay binding, use the **clear ipv6 dhcp relay binding** command in privileged EXEC mode.

clear ipv6 dhcp relay binding {**vrf** *vrf-name*} {**ipv6-addressipv6-prefix*}

Cisco uBR10012 and Cisco uBR7200 Series Universal Broadband Devices

clear ipv6 dhcp relay binding {**vrf** *vrf-name*} {** ipv6-prefix*}

Syntax Description

vrf *vrf-name*	Specifies a virtual routing and forwarding (VRF) configuration.
*	Clears all DHCPv6 relay bindings.
ipv6-address	DHCPv6 address.
ipv6-prefix	IPv6 prefix.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.
15.1(2)S	This command was modified. The **vrf** *vrf-name* keyword-argument pair was added.
Cisco IOS XE Release 3.3S	This command was modified. The **vrf** *vrf-name* keyword-argument pair was added.
15.2(1)S	The command was modified to delete the binding or route for IPv6 addresses.
Cisco IOS XE Release 3.5S	The command was modified to delete the binding or route for IPv6 addresses.
12.2(33)SCF4	This command was implemented on Cisco uBR10012 and Cisco uBR7200 series universal broadband devices.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Usage Guidelines

The **clear ipv6 dhcp relay binding** command deletes a specific IPv6 address or IPv6 prefix of a DHCP for IPv6 relay binding. If no relay client is specified, no binding is deleted.

Examples

The following example shows how to clear the binding for a client with a specified IPv6 address:

```
Device# clear ipv6 dhcp relay binding 2001:0DB8:3333:4::5
```

The following example shows how to clear the binding for a client with the VRF name vrf1 and a specified prefix on a Cisco uBR10012 universal broadband device:

```
Device# clear ipv6 dhcp relay binding vrf vrf1 2001:DB8:0:1::/64
```

Related Commands

Command	Description
show ipv6 dhcp relay binding	Displays DHCPv6 IANA and DHCPv6 IAPD bindings on a relay agent.

clear ipv6 dhcp route

To clear routes added by Dynamic Host Configuration Protocol for IPv6 (DHCPv6) on a DHCPv6 server for Internet Assigned Numbers Authority (IANA) and Identity Association for Prefix Delegation (IAPD), use the **clear ipv6 dhcp route** command in privileged EXEC mode.

clear ipv6 dhcp route {**vrf** *vrf-name*} {**ipv6-addressipv6-prefix*}

Syntax Description

vrf *vrf-name*	Specifies a virtual routing and forwarding (VRF) configuration.
*	Clears all DHCPv6 added routes.
ipv6-address	DHCPv6 address.
ipv6-prefix	IPv6 prefix.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(1)S	This command was introduced.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.

Examples

The following example shows how to clear routes added by DHCPv6 on a DHCPv6 server for IANA and IAPD:

```
Router# clear ipv6 dhcp route vrf vrfname 2001:0DB8:3333:4::5/126
```

Related Commands

Command	Description
show ipv6 dhcp route	Displays the routed added by DHCPv6 on the DHCPv6 server for IANA and IAPD.

clear ipv6 nat translation

To clear dynamic Network Address Translation--Protocol Translation (NAT-PT) translations from the dynamic state table, use the **clear ipv6 nat translation**command in privileged EXEC mode.

clear ipv6 nat translation *

Syntax Description

*	Clears all dynamic NAT-PT translations.

Command Default

Entries are deleted from the dynamic translation state table when they time out.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Use this command to clear entries from the dynamic translation state table before they time out. Static translation configuration is not affected by this command.

Examples

The following example shows the NAT-PT entries before and after the dynamic translation state table is cleared. Note that all the dynamic NAT-PT mappings are cleared, but the static NAT-PT configurations remain.

```
Router# show ipv6 nat translations
Prot  IPv4 source              IPv6 source
      IPv4 destination         IPv6 destination
---   ---                      ---
      192.168.123.2            2001::2
---   ---                      ---
      192.168.122.10           2001::10
tcp   192.168.124.8,11047      3002::8,11047
      192.168.123.2,23         2001::2,23
udp   192.168.124.8,52922      3002::8,52922
      192.168.123.2,69         2001::2,69
Router# clear ipv6 nat translation *
Router# show ipv6 nat translations
Prot  IPv4 source              IPv6 source
      IPv4 destination         IPv6 destination
---   ---                      ---
      192.168.123.2            2001::2
---   ---                      ---
      192.168.122.10           2001::10
```

Related Commands

Command	Description
ipv6 nat	Designates that traffic originating from or destined for the interface is subject to NAT-PT.
show ipv6 nat translations	Displays active NAT-PT translations.

clear logging ip access-list cache

To clear all the entries from the Optimized ACL Logging (OAL) cache and send them to the syslog, use the **clear logging ip access-list cache** command in privileged EXEC mode.

clear logging ip access-list cache

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720 only.

Examples

This example shows how to clear all the entries from the OAL cache and send them to the syslog:

```
Router#
clear logging ip access-list cache
```

Related Commands

Command	Description
logging ip access-list cache (global configuration)	Configures the OAL parameters globally.
logging ip access-list cache (interface configuration)	Enables an OAL-logging cache on an interface that is based on direction.
show logging ip access-list	Displays information about the logging IP access list.

clear mdns cache

To clear multicast Domain Name System (mDNS) cache information, use the **clear mdns cache** command in user EXEC or privileged EXEC mode.

clear mdns cache [**interface** *type number* | **mac** *mac-address*]

Syntax Description

interface *type number*	(Optional) Clears mDNS cache information for the specified interface.
mac *mac-address*	(Optional) Clears mDNS cache information for the device associated with the specified MAC address.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.2(1)E	This command was introduced.
15.2(2)E	This command was modified. The keyword-argument pairs **interface** *type number* and **mac** *mac-address* were added.
Cisco IOS XE 3.6E	This command was integrated into the Cisco IOS XE 3.6E release.
15.2(1)SY	This command was integrated into Cisco IOS Release 15.2(1)SY.
15.5(2)S	This command was integrated into Cisco IOS Release 15.5(2)S.
Cisco IOS XE Release 3.15S	This command was integrated into the Cisco IOS XE Release 3.15S

Usage Guidelines

To clear mDNS cache information for all the interfaces on the device, including all mDNS records in cache, use the command form **clear mdns cache**. To clear mDNS cache information for a specific interface, use the command form **clear mdns cache interface** *type number*.

Examples

The following example shows how to clear mDNS cache information for the interface ethernet 0/1:

```
Device> enable
Device# clear mdns cache interface ethernet 0/1
Device# exit
```

Related Commands

Command	Description
show mdns cache	Displays mDNS cache information.

clear mdns service-types

To clear multicast Domain Name System (mDNS) service-type information, use the **clear mdns service-types** command in user EXEC or privileged EXEC mode.

clear mdns service-types [**interface** *type number*]

Syntax Description

interface *type number*	(Optional) Clears mDNS service-type information for the specified interface.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.2(2)E	This command was introduced.
Cisco IOS XE 3.6E	This command was integrated into the Cisco IOS XE 3.6E release.
15.2(1)SY	This command was integrated into Cisco IOS Release 15.2(1)SY.
15.5(2)S	This command was integrated into Cisco IOS Release 15.5(2)S.
Cisco IOS XE Release 3.15S	This command was integrated into the Cisco IOS XE Release 3.15S

Usage Guidelines

To clear mDNS service-type information for all the interfaces on the device, use the command form **clear mdns service-types**. To clear mDNS service-type information for a specific interface, use the command form **clear mdns service-types interface** *type number*.

Examples

The following example shows how to clear mDNS service-type information for the interface ethernet 0/1:

```
Device> enable
Device# clear mdns service-types interface ethernet 0/1
Device# exit
```

Related Commands

Command	Description
show mdns service-types	Displays mDNS service-type information.

clear mdns statistics

To clear multicast Domain Name System (mDNS) statistics, use the **clear mdns statistics** command in user EXEC or privileged EXEC mode.

clear mdns statistics {**all** | **interface** *type number* | **service-list** *name* | **service-policy** {**all** | **interface** *type number*}}

Syntax Description

all	Clears mDNS statistics for the device or service-policy.
interface *type number*	Clears mDNS statistics or service-policy statistics for the specified interface.
service-list *name*	Clears mDNS statistics for the specified service-list.
service-policy	Clears mDNS service-policy statistics.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.2(1)E	This command was introduced.
15.2(2)E	This command was modified. The keyword-argument pair **service-list** *name* was added.
Cisco IOS XE 3.6E	This command was integrated into the Cisco IOS XE 3.6E release.
15.2(1)SY	This command was integrated into Cisco IOS Release 15.2(1)SY.
15.5(2)S	This command was integrated into Cisco IOS Release 15.5(2)S.
Cisco IOS XE Release 3.15S	This command was integrated into the Cisco IOS XE Release 3.15S

Usage Guidelines

The **all** keyword can be used in two forms of the **clear mdns statistics** command. You can clear mDNS statistics for the device using the **clear mdns statistics all** command form. To clear service-policy statistics for all interfaces, use the **clear mdns statistics service-policy all** command form.

The keyword-argument pair **interface** *type number* can be used in two forms of the **clear mdns statistics** command. To clear mDNS statistics for a specific interface, use the **clear mdns statistics interface** *type number* command form. To clear service-policy statistics for a specific interface, use the **clear mdns statistics service-policy interface** *type number* command form.

Examples

The following example shows how to clear mDNS statistics information for a device:

```
Device> enable
Device# clear mdns statistics
Device# exit
```

Related Commands

Command	Description
show mdns statistics	Displays mDNS statistics.

clear nat64 ha statistics

To clear the Network Address Translation 64 (NAT64) high availability (HA) statistics, use the **clear nat64 ha statistics** command in privileged EXEC mode.

clear nat64 ha statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

The HA statistics include the number of HA messages that are transmitted and received by the Route Processor (RP).

Examples

The following example shows how to use the **clear nat64 ha statistics** command to clear the NAT64 HA statistics:

```
Router# clear nat64 ha statistics
```

Related Commands

Command	Description
show nat64 ha status	Displays information about the NAT64 HA state.

clear nat64 statistics

To clear the Network Address Translation 64 (NAT64) statistics, use the **clear nat64 statistics** command in privileged EXEC mode.

clear nat64 statistics [**failure** | **global** | **interface** *type number* | **limit global** | **pool** *pool-name* | **prefix** [**stateful** *ipv6-prefix*/*prefix-length* | **stateless** [**v4v6** | **v6v4**] *ipv6-prefix*/*prefix-length*]]

Syntax Description

failure	(Optional) Clears NAT64 failure count statistics.
global	(Optional) Clears global NAT64 statistics.
interface	(Optional) Clears interface statistics.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
limit	(Optional) Clears the statistics about the maximum number of stateful NAT64 translations allowed on a router.
pool *pool-name*	(Optional) Clears statistics for a specified pool.
prefix	(Optional) Clears statistics for a specified prefix.
stateful	(Optional) Clears stateful NAT64 statistics.
ipv6-prefix	(Optional) IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/*prefix-length*	(Optional) Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
stateless	(Optional) Clears stateless NAT64 statistics.
v4v6	(Optional) Clears statistics about the IPv4 address that is associated with an IPv6 host for NAT64.
v6v4	(Optional) Clears statistics about the IPv6 address that is associated with an IPv4 host for NAT64.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Release	Modification
Cisco IOS XE Release 3.4S	This command was modified. The **failure**, **pool**, **stateful**, **stateless**, **v4v6**, and **v6v4** keywords and the *pool-name* argument were added.
15.4(1)T	This command was integrated into Cisco IOS Release 15.4(1)T.

Usage Guidelines

You can use the **clear nat64 statistics** command to clear the statistics of a specified interface or all the interfaces for a given stateful or stateless prefix.

Examples

The following example shows how to clear NAT64 statistics:

```
Device# clear nat64 statistics
```

Related Commands

Command	Description
nat64 v4v6	Translates an IPv4 source address to an IPv6 source address and an IPv6 destination address to an IPv4 destination address for NAT64.
nat64 v6v4	Translates an IPv6 source address to an IPv4 source address and an IPv4 destination address to an IPv6 destination address for NAT64.
show nat64 statistics	Displays statistics about NAT64 interfaces and the translated and dropped packet count.

clear nat64 translations

To clear dynamic stateful Network Address Translation 64 (NAT64) translations, use the **clear nat64 translations** command in privileged EXEC mode.

clear nat64 translations {**all** | **redundancy** *group-id* | **protocol** {**icmp** | **tcp** | **udp**}}

Syntax Description

all	Clears all NAT64 translations.
redundancy *group-id*	Clears translations that are filtered on the basis of the specified redundancy group ID. Valid values are 1 and 2.
protocol	Clears translations that are filtered on the basis of the specified protocol.
icmp	Clears NAT64 Internet Control Message Protocol (ICMP) translations.
tcp	Clears NAT64 TCP translations.
udp	Clears NAT64 UDP translations.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was modified. The **redundancy** *group-id* keyword-argument pair and the **protocol** and **icmp** keywords were added.
15.4(1)T	This command was integrated into Cisco IOS Release 15.4(1)T.

Examples

The following example shows how to clear all NAT64 translations:

```
Device# clear nat64 translations all
```

The following example shows how to clear translations that are filtered for redundancy group ID 1:

```
Device# clear nat64 translations redundancy 1
```

Related Commands

Command	Description
nat64 translation	Enables NAT64 translation.

client-identifier

To specify the unique identifier (in dotted hexadecimal notation) for a Dynamic Host Configuration Protocol (DHCP) client, use the **client-identifier** command in DHCP pool configuration mode. To delete the client identifier, use the **no** form of this command.

client-identifier *unique-identifier*
no client-identifier

Syntax Description

unique-identifier	The distinct identification of the client in 7- or 27-byte dotted hexadecimal notation. See the "Usage Guidelines" section for more information.

Command Default

No client identifier is specified.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid for manual bindings only. DHCP clients require client identifiers instead of hardware addresses. The client identifier is formed by concatenating the media type and the MAC address. You can specify the unique identifier for the client in either of the following ways:

- A 7-byte dotted hexadecimal notation. For example, 01b7.0813.8811.66, where 01 represents the Ethernet media type and the remaining bytes represent the MAC address of the DHCP client.
- A 27-byte dotted hexadecimal notation. For example, 7665.6e64.6f72.2d30.3032.342e.3937.6230.2e33.3734.312d.4661.302f.31. The equivalent ASCII string for this hexadecimal value is vendor-0024.97b0.3741-fa0/1, where vendor represents the vendor, 0024.97b0.3741 represents the MAC address of the source interface, and fa0/1 represents the source interface of the DHCP client.

For a list of media type codes, refer to the "Address Resolution Protocol Parameters" section of RFC 1700, *Assigned Numbers*.

You can determine the client identifier by using the **debug ip dhcp server packet** command.

Examples

The following example specifies the client identifier for MAC address 01b7.0813.8811.66 in dotted hexadecimal notation:

```
Device(dhcp-config)# client-identifier 01b7.0813.8811.66
```

Related Commands

Command	Description
hardware-address	Specifies the hardware address of a BOOTP client.
host	Specifies the IP address and network mask for a manual binding to a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

client-name

To specify the name of a Dynamic Host Configuration Protocol (DHCP) client, use the **client-name** command in DHCP pool configuration mode. To remove the client name, use the **no** form of this command.

client-name *name*
no client-name

Syntax Description

name	Specifies the name of the client, using any standard ASCII character. The client name should not include the domain name. For example, the name abc should not be specified as abc.cisco.com.

Command Default

No default behavior or values

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The client name should not include the domain name.

Examples

The following example specifies a string client1 that will be the name of the client:

```
client-name client1
```

Related Commands

Command	Description
host	Specifies the IP address and network mask for a manual binding to a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP Server and enters DHCP pool configuration mode.

control

To configure the control interface type and number for a redundancy group, use the **control**command in redundancy application group configuration mode. To remove the control interface for the redundancy group, use the **no** form of this command.

control *interface-type interface-number* **protocol** *id*
no control

Syntax Description

interface-type	Interface type.
interface-number	Interface number.
protocol	Specifies redundancy group protocol media.
id	Redundancy group protocol instance. The range is from 1 to 8.

Command Default

The control interface is not configured.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Examples

The following example shows how to configure the redundancy group protocol media and instance for the control Gigabit Ethernet interface:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# control GigabitEthernet 0/0/0 protocol
 1
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
data	Configures the data interface type and number for a redundancy group.
group(firewall)	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.

Command	Description
protocol	Defines a protocol instance in a redundancy group.

data

To configure the data interface type and number for a redundancy group, use the **data**command in redundancy application group configuration mode. To remove the configuration, use the **no** form of this command.

data *interface-type interface-number*
no data *interface-type interface-number*

Syntax Description

interface-type	Interface type.
interface-number	Interface number.

Command Default

No data interface is configured.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

Use the **data** command to configure the data interface. The data interface can be the same physical interface as the control interface.

Examples

The following example shows how to configure the data Gigabit Ethernet interface for group1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# data GigabitEthernet 0/0/0
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
control	Configures the control interface type and number for a redundancy group.
group(firewall)	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.
protocol	Defines a protocol instance in a redundancy group.

ddns (DDNS-update-method)

To specify an update method for address (A) Resource Records (RRs) as IETF standardized Dynamic Domain Name System (DDNS), use the **ddns**command in DDNS-update-method configuration mode. To disable the DDNS method for updating, use the **no** form of this command.

ddns [**both**]
no ddns

Syntax Description

both	(Optional) Both A and PTR RRs are updated.

Command Default

No DDNS updating is configured.

Command Modes

DDNS-update-method configuration

Command History

Release	Modification
12.3(8)YA	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Usage Guidelines

If Dynamic Host Configuration Protocol (DHCP) is used to configure the IP address on the interface, a DHCP client may not perform both A and PTR RRs or any updates. Also, if the DHCP server notifies the client during the DHCP interaction that it will perform the updates, then the DHCP client will not perform the updates. The DHCP server can always override the client even if the client is configured to perform the updates.

If the interface is configured using DHCP and if the DDNS update method is configured on that interface, then the DHCP fully qualified domain name (FQDN) option is included in the DHCP packets between the client and the server. The FQDN option contains the hostname, which is used in the update as well as information about what types of updates the client has been configured to perform.

If the **ddns** keyword is specified, the A RRs only are updated, but if the **ddns both** keyword are specified, both the A and the PTR RRs are updated. Also, if the DHCP server returns the the FQDN option with an updated hostname, that hostname is used in the update instead.

Examples

The following example shows how to configure a DHCP server to perform both A and PTR RR updates:

```
ip ddns update method unit-test
 ddns both
```

Related Commands

Command	Description
ip ddns update method	Enables DDNS as the update method and assigns a method name.

default-mapping-rule

To configure Network Address Translation 64 (NAT64) mapping of addresses and ports translation (MAP-T) default domain mapping rule, use the **default-mapping-rule** command in NAT64 MAP-T configuration mode. To remove the NAT64 MAP-T default domain mapping rule, use the **no** form of this command.

default-mapping-rule*ipv6-prefix/prefix-length*
no default-mapping-rule

Syntax Description

ipv6-prefix/prefix-mask	The IPv6 address assigned to the interface and the length of the IPv6 prefix. The prefix-length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

Mapping rules are not enabled.

Command Modes

NAT64 MAP-T configuration (config-nat64-mapt)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.
Cisco IOS Release 15.5(2)T	This command was integrated into Cisco IOS Release 15.5(2)T.

Usage Guidelines

MAP-T or Mapping of address and port (MAP) double stateless translation-based solution (MAP-T) provides IPv4 hosts connectivity to and across an IPv6 domain. MAP-T builds on existing stateless IPv4/IPv6 address translation techniques that are specified in RFC 6052, RFC 6144, and RFC 6145.

Examples

The following example shows how to configure a default domain mapping rule:

```
Device(config)# nat64 map-t domain 89
Device(config-nat64-mapt)# default-mapping-rule 2001:0DB8:0:1::/64
```

Related Commands

Command	Description
nat64 map-t	Configures NAT64 MAP-T settings.

default-router

To specify the default router list for a Dynamic Host Configuration Protocol (DHCP) client, use the **default-router** command in DHCP pool configuration mode. To remove the default router list, use the **no** form of this command.

default-router *address* [*address2 ... address8*]
no default-router

Syntax Description

address	Specifies the IP address of a router. One IP address is required, although you can specify up to eight addresses in one command line.
address2...address8	(Optional) Specifies up to eight addresses in the command line.

Command Default

No default behavior or values.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The IP address of the router should be on the same subnet as the client subnet. You can specify up to eight routers in the list. Routers are listed in order of preference (address1 is the most preferred router, address2 is the next most preferred router, and so on).

Examples

The following example specifies 10.12.1.99 as the IP address of the default router:

```
default-router 10.12.1.99
```

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

designated-gateway

To designate a specific device or interface in a domain for routing multicast Domain Name System (mDNS) announcement and query information, use the **designated-gateway** command in mDNS or interface mDNS configuration mode. To disable designated gateway status on a device or interface, use the **no** form of this command.

designated-gateway enable [**ttl** *ttl-duration*]
no designated-gateway enable [**ttl** *ttl-duration*]

Syntax Description

enable	Assigns the device or interface as the designated gateway for the domain.
ttl *duration*	(Optional) Specifies the Time to Live (TTL) duration. The TTL value is specified in minutes. The range is from 1 to 60 minutes.

Command Default

No device or interface is assigned as the designated gateway in a domain.

Command Modes

Multicast DNS configuration (config-mdns)

Interface mDNS configuration (config-if-mdns-sd)

Command History

Release	Modification
Cisco IOS 15.2(2)E	This command was introduced.
Cisco IOS XE 3.6E	This command was integrated into the Cisco IOS XE 3.6E release.
15.2(1)SY	This command was integrated into Cisco IOS Release 15.2(1)SY.
15.5(2)S	This command was integrated into Cisco IOS Release 15.5(2)S.
Cisco IOS XE Release 3.15S	This command was integrated into the Cisco IOS XE Release 3.15S.

Usage Guidelines

When multiple mDNS gateways are configured in a domain without a designated gateway, then queries and announcements are received by all the mDNS gateways in the link local domain. When you specify an mDNS gateway as the designated gateway, the designated gateway will give responses to queries for that domain; the other mDNS gateways do not respond since the other gateways know that the designated gateway will answer the query. In this way, duplicate responses are avoided.

Examples

The following example shows you how to specify an interface as the designated gateway with a TTL duration of 20 minutes:

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 0/1
Device(config-if)# service-routing mdns-sd
Device(config-if-mdns-sd)# designated-gateway enable ttl 20
Device(config-if-mdns-sd)# exit
```

Related Commands

Command	Description
service-routing mdns-sd	Enables mDNS gateway functionality for a device.
show mdns statistics	Displays mDNS statistics for the specified service-list.
show running-config mdns-sd policy	Displays current running mDNS service-policy configuration details for the device or interface.

device-role (DHCPv6 Guard)

To specify the role of the device attached to the target (which can be an interface or VLAN), use the **device-role** command in Dynamic Host Configuration Protocol version 6 (DHCPv6) guard configuration mode. To remove the specification, use the **no** form of this command.

device-role {**client** | **server**}
no device-role

Syntax Description

client	Sets the role of the device to client.
server	Sets the role of the device to server.

Command Default

The device role is client.

Command Modes

DHCPv6 guard configuration (config-dhcp-guard)

Command History

Release	Modification
15.2(4)S	This command was introduced.

Usage Guidelines

The **device-role** command specifies the role of the device attached to the target (which can be an interface or VLAN) . The device role is primarily used to allow and disallow DHCP replies and DHCP advertisements when they are received on an interface with a device role other than server or relay.

Examples

The following example defines a DHCPv6 guard policy name as policy1, places the router in DHCPv6 guard configuration mode, and configures the device as the server:

```
Router(config)# ipv6 dhcp guard policy policy1
Router(config-dhcp-guard)# device-role server
```

Related Commands

Command	Description
ipv6 dhcp guard policy	Defines the DHCPv6 guard policy name.

dns forwarder

To add an address to the end of the ordered list of IP addresses for a Domain Name System (DNS) view to use when forwarding incoming DNS queries, use the **dns forwarder** command in DNS view configuration mode. To remove an IP address from the list, use the **no** form of this command.

dns forwarder [**vrf** *vrf-name*] *forwarder-ip-address*
no dns forwarder [**vrf** *vrf-name*] *forwarder-ip-address*

Syntax Description

vrf *vrf-name*	(Optional) The *vrf-name* argument specifies the name of the Virtual Private Network (VPN) routing and forwarding (VRF) instance of the *forwarder-ip-address*. **Note** If no VRF is specified, the default is the global VRF.
forwarder-ip-address	IP address to use when forwarding DNS queries handled using the DNS view. **Note** You can specify an IPv4 or IPv6 address for the forwarder IP address.

Command Default

Provided that DNS forwarding (configured by using the **dns forwarding** command) is enabled and the interface to use when forwarding incoming DNS queries is configured (if using the **dns forwarding source-interface** command) and not shut down, incoming DNS queries handled using the DNS view are forwarded to one of the DNS forwarding name servers.

If no forwarding name servers are configured for the DNS view, the device uses any configured domain name server addresses.

If there are no domain name server addresses configured either, the device forwards incoming DNS queries to the limited broadcast address (255.255.255.255) so that the queries are received by all hosts on the local network segment but not forwarded by devices.

Command Modes

DNS view configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.
15.4(1)T	This command was modified. An IPv6 address can be specified for the *forwarder-ip-address* argument.

Usage Guidelines

This command can be entered multiple times to specify a maximum of six forwarding name servers. After six forwarding name servers have been specified, additional forwarding name servers cannot be specified unless an existing entry is removed.

To display the list of DNS forwarding name server addresses configured for the DNS view, use the **show ip dns view** command.

Note DNS resolving name servers and DNS forwarding name servers are configured separately. The **domain name-server** and **domain name-server interface** commands are used to specify the DNS resolving name servers (the ordered list of IP addresses to use when resolving internally generated DNS queries handled using the DNS view). The **dns forwarder** command specifies the forwarder addresses (the ordered list of IP addresses to use when forwarding incoming DNS queries handled using the DNS view). Earlier to this command being introduced, the resolving name server list was used for resolving internal DNS queries and forwarding DNS queries received by the DNS server. For backward compatibility, if there are no forwarding name servers configured, the resolving name server list will be used instead.

Examples

The following example shows how to add three IP addresses to the list of forwarder addresses for the DNS view named user3 that is associated with the VRF vpn32:

```
Device(config)# ip dns view vrf vpn32 user3

Device(cfg-dns-view)# dns forwarder 192.168.2.0

Device(cfg-dns-view)# dns forwarder 192.168.2.1

Device(cfg-dns-view)# dns forwarder 192.168.2.2
```

The following example shows how to add the IP address 192.0.2.3 to the list of forwarder addresses for the DNS view named user1 that is associated with the VRF vpn32, with the restriction that incoming DNS queries will be forwarded to 192.0.2.3 only if the queries are from the VRF named vpn1:

```
Device(config)# ip dns view vrf vpn32 user1

Device(cfg-dns-view)# dns forwarder vrf vpn1 192.168.2.3
```

Related Commands

Command	Description
dns forwarding	Enables forwarding of incoming DNS queries by the DNS view.
dns forwarding source-interface	Specifies the interface to use when forwarding incoming DNS queries handled using the DNS view.
domain name-server	Specifies the ordered list of IP addresses to use when resolving internally generated DNS queries handled using the DNS view.
domain name-server interface	Specifies the interface from which the device can learn (through either DHCP or PPP interaction on the interface) a DNS resolving name server address for the DNS view.
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

dns forwarding

To enable forwarding of incoming Domain Name System (DNS) queries handled using the DNS view, use the **dns forwarding** command in DNS view configuration mode. To disable forwarding and revert to the default configuration, use the **no** form of this command.

dns forwarding [**retry** *number* | **timeout** *seconds*]
no dns forwarding [**retry** | **timeout**]

Syntax Description

retry	(Optional) Specifies the time to retry forwarding a DNS query.
number	(Optional) Number of retries. The range is from 0 to 100.
timeout	(Optional) Specifies the timeout waiting for response to a forwarded DNS.
seconds	(Optional) Timeout in seconds. The range is from 1 to 3600.

Command Default

The default value is inherited from the global setting configured using the **ip domain lookup** global configuration command. However, the **dns forwarding** command for the DNS view does not have a reciprocal side effect on the setting configured by the **ip domain lookup** command.

Command Modes

DNS view configuration (cfg-dns-view)

Command History

Release	Modification
12.4(9)T	This command was introduced.
15.0(1)M	This command was modified. The **retry** *number* and **timeout** *seconds* keywords and arguments were added.

Usage Guidelines

This command enables forwarding of incoming DNS queries handled using the DNS view.

To display the DNS forwarding setting for a DNS view, use the **show ip dns view** command.

If you configure the **no domain lookup** command for a DNS view while the **dns forwarding** command has not been disabled for that view, then the **dns forwarding** command setting will appear in the **show ip dns view** command output in order to make it clear that DNS forwarding is still enabled.

If you configure the **no ip domain lookup** global configuration command, however, the **no dns forwarding** setting is automatically configured also, in order to be backward compatible with the global command form.



Note DNS lookup and DNS forwarding are configured separately. The **domain lookup** command enables the resolution of internally generated DNS queries handled using the DNS view. The **dns forwarding** command enables the forwarding of incoming DNS queries handled using the DNS view. By default, domain lookup and DNS forwarding are both enabled for a view. If you then configure the **no domain lookup**command, DNS forwarding is still enabled. However, if you instead use the older Cisco IOS command **no ip domain lookup** to disable domain lookup for the global default view, then DNS forwarding is disabled automatically. This is done for backward compatibility with the functionality of the **no ip domain lookup** global configuration command.

Examples

The following example shows how to enable forwarding of incoming DNS queries handled using the DNS view named user3 that is associated with the VRF vpn32:

```
Router(config)# ip dns view vrf vpn32 user3

Router(cfg-dns-view)# dns forwarding
```

Related Commands

Command	Description
dns forwarding source-interface	Specifies the interface to use when forwarding incoming DNS queries handled using the DNS view.
domain lookup	Enables the IP DNS-based hostname-to-address translation for internally generated DNS queries handled using the DNS view.
ip domain lookup	Enables the IP DNS-based hostname-to-address translation.
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

dns forwarding source-interface

To specify the interface to use when forwarding incoming Domain Name System (DNS) queries handled using the DNS view, use the **dns forwarding source-interface** command in DNS view configuration mode. To remove the specification of the source interface for a DNS view to use when forwarding DNS queries, use the **no** form of this command.

dns forwarding source-interface *interface*
no dns forwarding source-interface

Syntax Description

interface	Router interface to use when forwarding DNS queries.

Command Default

No interface is specified for forwarding incoming DNS queries handled using the DNS view, so the router selects the appropriate source IP address automatically, according to the interface used to send the packet, when the query is forwarded.

Command Modes

DNS view configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command specifies the interface to use when forwarding incoming DNS queries handled using the DNS view.

To display the interface configured by this command, use the **show ip dns view** command.

Tip To list all the interfaces configured on the router or access server, use the **show interfaces** command with the **summary** keyword. Use the appropriate interface specification, typed exactly as it is displayed under the Interface column of the **show interfaces** command output, to replace the *interface* argument in the **dns forwarding source-interface** command.

Examples

The following is sample output from the **show interfaces** command used with the **summary** keyword:

```
Router# show interfaces summary

 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count
  Interface              IHQ   IQD  OHQ   OQD  RXBS RXPS  TXBS TXPS TRTL
------------------------------------------------------------------------
* FastEthernet0/0          0     0    0     0     0    0     0    0    0
  FastEthernet0/1          0     0    0     0     0    0     0    0    0
  ATM2/0                   0     0    0     0     0    0     0    0    0
  Ethernet3/0              0     0    0     0     0    0     0    0    0
  Ethernet3/1              0     0    0     0     0    0     0    0    0
```

```
  Ethernet3/2              0     0    0     0     0    0     0    0    0
  Ethernet3/3              0     0    0     0     0    0     0    0    0
  ATM6/0                   0     0    0     0     0    0     0    0    0
NOTE:No separate counters are maintained for subinterfaces
     Hence Details of subinterface are not shown
```

The following example shows how to configure FastEthernet slot 0, port 1 as the interface to be used to forward DNS queries for the DNS view named user3 that is associated with the VRF vpn32:

```
Router(config)# ip dns view vrf vpn32 user3

Router(cfg-dns-view)# dns forwarder source-interface FastEthernet0/1
```

Related Commands

Command	Description
dns forwarding	Enables forwarding of incoming DNS queries by the DNS view.
show interfaces	Display statistics for all interfaces configured on the router or access server.
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

dns-server

To specify the Domain Name System (DNS) IP servers available to a Dynamic Host Configuration Protocol (DHCP) client, use the **dns-server** command in DHCP pool configuration mode. To remove the DNS server list, use the **no** form of this command.

dns-server *address* [*address2* **. . .** *address8*]
no dns-server

Syntax Description

address	The IP address of a DNS server. One IP address is required, although you can specify up to eight addresses in one command line.
address2...address8	(Optional) Specifies up to eight addresses in the command line.

Command Default

If DNS IP servers are not configured for a DHCP client, the client cannot correlate host names to IP addresses.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Servers are listed in order of preference (address1 is the most preferred server, address2 is the next most preferred server, and so on).

Examples

The following example specifies 10.12.1.99 as the IP address of the domain name server of the client:

```
dns-server 10.12.1.99
```

Related Commands

Command	Description
domain-name (DHCP)	Specifies the domain name for a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

dns-server (config-dhcp-global-options)

To configure the Domain Name System (DNS) servers that are available to DHCP clients on request, use the **dns-server** command in DHCP global options configuration mode. To remove the DNS server list, use the **no** form of this command.

dns-server *ip-address* [*ip-address2...ip-address8*]
no dns-server

Syntax Description

ip-address	IP address of a DNS server.
ip-address2...ip-address8	(Optional) IP address of DNS servers. You can specify up to eight IP addresses.

Command Default

If DNS servers are not configured for a DHCP client, the client cannot correlate hostnames to IP addresses.

Command Modes

DHCP global options configuration (config-dhcp-global-options)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.

Usage Guidelines

Before you configure the **dns-server** command, you must enter DHCP global options configuration mode by using the **ip dhcp global-options** command.

Examples

The following example shows how to configure two DNS servers:

```
Router(config)# ip dhcp global-options
Router(config-dhcp-global-options)# dns-server 192.0.2.1 192.168.2.1
```

Related Commands

Command	Description
ip dhcp global-options	Enters DHCP global options configuration mode, which is used to configure DHCP-related global configurations.

dns-server (IPv6)

To specify the Domain Name System (DNS) IPv6 servers available to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **dns-server** command in DHCP for IPv6 pool configuration mode. To remove the DNS server list, use the **no** form of this command.

dns-server *ipv6-address*
no dns-server *ipv6-address*

Syntax Description

ipv6-address	The IPv6 address of a DNS server. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

When a DHCP for IPv6 pool is first created, no DNS IPv6 servers are configured.

Command Modes

DHCP for IPv6 pool configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Multiple Domain Name System (DNS) server addresses can be configured by issuing this command multiple times. New addresses will not overwrite old addresses.

Examples

The following example specifies the DNS IPv6 servers available:

```
dns-server 2001:0DB8:3000:3000::42
```

Related Commands

Command	Description
domain-name	Configures a domain name for a DHCP for IPv6 client.
ipv6 dhcp pool	Configures a DHCP for IPv6 configuration information pool and enters DHCP for IPv6 pool configuration mode.

domain list

To add a domain name to the end of the ordered list of domain names used to complete unqualified hostnames (names without a dotted-decimal domain name) in Domain Name System (DNS) queries handled using the DNS view, use the **domain list** command in DNS view configuration mode. To remove a name from the domain search list, use the **no** form of this command.

domain list *domain-name*
no domain list *domain-name*

Syntax Description

domain-name	Domain name to add or delete from the domain search list. **Note** Do not include the initial period that separates an unqualified name from the domain name.

Command Default

No domain list is defined for the DNS view.

Command Modes

DNS view configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command adds a domain name to the end of the domain search list for the DNS view.

Note The **domain list** and **domain name** commands are similar, except that the **domain list** command can be used to define a list of domain names for the view, each to be tried in turn. If DNS lookup is enabled for the DNS view but the domain search list (specified using the **domain list** command) is empty, the default domain name (specified by using the **domain name** command) is used instead. If the domain search list is not empty, the default domain name is not used.

To display the list of domain names used to complete unqualified hostnames in DNS queries received by a DNS view, use the **show hosts** command or the **show ip dns view** command.

Examples

The following example shows how to add two domain names to the list for the DNS view named user3 that is associated with the VRF vpn32:

```
Router(config)# ip dns view vrf vpn32 user3

Router(cfg-dns-view)# domain list example1.com

Router(cfg-dns-view)# domain list example1.org
```

The following example shows how to add two domain names to the list for the DNS view and then delete one of the domain names from the list:

```
Router(cfg-dns-view)# domain list example2.com
```

```
Router(cfg-dns-view)# domain list example2.org

Router(cfg-dns-view)# no domain list example2.net
```

Related Commands

Command	Description
domain name	Specifies a single default domain name to use to complete unqualified hostnames in internally generated DNS queries handled using the DNS view.
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views.
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

domain lookup

To enable the IP Domain Name System (DNS)-based hostname-to-address translation for internally generated DNS queries handled using the DNS view, use the **domain lookup** command in DNS view configuration mode. To disable domain lookup for hostname resolution, use the **no** form of this command.

domain lookup
no domain lookup

Syntax Description

This command has no arguments or keywords.

Command Default

The default value is inherited from the global setting configured using the **ip domain lookup** global command. However, the **domain lookup** DNS view command does not have a reciprocal side effect on the setting configured by the **ip domain lookup** global command.

Command Modes

DNS view configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command enables DNS-based hostname-to-address translation for internally generated DNS queries handled using the DNS view.

To display the DNS lookup setting for a DNS view, use the show ip dns view command.

If you configure **no dns forwarding** for a DNS view while **domain lookup** has not been disabled for that view, then the **domain lookup** setting will appear in the **show ip dns view** command output in order to make it clear that domain lookup is still enabled.

If you configure the **no ip domain lookup** global command, however, the **no domain lookup** setting is automatically configured also, in order to be backward compatible with the global command form.



Note DNS lookup and DNS forwarding are configured separately. The **domain lookup** command enables the resolution of internally generated DNS queries handled using the DNS view. The **dns forwarding** command enables the forwarding of incoming DNS queries handled using the DNS view. By default, both domain lookup and DNS forwarding are both enabled for a view. If you then configure **no domain lookup**, DNS forwarding is still enabled. However, if you instead uses the older Cisco IOS command **no ip domain lookup** to disable domain lookup for the global default view, then DNS forwarding is disabled automatically. This is done for backward compatibility with the functionality of the **no ip domain lookup** global command.

Examples

The following example shows how to enable IP DNS-based hostname-to-address translation in the DNS view named user3 that is associated with the VRF vpn32:

```
Router(config)# ip dns view vrf vpn32 user3

Router(cfg-dns-view)# domain lookup
```

Related Commands

Command	Description
dns forwarding	Enables forwarding of incoming DNS queries by the DNS view.
domain name-server	Specifies the ordered list of IP addresses to use when resolving internally generated DNS queries handled using the DNS view.
domain name-server interface	Specifies the interface from which the router can learn (through either DHCP or PPP interaction on the interface) a DNS resolving name server address for the DNS view.
ip domain lookup	Enables the IP DNS-based hostname-to-address translation.
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

domain multicast

To configure the domain name to be used when performing multicast address lookups for internally generated Domain Name System (DNS) queries handled using the DNS view, use the **domain multicast** command in DNS view configuration mode. To remove the specification of the domain name for multicast address lookups, use the **no** form of this command.

domain multicast *domain-name*
no domain multicast

Syntax Description

domain-name	Domain name to be used when performing multicast address lookups.

Command Default

No IP address is specified for performing multicast address lookups for the DNS view.

Command Modes

DNS view configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command configures the domain name to be used when performing multicast address lookups for internally generated DNS queries handled using the DNS view.

To display the domain name for multicast address lookups, use the **show ip dns view** command.

Examples

The following example shows how to configure the domain name www.example.com as the domain name to be used when performing multicast lookups for internally generated DNS queries handled using the DNS view named user3 that is associated with the VRF vpn32:

```
Router(config)# ip dns view vrf vpn32 user3

Router(cfg-dns-view)# domain multicast www.example.com
```

Related Commands

Command	Description
ip domain multicast	Changes the domain prefix used by Cisco IOS software for DNS-based SSM mapping.
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

domain name

To specify the default domain for a Domain Name System (DNS) view to use to complete unqualified hostnames (names without a dotted-decimal domain name), use the **domain name** command in DNS view configuration mode. To remove the specification of the default domain name for a DNS view, use the **no** form of this command.

domain name *domain-name*
no domain name

Syntax Description

domain-name	Default domain name used to complete unqualified hostnames. **Note** Do not include the initial period that separates an unqualified name from the domain name.

Command Default

No default domain name is defined for the DNS view.

Command Modes

DNS view configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command configures the default domain name used to complete unqualified hostnames in DNS queries handled using the DNS view.

Note The **domain list** and **domain name** commands are similar, except that the **domain list** command can be used to define a list of domain names for the view, each to be tried in turn. If DNS lookup is enabled for the DNS view but the domain search list (specified using the **domain list** command) is empty, the default domain name (specified by using the **domain name** command) is used instead. If the domain search list is not empty, the default domain name is not used.

To display the default domain name configured for a DNS view, use the **show hosts** command or the **show ip dns view** command.

Examples

The following example shows how to define example.com as the default domain name for the DNS view named user3 that is associated with the VRF vpn32:

```
Router(config)# ip dns view vrf vpn32 user3

Router(cfg-dns-view)# domain name example.com
```

Related Commands

Command	Description
domain list	Defines the ordered list of default domain names to use to complete unqualified hostnames in internally generated DNS queries handled using the DNS view.
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views.
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

domain-name (IPv6)

To configure a domain name for a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) client, use the **domain-name**command in DHCPv6 pool configuration mode. To return to the default for this command, use the **no** form of this command.

domain-name *domain-name*
no domain-name

Syntax Description

domain-name	Default domain name used to complete unqualified hostnames. **Note** Do not include the initial period that separates an unqualified name from the domain name.

Command Default

No default domain name is defined for the DNS view.

Command Modes

DHCPv6 pool configuration mode (config-dhcp)

Command History

Release	Modification
12.4(9)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Use the domain-name command in IPv6 configure a domain name for a DHCPv6 client.

Examples

The following example configures a domain name for a DHCPv6 client:

```
Router(config)# ipv6 dhcp pool pool1
Router(cfg-dns-view)# domain-name domainv6
```

domain name-server

To add a name server to the list of Domain Name System (DNS) name servers to be used for a DNS view to resolve internally generated DNS queries, use the **domain name-server** command in DNS view configuration mode. To remove a DNS name server from the list, use the **no** form of this command.

domain name-server [**vrf** *vrf-name*] *name-server-ip-address*
no domain name-server [**vrf** *vrf-name*] [*name-server-ip-address*]

Syntax Description

vrf *vrf-name*	(Optional) The *vrf-name* argument specifies the name of the Virtual Private Network (VPN) routing and forwarding (VRF) instance of the *forwarder-ip-address*. **Note** If no VRF is specified, the default is the global VRF.
name-server-ip-address	IP address of a DNS name server. **Note** You can specify an IPv4 or IPv6 address for the DNS name server.

Command Default

No IP address is explicitly added to the list of resolving name servers for this view, although an IP address can be added to the list if dynamic name server acquisition is enabled. If the list of resolving name servers is empty, the device will send the query to the limited broadcast address 255.255.255.255 when this view is used.

Command Modes

DNS view configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.
15.4(1)T	This command was modified. An IPv6 address can be specified for the *name-server-ip-address* argument.

Usage Guidelines

This command can be entered multiple times to specify a maximum of six resolving name servers. After six resolving name servers have been specified, additional resolving name servers cannot be specified unless an existing entry is removed.

This method of explicitly populating the list of resolving name servers is useful in an enterprise network where the population of available DNS servers is relatively static. In an Internet service provider (ISP) environment, where primary and secondary DNS server addresses can change frequently, the device can learn a DNS server address through either DHCP or PPP on the interface. To configure the dynamic acquisition of DNS resolving name server addresses, use the **domain name-server interface** command. Regardless of the method or methods used to populate the list of DNS resolving name servers for the view, no more than six resolving name servers are maintained for the view.

To display the list of DNS resolving name server IP addresses configured for a DNS view, use the **show hosts** command or the **show ip dns view** command.



Note The DNS resolving name servers and DNS forwarding name servers are configured separately. The **domain name-server** and **domain name-server interface** commands are used to specify the DNS resolving name servers (the ordered list of IP addresses to use when resolving internally generated DNS queries for the DNS view). The **dns forwarder** command specifies the forwarder addresses (the ordered list of IP addresses to use when forwarding incoming DNS queries for the DNS view). If there is no DNS forwarder configuration in a view, then the domain name server list will be used when forwarding DNS queries. This is done for backward compatibility with the **ip name-server** global command.

Examples

The following example shows how to specify the hosts at 192.168.2.111 and 192.168.2.112 as the name servers for the DNS view named user3 that is associated with the VRF vpn32:

```
Device(config)# ip dns view vrf vpn32 user3

Device(cfg-dns-view)# domain name-server 192.168.2.111

Device(cfg-dns-view)# domain name-server 192.168.2.112
```

Related Commands

Command	Description
dns forwarder	Specifies the ordered list of IP addresses to use when forwarding incoming DNS queries handled using the DNS view.
domain name-server interface	Specifies the interface from which the device can learn (through either DHCP or PPP interaction on the interface) a DNS resolving name server address for the DNS view.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views.
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

domain name-server interface

To specify the interface on which the router can learn (through either DHCP or PPP) Domain Name System (DNS) a resolving name server address for the DNS view, use the **domain name-server interface** command in DNS view configuration mode. To remove the definition of the interface, use the **no** form of this command.

domain name-server interface *interface*
no domain name-server interface *interface*

Syntax Description

interface	Interface on which to acquire the IP address of a DNS name server that the DNS view can use to resolve internally generated DNS queries. The interface must connect to another router on which the DHCP agent or the PPP agent has been configured to allocate the IP address of the DNS server.

Command Default

No interface is used to acquire the DHCP or PPP address to be used for a DNS view to resolve internally generated DNS queries.

Command Modes

DNS view configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command specifies the interface from which to acquire (through DHCP or PPP interaction on the interface) the IP address of a DNS server to add to the list of DNS name servers used to resolve internally generated DNS queries for the DNS view.

The dynamic acquisition of DNS resolving name server addresses is useful in an Internet service provider (ISP) environment, where primary and secondary DNS server addresses can change frequently. To explicitly populate the list of resolving name servers in an enterprise network where the population of available DNS servers is relatively static, use the **domain name-server** command. Regardless of the method or methods used to populate the list of DNS resolving name servers for the view, no more than six resolving name servers are maintained for the view.

Note The DNS resolving name servers and DNS forwarding name servers are configured separately. The **domain name-server** and **domain name-server interface** commands are used to specify the DNS resolving name servers (the ordered list of IP addresses to use when resolving internally generated DNS queries for the DNS view). The **dns forwarder** command specifies the forwarder addresses (the ordered list of IP addresses to use when forwarding incoming DNS queries for the DNS view). If there is no DNS forwarder configuration in a view, then the domain name server list will be used when forwarding DNS queries. This is done for backward compatibility with the **ip name-server** global command.



Tip To list all the interfaces configured on the router or access server, use the **show interfaces** command with the **summary** keyword. Use the appropriate interface specification, typed exactly as it is displayed under the Interface column of the **show interfaces** command output, to replace the *interface* argument in the **domain name-server interface** command.

Examples

The following is sample output from the **show interfaces** command used with the **summary** keyword:

```
Router# show interfaces summary
 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count
  Interface              IHQ   IQD  OHQ   OQD  RXBS RXPS  TXBS TXPS TRTL
------------------------------------------------------------------------
* FastEthernet0/0          0     0    0     0     0    0     0    0    0
  FastEthernet0/1          0     0    0     0     0    0     0    0    0
  ATM2/0                   0     0    0     0     0    0     0    0    0
  Ethernet3/0              0     0    0     0     0    0     0    0    0
  Ethernet3/1              0     0    0     0     0    0     0    0    0
  Ethernet3/2              0     0    0     0     0    0     0    0    0
  Ethernet3/3              0     0    0     0     0    0     0    0    0
  ATM6/0                   0     0    0     0     0    0     0    0    0
NOTE:No separate counters are maintained for subinterfaces
     Hence Details of subinterface are not shown
```

The following example shows how to specify a list of name servers for the DNS view named user3 that is associated with the VRF vpn32. First, the list of name server addresses is cleared, then five DNS server IP addresses are added to the list. Finally, FastEthernet slot 0, port 0 is specified as the interface on which to acquire, by DHCP or PPP interaction, a sixth DNS server IP address.

```
Router(config)# ip dns view vrf vpn32 user3

Router(cfg-dns-view)# no domain name-server

Router(cfg-dns-view)# domain name-server 192.168.2.1

Router(cfg-dns-view)# domain name-server 192.168.2.2

Router(cfg-dns-view)# domain name-server 192.168.2.3

Router(cfg-dns-view)# domain name-server 192.168.2.4

Router(cfg-dns-view)# domain name-server 192.168.2.5

Router(cfg-dns-view)# domain name-server interface FastEthernet0/0
```

Related Commands

Command	Description
domain name-server	Specifies the ordered list of IP addresses to use when resolving internally generated DNS queries handled using the DNS view.

Command	Description
show interfaces	Display statistics for all interfaces configured on the router or access server.
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

domain resolver source-interface

To set the source IP address of the Domain Name Server (DNS) queries for the DNS resolver functionality, use the **domain resolver source-interface** command in DNS view configuration mode. To disable the configuration, use the **no** form of this command.

domain resolver source-interface *interface-type number*
no domain resolver source-interface

Syntax Description

interface-type	Interface type. For more information, use the question mark (?) online help function.
number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Default

Disabled. (DNS queries are not forwarded through the expected interface.)

Command Modes

DNS view configuration (cfg-dns-view)

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Sometimes, when a source interface is configured on a router with the split DNS feature to forward DNS queries, the router does not forward the DNS queries through the configured interface. If you want the router to forward the DNS queries through a particular source interface, configure the router using the **domain resolver source-interface** command.

Examples

The following example shows how to set the source IP address of the DNS queries for the DNS resolver functionality:

```
Router(config)# ip dns view vrf vpn32 user3
Router(cfg-dns-view)# domain resolver source-interface fastethernet 0/0
```

Related Commands

Command	Description
ip dns view	Creates the DNS view of the specified name associated with the specified VRF instance and then enters DNS view configuration mode.

domain retry

To configure the number of retries to perform when sending or forwarding Domain Name System (DNS) queries handled using the DNS view, use the **domain retry** command in DNS view configuration mode. To remove the specification of the number of retries for a DNS view, use the **no** form of this command.

domain retry *number*
no domain retry

Syntax Description

number	Number of times to retry sending or forwarding a DNS query. The range is from 0 to 100.

Command Default

number : 2 times

Command Modes

DNS view configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command configures the number of retries to perform when sending or forwarding DNS queries handled using the DNS view.

To display the number of retries configured for the DNS view, use the **show ip dns view** command.

Examples

The following example shows how to configure the router to send out or forward ten DNS queries from the DNS view named user3 that is associated with the VRF vpn32 before giving up:

```
Router(config)# ip dns view vrf vpn32 user3

Router(cfg-dns-view)# domain retry 10
```

Related Commands

Command	Description
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

domain round-robin

To enable round-robin rotation of multiple IP addresses associated with a name in the hostname cache used by the DNS view, use the **domain round-robin** command in DNS view configuration mode. To disable round-robin functionality for the DNS view, use the **no** form of this command.

domain round-robin
no domain round-robin

Syntax Description

This command has no arguments or keywords.

Command Default

Round-robin rotation of multiple IP addresses associated with a name in the hostname cache is disabled for the DNS view.

Command Modes

DNS view configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command enables round-robin rotation such that each time a hostname in the internal cache is accessed, the system returns the next IP address in the cache, rotated such that the second IP address in the list becomes the first one and the first one is moved to the end of the list. For a more detailed description of round-robin functionality, see the description of the **ip domain round-robin** global command in the *Cisco IOS IP Addressing Services Command Reference* .

To display the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views, use the **show hosts** command. To define static hostname-to-address mappings in the global hostname cache or VRF hostname cache for the specified DNS view, use the **ip host** command. To display the round-robin setting for the DNS view, use the **show ip dns view** command.

Examples

The following example shows how to define the hostname www.example.com with three IP addresses and then enable round-robin rotation for the default DNS view associated with the global VRF. Each time that hostname is referenced internally or queried by a DNS client sending a query to the Cisco IOS DNS server on this system, the order of the IP addresses associated with the host www.example.com will be changed. Because most client applications look only at the first IP address associated with a hostname, this results in different clients using each of the different addresses and thus distributing the load among the three different IP addresses.

```
Router(config)# ip host view www.example.com 192.168.2.100 192.168.2.200 192.168.2.250

Router(config)# ip dns view default

Router(cfg-dns-view)# domain lookup

Router(cfg-dns-view)# domain round-robin
```

Related Commands

Command	Description
ip host	Defines static hostname-to-address mappings in the DNS hostname cache for a DNS view.
ip domain round-robin	Enables round-robin functionality on DNS servers.
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views.
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

domain timeout

To configure the number of seconds to wait for a response to a Domain Name System (DNS) query sent or forwarded by the DNS view, use the **domain timeout** command in DNS view configuration mode. To remove the specification of the number of seconds for a DNS view to wait, use the **no** form of this command.

domain timeout *seconds*
no domain timeout

Syntax Description

seconds	Time, in seconds, to wait for a response to a DNS query. The range is from 0 to 3600.

Command Default

number : 3 seconds

Command Modes

DNS view configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command configures the number of seconds to wait for a response to a DNS query sent or forwarded by the DNS view.

To display the number of seconds configured for the DNS view, use the **show ip dns view** command.

Examples

The following example shows how to configure the router to wait 8 seconds for a response to a DNS query received in the DNS view named user3 that is associated with the VRF vpn32:

```
Router(config)# ip dns view vrf vpn32 user3

Router(cfg-dns-view)# domain timeout 8
```

Related Commands

Command	Description
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

domain-name (DHCP)

To specify the domain n ame for a Dynamic Host Configuration Protocol (DHCP) client, use the **domain-name** command in DHCP pool configuration mode. To remove the domain name, use the no form of this command.

domain-name *domain*
no domain-name

Syntax Description

domain	Specifies the domain name string of the client.

Command Default

No default behavior or values.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies cisco.com as the domain name of the client:

```
domain-name cisco.com
```

Related Commands

Command	Description
dns-server	Specifies the DNS IP servers available to a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

designated-gateway

To designate a specific device or interface in a domain for routing multicast Domain Name System (mDNS) announcement and query information, use the **designated-gateway** command in mDNS or interface mDNS configuration mode. To disable designated gateway status on a device or interface, use the **no** form of this command.

designated-gateway enable [**ttl** *ttl-duration*]
no designated-gateway enable [**ttl** *ttl-duration*]

Syntax Description

enable	Assigns the device or interface as the designated gateway for the domain.
ttl *duration*	(Optional) Specifies the Time to Live (TTL) duration. The TTL value is specified in minutes. The range is from 1 to 60 minutes.

Command Default

No device or interface is assigned as the designated gateway in a domain.

Command Modes

Multicast DNS configuration (config-mdns)

Interface mDNS configuration (config-if-mdns-sd)

Command History

Release	Modification
Cisco IOS 15.2(2)E	This command was introduced.
Cisco IOS XE 3.6E	This command was integrated into the Cisco IOS XE 3.6E release.
15.2(1)SY	This command was integrated into Cisco IOS Release 15.2(1)SY.
15.5(2)S	This command was integrated into Cisco IOS Release 15.5(2)S.
Cisco IOS XE Release 3.15S	This command was integrated into the Cisco IOS XE Release 3.15S.

Usage Guidelines

When multiple mDNS gateways are configured in a domain without a designated gateway, then queries and announcements are received by all the mDNS gateways in the link local domain. When you specify an mDNS gateway as the designated gateway, the designated gateway will give responses to queries for that domain; the other mDNS gateways do not respond since the other gateways know that the designated gateway will answer the query. In this way, duplicate responses are avoided.

Examples

The following example shows you how to specify an interface as the designated gateway with a TTL duration of 20 minutes:

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 0/1
Device(config-if)# service-routing mdns-sd
Device(config-if-mdns-sd)# designated-gateway enable ttl 20
Device(config-if-mdns-sd)# exit
```

Related Commands

Command	Description
service-routing mdns-sd	Enables mDNS gateway functionality for a device.
show mdns statistics	Displays mDNS statistics for the specified service-list.
show running-config mdns-sd policy	Displays current running mDNS service-policy configuration details for the device or interface.

group (firewall)

To enter redundancy application group configuration mode, use the **group** command in redundancy application configuration mode. To remove the group configuration, use the **no** form of this command.

group *id*
no group *id*

Syntax Description

id	Redundancy group ID. Valid values are 1 and 2.

Command Default

No group is configured.

Command Modes

Redundancy application configuration (config-red-app)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Examples

The following example shows how to configure a redundancy group with group ID 1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)#
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.

hardware-address

To specify the hardware address of a BOOTP client, use the **hardware-address** command in DHCP pool configuration mode. To remove the hardware address, use the no form of this command.

hardware-address *hardware-address* [*protocol-typehardware-number*]
no hardware-address

Syntax Description

hardware-address	MAC address of the client.
protocol-type	(Optional) Protocol type. The valid entries are: • **ethernet** • **ieee802** If no protocol type is specified, the default is Ethernet.
hardware-number	(Optional) ARP hardware specified in an online database at http://www.iana.org/assignments/arp-parameters. The valid range is from 0 to 255. See the table below for valid entries.

Command Default

Only the hardware address is enabled.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid for manual bindings only.

The table below lists the valid assigned hardware numbers found online at http://www.iana.org/assignments/arp-parameters.

Table 1: ARP Hardware Numbers and Types

Hardware Number	Hardware Type
1	Ethernet
2	Experimental Ethernet (3Mb)
3	Amateur Radio AX.25
4	ProNET Token Ring

Hardware Number	Hardware Type
5	Chaos
6	IEEE 802 Networks
7	ARCNET
8	Hyperchannel
9	Lanstar
10	Autonet Short Address
11	LocalTalk
12	LocalNet (IBM PCNet or SYTEK LocalNET)
13	Ultra link
14	SMDS
15	Frame Relay
16	Asynchronous Transmission Mode (ATM)
17	HDLC
18	Fibre Channel
19	Asynchronous Transmission Mode (ATM) (RFC2225)
20	Serial Line
21	Asynchronous Transmission Mode (ATM)
22	MIL-STD-188-220
23	Metricom
24	IEEE 1394.1995
25	MAPOS and Common Air Interface (CAI)
26	Twinaxial
27	EUI-64
28	HIPARP
29	IP and ARP over ISO 7816-3
30	ARPSec
31	IPsec tunnel (RFC3456)
32	InfiniBand (RFC-ietf-ipoib-ip-over-infiniband-09.txt)

Hardware Number	Hardware Type
33	TIA-102 Project

Examples

The following example specifies b708.1388.f166 as the MAC address of the client:

```
hardware-address b708.1388.f166 ieee802
```

Related Commands

Command	Description
client-identifier	Specifies the unique identifier of a DHCP client in dotted hexadecimal notation.
host	Specifies the IP address and network mask for a manual binding to a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

host

To specify the IP address and network mask for a manual binding to a Dynamic Host Configuration Protocol (DHCP) client, use the **host**command in DHCP pool configuration mode. To remove the IP address of the client, use the no form of this command.

host *address* [*mask* | */prefix-length*]
no host

Syntax Description

address	Specifies the IP address of the client.
mask	(Optional) Specifies the network mask of the client.
/ prefix-length	(Optional) Specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).

Command Default

The natural mask is used.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the mask and prefix length are unspecified, DHCP examines its address pools. If no mask is found in the pool database, the Class A, B, or C natural mask is used. This command is valid for manual bindings only.

There is no limit on the number of manual bindings but you can configure only one manual binding per host pool.

Examples

The following example specifies 10.12.1.99 as the IP address of the client and 255.255.248.0 as the subnet mask:

```
host 10.12.1.99 255.255.248.0
```

Related Commands

Command	Description
client-identifier	Specifies the unique identifier of a Microsoft DHCP client in dotted hexadecimal notation.
hardware-address	Specifies the hardware address of a DHCP client.

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.
network (DHCP)	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.

host (host-list)

To specify a list of hosts that will receive Dynamic Domain Name System (DDNS) updates of address (A) and pointer (PTR) Resource Records (RRs), use the **host**command in host-list configuration mode. To disable the host list, use the **no** form of this command.

host [**vrf** *vrf-name*] {*host-ip-addresshostname*}
no host [**vrf** *vrf-name*] {*host-ip-addresshostname*}

Syntax Description

vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) table. The *vrf-name* argument is a name with which the address pool is associated. **Note** All hostnames or IP addresses specified on the same line as the **vrf** keyword are associated with that VRF.
host-ip-address	List of server IP addresses that will receive DDNS updates.
hostname	Specifies a hostname.

Command Default

No list is configured for hosts.

Command Modes

Host-list configuration

Command History

Release	Modification
12.3(8)YA	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Examples

The following example shows how to configure a list of hosts:

```
ip host-list test
 host vrf abc 10.10.0.0
```

Related Commands

Command	Description
debug dhcp	Displays debugging information about the DHCP client and monitors the status of DHCP packets.
debug ip ddns update	Enables debugging for DDNS updates.
debug ip dhcp server	Enables DHCP server debugging.
ip ddns update hostname	Enables a host to be used for DDNS updates of A and PTR RRs.
ip ddns update method	Specifies a method of DDNS updates of A and PTR RRs and the maximum interval between the updates.

Command	Description
ip dhcp client update dns	Enables DDNS updates of A RRs using the same hostname passed in the hostname and FQDN options by a client.
ip dhcp-client update dns	Enables DDNS updates of A RRs using the same hostname passed in the hostname and FQDN options by a client.
ip dhcp update dns	Enables DDNS updates of A and PTR RRs for most address pools.
ip host-list	Specifies a list of hosts that will receive DDNS updates of A and PTR RRs.
show ip ddns update	Displays information about the DDNS updates.
show ip ddns update method	Displays information about the DDNS update method.
show ip host-list	Displays the assigned hosts in a list.
update dns	Dynamically updates a DNS with A and PTR RRs for some address pools.

http (DDNS-update-method)

To specify an update method for address (A) and pointer (PTR) Resource Records (RRs) as HTTP and enter DDNS-HTTP configuration mode, use the **http** command in DDNS-update-method configuration mode. To disable HTTP dynamic updates, use the **no** form of this command.

http
no http

Syntax Description

This command has no arguments or keywords.

Command Default

No HTTP update method is configured.

Command Modes

DDNS-update-method configuration (DDNS-update-method)

Command History

Release	Modification
12.3(8)YA	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Usage Guidelines

When you use the **http** command, you enter DDNS-HTTP configuration mode. In this mode, you can add or remove a mapping between a hostname and an IP address. Details are given below:

Use this command form..	To..

add *url-string*	Add or change a mapping between a hostname and an IP address. You must specify the URL to be used to add or change a mapping between a hostname and an IP address. The *url-string* argument takes the following form: http://*userid:password@domain-name/update-folder-name*/**update?system=** *system-name* **&hostname=** *hostname* **&myip=** *myipaddr* • *userid* and *password*—Strings for the organization website that you use for performing the A and PTR RRs updates. • *domain-name* —String for the organizational URL that you are using for the updates; for example www.Cisco.com. • *update-folder-name* —String of the folder name within the organizational website in which your updates are stored. • **update?system** =*system-name* --Update system (method) being used; for example, dydns is DDNS and dyn is EasyDNS. **Note** Before entering the question mark (?) character, press the control (Ctrl) key and the v key together on your keyboard. This will allow you to enter the ? without the software interpreting the ? as a help query. • **&hostname=** *hostname*-- Hostname to update. • **&myip** =*myipaddr*--IP address with which the specified hostname is associated, respectively. **Note** There are other special character strings that can be entered into the *url-string*. For example, if <s> is entered into the string, and when the update is processed, the IP address of the server to which the update is being sent is substituted at that location. The list of available special characters and their purpose are given below: • <a>—Substitutes the address being updated. • <h>—Substitutes the hostname being updated. • <s>—Substitutes the IP address of the server to which the update is being sent. • <q>—Substitutes a question mark character ("?"). • <o>—Substitutes an open angle bracket ("<"). • <c>—Substitutes a close angle bracket (">").
remove *url-string*	Remove a mapping between a hostname and an IP address. You must specify the URL to be used to remove a mapping between a hostname and an IP address. The *url-string* argument takes the same form as the one shown in the **add** keyword description.

Examples

The following example shows how to specify the DynDNS.org to process the updates:

```
ip ddns update method unit-test
 http
  add http://myuserid:secret@members.dyndns.org/nic/update?system=dyndns&hostname=
mywebsite&myip=10.10.10.10
```

The following are examples of URLs that can be used to update some HTTP DNS update services. These URLs are correct to the best of the knowledge of Cisco but have not been tested in all cases. Where the word "USERNAME:" appears in the URL, your account username at the HTTP site should be used. Where the word "PASSWORD" appears in the URL, your password for that account should be used:

DDNS

```
http://USERNAME:PASSWORD@members.dyndns.org/nic/update?system=dyndns&hostname=<h>&myip=<a>
!Requires "interval max 28 0 0 0" in the update method definition.
```

TZO

```
http://cgi.tzo.com/webclient/signedon.html?TZOName=<h>&Email=USERNAME&TZOKey=PASSWORD&IP
Address=<a>
```

EASYDNS

```
http://USERNAME:PASSWORD@members.easydns.com/dyn/ez-ipupdate.php?action=edit&myip=<a>&
host_id=<h>
```

JUSTLINUX

```
http://USERNAME:PASSWORD@www.justlinux.com/bin/controlpanel/dyndns/jlc.pl?direst=1&
username=USERNAME&password=PASSWORD&host=<h>&ip=<a>
```

DYNS

```
http://USERNAME:PASSWORD@www.dyns.cx/postscript.php?username=USERNAME&password=PASSWORD&
host=<h>&ip=<a>
```

HN

```
http://USERNAME:PASSWORD@dup.hn.org/vanity/update?ver=1&IP=<a>
```

ZONEEDIT

```
http://USERNAME:PASSWORD@www.zoneedit.com/auth/dynamic.html?host=<h>&dnsto=<a>
```



Note Since these services are provided by the respective companies, the URLs may be subject to change or the service could be discontinued at any time. Cisco takes no responsibility for the accuracy or use of any of this information. The URLs were obtained using an application called "ez-ipupdate," which is available for free on the internet.

Related Commands

Command	Description
ddns	Specifies DDNS as the update method for A and PTR RRs.
debug dhcp	Displays debugging information about the DHCP client and monitors the status of DHCP packets.
debug ip ddns update	Enables debugging for DDNS updates.
debug ip dhcp server	Enables DHCP server debugging.
default	Specifies the command default.
host (host-list)	Specifies a list of hosts that will receive DDNS updates of A and PTR RRs.
internal	Specifies the internal Cisco IOS cache is used for DDNS updates of A and PTR RRs.
interval maximum	Specifies a maximum interval for DDNS updates of A and PTR RRs.
ip ddns update hostname	Enables a host to be used for DDNS updates of A and PTR RRs.
ip ddns update method	Enables DDNS as the update method and assigns a method name.
ip dhcp client update dns	Enables DDNS updates of A RRs using the same hostname passed in the hostname and FQDN options by a client.
ip dhcp-client update dns	Enables DDNS updates of A RRs using the same hostname passed in the hostname and FQDN options by a client.
ip dhcp update dns	Enables DDNS updates of A and PTR RRs for most address pools.
ip host-list	Specifies a list of hosts that will receive DDNS updates of A and PTR RRs.
show ip ddns update	Displays information about the DDNS updates.
show ip ddns update method	Displays information about the DDNS update method.
show ip host-list	Displays the assigned hosts in a list.
update dns	Dynamically updates a DNS with A and PTR RRs for some address pools.

import all

To import Dynamic Host Configuration Protocol (DHCP) option parameters into the DHCP server database, use the **import all** command in DHCP pool configuration mode. To disable this feature, use the **no** form of this command.



Note When two servers provide DHCP addresses to a single device configured with **ip address dhcp** on two different interfaces, the imported information is merged and, for those options that take a single value, the last known option value will be used.

import all
no import all

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When the **no import all** command is used, the DHCP server deletes all "imported" option parameters that were added to the specified pool in the server database. Manually configured DHCP option parameters override imported DHCP option parameters.

Imported option parameters are not part of the router configuration and are not saved in NVRAM.

Examples

The following example allows the importing of all DHCP options for a pool named pool1:

```
ip dhcp pool pool1
 network 172.16.0.0 /16
 import all
```

Related Commands

Command	Description
ip dhcp database	Configures a DHCP server to save automatic bindings on a remote host called a database agent.
show ip dhcp import	Displays the option parameters that were imported into the DHCP server database.

import dns-server

To import the Domain Name System (DNS) recursive name server option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import dns-server**command in IPv6 DHCP pool configuration mode. To remove the available DNS recursive name server list, use the **no** form of this command.

import dns-server
no import dns-server

Syntax Description

This command has no arguments or keywords.

Command Default

The DNS recursive name server list is not imported to a client.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The DNS recursive name server option provides a list of one or more IPv6 addresses of DNS recursive name servers to which a client's DNS resolver may send DNS queries. The DNS servers are listed in the order of preference for use by the client resolver.

The DNS recursive name server list option code is 23. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to import a list of available DNS recursive name servers to a client:

```
Router(config-dhcp)# import dns-server
```

Related Commands

Command	Description
import domain-name	Imports the domain search list option to a DHCP for IPv6 client.

import domain-name

To import the domain name search list option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import domain-name**command in IPv6 DHCP pool configuration mode. To remove the domain name search list, use the **no** form of this command.

import domain-name
no import domain-name

Syntax Description

This command has no arguments or keywords.

Command Default

The domain search list is not imported to the client.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The domain name search list option specifies the domain search list the client is to use when resolving hostnames with DNS.

The domain name search list option code is 24. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to import a domain search list to the client:

```
Router(config-dhcp)# import domain-name
```

Related Commands

Command	Description
import dns-server	Imports the DNS recursive name server option to a DHCP for IPv6 client.

import information refresh

To import the information refresh time option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import information refresh**command in IPv6 DHCP pool configuration mode. To remove the specified refresh time, use the **no** form of this command.

import information refresh
no import information refresh

Syntax Description

This command has no arguments or keywords.

Command Default

The information refresh time option is not imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The information refresh time option specifies an upper bound for how long a client should wait before refreshing information retrieved from DHCP for IPv6. It is used only in Reply messages in response to Information Request messages. In other messages, there will usually be other options that indicate when the client should contact the server (for example, addresses with lifetimes).

The information refresh time option code is 32. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to import the information refresh time:

```
import information refresh
```

Related Commands

Command	Description
information refresh	Specifies the information refresh time to be sent to the client.

import nis address

To import the network information service (NIS) address option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import nis address** command in IPv6 DHCP pool configuration mode. To remove the NIS address, use the **no** form of this command.

import nis address
no import nis address

Syntax Description

This command has no arguments or keywords.

Command Default

No NIS address is imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS servers option provides a list of one or more IPv6 addresses of NIS servers available to send to the client. The client must view the list of NIS servers as an ordered list, and the server may list the NIS servers in the order of the server's preference.

The NIS servers option code is 27. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to import the NIS address of an IPv6 server:

```
import nis address
```

Related Commands

Command	Description
import nis domain	Imports the NIS domain name option to a DHCP for IPv6 client.
nis address	Specifies the NIS address of an IPv6 server to be sent to the client.
nis domain-name	Enables a server to convey a client's NIS domain name information to the client.

import nis domain-name

To import the network information service (NIS) domain name option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import nis domain-name** command in IPv6 DHCP pool configuration mode. To remove the domain name, use the **no** form of this command.

import nis domain-name

Syntax Description

This command has no arguments or keywords.

Command Default

No NIS domain name is imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS domain name option provides a NIS domain name for the client.

The NIS domain name option code is 29.

Examples

The following example shows how to import a client's NIS domain name:

```
import nis domain-name
```

Related Commands

Command	Description
import nis address	Imports the NIS server option to a DHCP for IPv6 client.
nis address	Specifies the NIS address of an IPv6 server to be sent to the client.
nis domain-name	Enables a server to convey a client's NIS domain name information to the client.

import nisp address

To import the network information service plus (NIS+) servers option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import nisp address** command in IPv6 DHCP pool configuration mode. To remove the NIS address, use the **no** form of this command.

import nisp address
no import nisp address

Syntax Description

This command has no arguments or keywords.

Command Default

No NIS+ address is imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS+ servers option provides a list of one or more IPv6 addresses of NIS+ servers available to send to the client. The client must view the list of NIS+ servers as an ordered list, and the server may list the NIS+ servers in the order of the server’s preference.

The NIS+ servers option code is 28. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to import the NIS+ address of an IPv6 server:

```
import nisp address
```

Related Commands

Command	Description
import nisp domain	Imports the NIS+ domain name option to a DHCP for IPv6 client.
nisp address	Specifies the NIS+ address of an IPv6 server to be sent to the client.
nisp domain-name	Enables a server to convey a client’s NIS+ domain name information to the client.

import nisp domain-name

To import the network information service plus (NIS+) domain name option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import nisp domain-name**command in IPv6 DHCP pool configuration mode. To remove the domain name, use the **no** form of this command.

import nisp domain-name
no import nisp domain-name

Syntax Description

This command has no arguments or keywords.

Command Default

No NIS+ domain name is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS+ domain name option provides an NIS+ domain name for the client.

The NIS+ domain name option code is 30. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to import the NIS+ domain name of a client:

```
import nisp domain-name
```

Related Commands

Command	Description
import nisp address	Imports the NIS+ server option to a DHCP for IPv6 client.
nisp address	Specifies the NIS+ address of an IPv6 server to be sent to the client.
nisp domain-name	Enables a server to convey a client’s NIS+ domain name information to the client.

import sip address

To import the Session Initiation Protocol (SIP) server IPv6 address list option to the outbound SIP proxy server, use the **import sip address**command in IPv6 DHCP pool configuration mode. To remove the SIP server IPv6 address list, use the **no** form of this command.

import sip address
no import sip address

Syntax Description

This command has no arguments or keywords.

Command Default

SIP IPv6 address list is not imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

A SIP server is the host on which the outbound SIP proxy server is running.

The SIP server IPv6 address list option specifies a list of IPv6 addresses that indicate SIP outbound proxy servers available to the client. Servers must be listed in order of preference.

The SIP server IPv6 address list option code is 22. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example enables the user to import a SIP server IPv6 address list to the client:

```
Router(config-dhcp)# import
 sip address
```

Related Commands

Command	Description
import sip domain-name	Imports a SIP server domain-name list option to the outbound SIP proxy server.

import sip domain-name

To import a Session Initiation Protocol (SIP) server domain-name list option to the outbound SIP proxy server, use the **import sip domain-name**command in IPv6 DHCP pool configuration mode. To remove the SIP server domain-name list, use the **no** form of this command.

import sip domain-name
no import sip domain-name

Syntax Description

This command has no arguments or keywords.

Command Default

SIP domain-name list is not imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

A SIP server is the host on which the outbound SIP proxy server is running.

The SIP server domain-name list option contains the domain names of the SIP outbound proxy servers. Domain names must be listed in order of preference. The option may contain multiple domain names, but the client must try the records in the order listed. The client resolves the subsequent domain names only if attempts to contact the first one failed or yielded no common transport protocols between client and server or denoted a domain administratively prohibited by client policy.

The SIP server domain-name list option code is 21. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example enables the user to import a SIP server domain-name list to the client:

```
Router(config-dhcp)# import sip domain-name
```

Related Commands

Command	Description
import sip address	Imports the SIP server IPv6 address list option to the outbound SIP proxy server.

import sntp address

To import the Simple Network Time Protocol (SNTP) address option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import sntp address** command in IPv6 DHCP pool configuration mode. To remove the SNTP server address, use the **no** form of the command.

import sntp address *ipv6-address*
no import sntp address *ipv6-address*

Syntax Description

ipv6-address	(Optional) The IPv6 address for SNTP. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

No SNTP server address is imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The SNTP server option provides a list of one or more IPv6 addresses of SNTP servers available to the client for synchronization. The clients use these SNTP servers to synchronize their system time to that of the standard time servers.

Clients must treat the list of SNTP servers as an ordered list, and the server may list the SNTP servers in decreasing order of preference. The SNTP address option can be used only to configure information about SNTP servers that can be reached using IPv6.

The SNTP server option code is 31. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to import the SNTP server address:

```
import sntp address
```

Related Commands

Command	Description
sntp address	Specifies the SNTP server to be sent to the client.

information refresh

To specify the information refresh time to be sent to the client, use the **information refresh**command in IPv6 DHCP pool configuration mode. To remove the specified refresh time, use the **no** form of this command.

information refresh {*days* [*hours minutes*] | **infinity**}
no information refresh {*days* [*hours minutes*] | **infinity**}

Syntax Description

days	Refresh time specified in number of days. The default is 0 0 86400, which equals 24 hours.
hours	(Optional) Refresh time specified in number of hours.
minutes	(Optional) Refresh time specified in number of minutes. The minimum refresh time that can be used is 0 0 600, which is 10 minutes.
infinity	Sets the IPv6 value of 0xffffffff used to configure the information refresh time to infinity.

Command Default

Information refresh information is not sent to the client. The client refreshes every 24 hours if no refresh information is sent.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The information refresh time option specifies the maximum time a client should wait before refreshing information retrieved from DHCP for IPv6. It is only used in Reply messages in response to Information Request messages. In other messages, there will usually be other options that indicate when the client should contact the server (for example, addresses with lifetimes).

The maximum value for the information refresh period on the DHCP for IPv6 client is 7 days. The maximum value is not configurable.

The information refresh time option code is 32. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to specify the information refresh time to be 1 day, 1 hour, and 1 second:

```
information refresh 1 1 1
```

Related Commands

Command	Description
import information refresh	Imports the information refresh time option to a DHCP for IPv6 client.

internal (DDNS-update-method)

To specify an update method for Dynamic Domain Name System (DDNS) address (A) and pointer (PTR) Resource Records (RRs) as a Cisco IOS internal cache, use the **internal**command in DDNS-update-method configuration mode. To disable the internal dynamic updates, use the **no** form of this command.

internal
no internal

Syntax Description

This command has no arguments or keywords.

Command Default

No internal cache update method is configured.

Command Modes

DDNS-update-method configuration

Command History

Release	Modification
12.3(8)YA	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

This command is useful in conjunction with turning on the internal Cisco IOS DNS name-server. The DNS name-server is enabled by using the **ip dns server** command. This command enables the name-server to reply to requests for an IP address associated with the hostname that was added to the internal name cache. Not all images have Cisco IOS DNS name-server functionality, so the internal command will not be available. Refer to Feature Navigator at http://www.cisco.com/go/fn to verify the name-server functionality in your image.

When the internal type of update is specified, an entry into the Cisco IOS name cache is added, which is basically the same as entering the **ip host abc.com 10.0.0.1** command. The hostname “abc” and the IP address “10.0.0.1” are associated with an interface.

Examples

The following example shows how to configure a server to send DDNS updates to the internal Cisco IOS cache:

```
ip ddns update method mytest
 internal
```

Related Commands

Command	Description
ip ddns update method	Enables DDNS as the update method and assigns a method name.

interval maximum

To specify a maximum interval at which Dynamic Domain Name System (DDNS) updates of address (A) and pointer (PTR) Resource Records (RRs) occur, use the **interval maximum**command in DDNS-update-method configuration mode. To disable the interval, use the **no** form of this command.

interval maximum *days hours minutes seconds*
no interval maximum

Syntax Description

days	Maximum interval, in days, at which updates occur. The range is from 0 to 365.
hours	Maximum interval, in hours, at which updates occur. The range is from 0 to 23.
minutes	Maximum interval, in minutes, at which updates occur. The range is from 0 to 59.
seconds	Maximum interval, in seconds, at which updates occur. The range is from 0 to 59.

Command Default

No maximum interval is configured.

Command Modes

DDNS-update-method configuration

Command History

Release	Modification
12.3(8)YA	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Examples

The following example shows how to configure the update method, the maximum interval of the updates (globally), and the hostname on the interface:

```
interface ethernet1
 ip ddns update hostname abc.dyndns.org
 ip ddns update mytest
ip ddns update method mytest
 http add http://test:test@members.dyndns.org/nic/update?system=dyndns&hostname=myhost&
 myip=10.10.10.10
 interval maximum 1 0 0 0
```

Related Commands

Command	Description
ip ddns update method	Enables DDNS as the update method and assigns a method name.

interval minimum

To specify a minimum interval at which Dynamic Domain Name System (DDNS) updates of address (A) and pointer (PTR) Resource Records (RRs) occur, use the **interval minimum**command in DDNS-update-method configuration mode. To disable the minimum interval, use the **no** form of this command.

interval minimum *days hours minutes seconds*
no interval minimum

Syntax Description

days	Minimum interval, in days, at which updates occur. The range is from 0 to 365.
hours	Minimum interval, in hours, at which updates occur. The range is from 0 to 23.
minutes	Minimum interval, in minutes, at which updates occur. The range is from 0 to 59.
seconds	Minimum interval, in seconds, at which updates occur. The range is from 0 to 59.

Command Default

No minimum interval is configured.

Command Modes

DDNS-update-method configuration

Usage Guidelines

DDNS updates for interfaces acquiring their address through DHCP occur every time the DHCP lease is renewed. If the lease is renewed more often than the minimum update interval needed, then a problem may occur with the updates. Sites accepting HTTP-style updates, such as DynDNS.org, may report an error if the updates occur too often. The **interval minimum** command forces the system to ignore updates that would occur too often.

Currently, the DynDNS.org policy is that updates can not be made more often than once every 10 minutes. This policy is subject to change in the future. The **interval minimum** command helps to guarantee that updates will not be sent too often.

Command History

Release	Modification
12.4	This command was introduced.

Examples

The following example shows how to configure the minimum interval so that updates would not be sent to DynDNS.org any more often than once every 15 minutes.

```
!
 ip ddns update method my test
 interval minimum 0 0 15 0
 http
 add  http://test:test@members.dyndns.org/nic/update?system=dyndns&hostname=myhostname&
 myip=10.10.10 .1
```

Related Commands

Command	Description
ddns	Specifies DDNS as the update method for A and PTR RRs.

Command	Description
host (host-list)	Specifies a list of hosts that will receive DDNS updates of A and PTR RRs.
http	Specifies HTTP as the update method for A and PTR RRs.
internal	Specifies the internal Cisco IOS cache is used for DDNS udpates of A and PTR RRs.
interval maximum	Specifies a maximum interval at which DDNS updates of A and pointer PTR Resource RRs occur.
ip ddns update hostname	Enables a host to be used for DDNS updates of A and PTR RRs.
ip ddns update method	Enables DDNS as the update method and assigns a method name.
ip dhcp client update dns	Enables DDNS updates of A RRs using the same hostname passed in the hostname and FQDN options by a client.
ip dhcp-client update dns	Enables DDNS updates of A RRs using the same hostname passed in the hostname and FQDN options by a client.
ip dhcp update dns	Enables DDNS updates of A and PTR RRs for most address pools.
ip host-list	Specifies a list of hosts that will receive DDNS updates of A and PTR RRs.
show ip ddns update	Displays information about the DDNS updates.
show ip ddns update method	Displays information about the DDNS update method.
show ip host-list	Displays the assigned hosts in a list.
update dns	Dynamically updates a DNS with A and PTR RRs for some address pools.

ip address

To set a primary or secondary IP address for an interface, use the **ip address** command in interface configuration mode. To remove an IP address or disable IP processing, use the noform of this command.

ip address *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
no ip address *ip-address mask* [**secondary** [**vrf** *vrf-name*]]

Syntax Description

ip-address	IP address.
mask	Mask for the associated IP subnet.
secondary	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address. **Note** If the secondary address is used for a VRF table configuration with the **vrf** keyword, the **vrf** keyword must be specified also.
vrf	(Optional) Name of the VRF table. The *vrf-name* argument specifies the VRF name of the ingress interface.

Command Default

No IP address is defined for the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.2(28)SB	The **vrf** keyword and *vrf-name* argument were introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	Support for IPv6 was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

An interface can have one primary IP address and multiple secondary IP addresses. Packets generated by the Cisco IOS software always use the primary IP address. Therefore, all routers and access servers on a segment should share the same primary network number.

Hosts can determine subnet masks using the Internet Control Message Protocol (ICMP) mask request message. Routers respond to this request with an ICMP mask reply message.

You can disable IP processing on a particular interface by removing its IP address with the **no ip address** command. If the software detects another host using one of its IP addresses, it will print an error message on the console.

The optional **secondary** keyword allows you to specify an unlimited number of secondary addresses. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and Address Resolution Protocol (ARP) requests are handled properly, as are interface routes in the IP routing table.

Secondary IP addresses can be used in a variety of situations. The following are the most common applications:

- There may not be enough host addresses for a particular network segment. For example, your subnetting allows up to 254 hosts per logical subnet, but on one physical subnet you need 300 host addresses. Using secondary IP addresses on the routers or access servers allows you to have two logical subnets using one physical subnet.
- Many older networks were built using Level 2 bridges. The judicious use of secondary addresses can aid in the transition to a subnetted, router-based network. Routers on an older, bridged segment can be easily made aware that many subnets are on that segment.
- Two subnets of a single network might otherwise be separated by another network. This situation is not permitted when subnets are in use. In these instances, the first network is *extended*, or layered on top of the second network using secondary addresses.



Note If any router on a network segment uses a secondary address, all other devices on that same segment must also use a secondary address from the same network or subnet. Inconsistent use of secondary addresses on a network segment can very quickly cause routing loops.



Note When you are routing using the Open Shortest Path First (OSPF) algorithm, ensure that all secondary addresses of an interface fall into the same OSPF area as the primary addresses.

To transparently bridge IP on an interface, you must perform the following two tasks:

- Disable IP routing (specify the **no ip routing** command).
- Add the interface to a bridge group, see the **bridge-group** command.

To concurrently route and transparently bridge IP on an interface, see the **bridge crb**command.

Examples

In the following example, 192.108.1.27 is the primary address and 192.31.7.17 and 192.31.8.17 are secondary addresses for Ethernet interface 0:

```
interface ethernet 0
 ip address 192.108.1.27 255.255.255.0
 ip address 192.31.7.17 255.255.255.0 secondary
 ip address 192.31.8.17 255.255.255.0 secondary
```

In the following example, Ethernet interface 0/1 is configured to automatically classify the source IP address in the VRF table vrf1:

```
interface ethernet 0/1
 ip address 10.108.1.27 255.255.255.0
 ip address 10.31.7.17 255.255.255.0 secondary vrf vrf1
 ip vrf autoclassify source
```

Related Commands

Command	Description
bridge crb	Enables the Cisco IOS software to both route and bridge a given protocol on separate interfaces within a single router.
bridge-group	Assigns each network interface to a bridge group.
ip vrf autoclassify	Enables VRF autoclassify on a source interface.
match ip source	Specifies a source IP address to match to required route maps that have been set up based on VRF connected routes.
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.
set vrf	Enables VPN VRF selection within a route map for policy-based routing VRF selection.
show ip arp	Displays the ARP cache, in which SLIP addresses appear as permanent ARP table entries.
show ip interface	Displays the usability status of interfaces configured for IP.
show route-map	Displays static and dynamic route maps.

ip address dhcp

To acquire an IP address on an interface from the DHCP, use the **ip address dhcp**command in interface configuration mode. To remove any address that was acquired, use the **no** form of this command.

ip address dhcp [**client-id** *interface-type number*] [**hostname** *hostname*]
no ip address dhcp [**client-id** *interface-type number*] [**hostname** *hostname*]

Syntax Description

client-id	(Optional) Specifies the client identifier. By default, the client identifier is an ASCII value. The **client-id** *interface-type number*option sets the client identifier to the hexadecimal MAC address of the named interface.
interface-type	(Optional) Interface type. For more information, use the question mark (?) online help function.
number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
hostname	(Optional) Specifies the hostname.
hostname	(Optional) Name of the host to be placed in the DHCP option 12 field. This name need not be the same as the hostname entered in global configuration mode.

Command Default

The hostname is the globally configured hostname of the router. The client identifier is an ASCII value.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.1(3)T	This command was modified. The **client-id**keyword and *interface-type number*argument were added.
12.2(3)	This command was modified. The **hostname**keyword and *hostname*argument were added. The behavior of the **client-id** *interface-type number*option changed. See the "Usage Guidelines" section for details.
12.2(8)T	This command was modified. The command was expanded for use on PPP over ATM (PPPoA) interfaces and certain ATM interfaces.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)T	This command was modified. Support was provided on the tunnel interface.

Usage Guidelines

Note Prior to Cisco IOS Release 12.2(8)T, the **ip address dhcp** command could be used only on Ethernet interfaces.

The **ip address dhcp** command allows any interface to dynamically learn its IP address by using the DHCP protocol. It is especially useful on Ethernet interfaces that dynamically connect to an Internet service provider (ISP). Once assigned a dynamic address, the interface can be used with the Port Address Translation (PAT) of Cisco IOS Network Address Translation (NAT) to provide Internet access to a privately addressed network attached to the router.

The **ip address dhcp** command also works with ATM point-to-point interfaces and will accept any encapsulation type. However, for ATM multipoint interfaces you must specify Inverse ARP via the **protocol ip inarp** interface configuration command and use only the aa15snap encapsulation type.

Some ISPs require that the DHCPDISCOVER message have a specific hostname and client identifier that is the MAC address of the interface. The most typical usage of the **ip address dhcp client-id** *interface-type number* **hostname** *hostname* command is when *interface-type*is the Ethernet interface where the command is configured and *interface-type number*is the hostname provided by the ISP.

A client identifier (DHCP option 61) can be a hexadecimal or an ASCII value. By default, the client identifier is an ASCII value. The **client-id** *interface-type number*option overrides the default and forces the use of the hexadecimal MAC address of the named interface.

Note Between Cisco IOS Releases 12.1(3)T and 12.2(3), the **client-id** optional keyword allows the change of the fixed ASCII value for the client identifier. After Release 12.2(3), the optional **client-id** keyword forces the use of the hexadecimal MAC address of the named interface as the client identifier.

If a Cisco router is configured to obtain its IP address from a DHCP server, it sends a DHCPDISCOVER message to provide information about itself to the DHCP server on the network.

If you use the **ip address dhcp** command with or without any of the optional keywords, the DHCP option 12 field (hostname option) is included in the DISCOVER message. By default, the hostname specified in option 12 will be the globally configured hostname of the router. However, you can use the **ip address dhcp hostname** *hostname* command to place a different name in the DHCP option 12 field than the globally configured hostname of the router.

The **no ip address dhcp** command removes any IP address that was acquired, thus sending a DHCPRELEASE message.

You might need to experiment with different configurations to determine the one required by your DHCP server. The table below shows the possible configuration methods and the information placed in the DISCOVER message for each method.

Table 2: Configuration Method and Resulting Contents of the DISCOVER Message

Configuration Method	Contents of DISCOVER Messages
ip address dhcp	The DISCOVER message contains “cisco- *mac-address* -Eth1” in the client ID field. The *mac-address* is the MAC address of the Ethernet 1 interface and contains the default hostname of the router in the option 12 field.

Configuration Method	Contents of DISCOVER Messages
ip address dhcp hostname *hostname*	The DISCOVER message contains “cisco- *mac-address* -Eth1” in the client ID field. The *mac-address* is the MAC address of the Ethernet 1 interface, and contains *hostname* in the option 12 field.
ip address dhcp client-id ethernet 1	The DISCOVER message contains the MAC address of the Ethernet 1 interface in the client ID field and contains the default hostname of the router in the option 12 field.
ip address dhcp client-id ethernet 1 hostname *hostname*	The DISCOVER message contains the MAC address of the Ethernet 1 interface in the client ID field and contains *hostname* in the option 12 field.

Examples

In the examples that follow, the command **ip address dhcp** is entered for Ethernet interface 1. The DISCOVER message sent by a router configured as shown in the following example would contain “cisco- *mac-address* -Eth1” in the client-ID field, and the value abc in the option 12 field.

```
hostname abc
!
interface Ethernet 1
 ip address dhcp
```

The DISCOVER message sent by a router configured as shown in the following example would contain “cisco- mac-address -Eth1” in the client-ID field, and the value def in the option 12 field.

```
hostname abc
!
interface Ethernet 1
 ip address dhcp hostname def
```

The DISCOVER message sent by a router configured as shown in the following example would contain the MAC address of Ethernet interface 1 in the client-id field, and the value abc in the option 12 field.

```
hostname abc
!
interface Ethernet 1
 ip address dhcp client-id Ethernet 1
```

The DISCOVER message sent by a router configured as shown in the following example would contain the MAC address of Ethernet interface 1 in the client-id field, and the value def in the option 12 field.

```
hostname abc
!
interface Ethernet 1
 ip address dhcp client-id Ethernet 1 hostname def
```

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

ip address pool (DHCP)

To enable the IP address of an interface to be automatically configured when a Dynamic Host Configuration Protocol (DHCP) pool is populated with a subnet from IP Control Protocol (IPCP) negotiation, use the **ip address pool** command in interface configuration mode. To disable autoconfiguring of the IP address of the interface, use the **no** form of this command.

ip address pool *name*
no ip address pool

Syntax Description

name	Name of the DHCP pool. The IP address of the interface will be automatically configured from the DHCP pool specified in *name*.

Command Default

IP address pooling is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Use this command to automatically configure the IP address of a LAN interface when there are DHCP clients on the attached LAN that should be serviced by the DHCP pool on the router. The DHCP pool obtains its subnet dynamically through IPCP subnet negotiation.

Examples

The following example specifies that the IP address of Ethernet interface 2 will be automatically configured from the address pool named abc:

```
ip dhcp pool abc
  import all
  origin ipcp
!
interface Ethernet 2
  ip address pool abc
```

Related Commands

Command	Description
show ip interface	Displays the usability status of interfaces configured for IP.

ip arp entry learn

To specify the maximum number of learned Address Resolution Protocol (ARP) entries, use the **ip arp entry learn** command in global configuration mode. To return to the default settings, use the **no** form of this command.

ip arp entry learn *max-limit*
no ip arp entry learn *max-limit*

Syntax Description

max-limit	The maximum number of learned ARP entries; valid values are from 1 to 512000.

Command Default

No maximum number of learned ARP entries is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRD3	This command was introduced to support the Cisco 7600 router.

Usage Guidelines

The **ip arp entry learn** command is available on the Cisco 7600 series routers, which can support a maximum limit of learned ARP entries of 256,000. If a memory card is installed on the router the maximum limit is extended to 512,000.

When the number of ARP entries that can be created by the system is not limited, memory exhaustion can cause system instability. The **ip arp entry learn** command overcomes this problem by defining a maximum number of learned ARP entries.

The limit is not enforced on nonlearned entries. Upon reaching the learn ARP entry threshold limit, or 80 percent of the configured maximum limit, the system will generate a syslog message with a priority set to Level 3 (LOG_NOTICE). Upon reaching the configured maximum limit, the system starts discarding newly learned ARP entries and generates a syslog message. The priority will be set to Level 3 (LOG_NOTICE). The system administrator will have to take appropriate action.

A syslog message is also generated when the number of learned ARP entries in the ARP table decreases from the maximum configured limit to the permit threshold limit, or 95 percent of the maximum configured limit to notify the system administrator that the ARP table is back to normal operation.

The default behavior of the system is not to enforce a maximum limit of learned ARP entries on the system.

When a user tries to configure a maximum limit value for the number of ARP entries that is lower than the current number of ARP entries in the system, the configuration will be rejected with an error message.

The following example configures a maximum limit of the number of learned ARP entries of 512,000:

```
Router# configure terminal
Router(config)# ip arp entry learn 512000
```

Related Commands

Command	Description
show arp summary	Displays the total number of ARP table entries, the number of ARP table entries for each ARP entry mode, and the number of ARP table entries for each interface on the router.



ip arp gratuitous through ip dhcp ping packets

- ip arp gratuitous, on page 189
- ip arp incomplete, on page 190
- ip arp inspection filter vlan, on page 191
- ip arp inspection limit (interface configuration), on page 193
- ip arp inspection log-buffer, on page 195
- ip arp inspection trust, on page 197
- ip arp inspection validate, on page 198
- ip arp inspection vlan, on page 200
- ip arp inspection vlan logging, on page 201
- ip arp nat-garp-retry, on page 203
- ip arp poll, on page 205
- ip arp proxy disable, on page 206
- ip arp queue, on page 207
- ip classless, on page 208
- ip ddns update hostname, on page 209
- ip ddns update method, on page 210
- ip default-gateway, on page 211
- ip dhcp aaa default username, on page 212
- ip dhcp auto-broadcast, on page 214
- ip dhcp bootp ignore, on page 215
- ip dhcp class, on page 216
- ip dhcp client, on page 218
- ip dhcp client authentication key-chain, on page 219
- ip dhcp client authentication mode, on page 220
- ip dhcp client broadcast-flag (interface), on page 222
- ip dhcp client class-id, on page 223
- ip dhcp client client-id, on page 224
- ip dhcp client default-router distance, on page 226
- ip dhcp client hostname, on page 227
- ip dhcp client lease, on page 228
- ip dhcp client mobile renew, on page 230
- ip dhcp client request, on page 231
- ip dhcp client route, on page 233

- ip dhcp client update dns, on page 234
- ip dhcp compatibility lease-query client, on page 236
- ip dhcp compatibility suboption link-selection, on page 238
- ip dhcp conflict logging, on page 239
- ip dhcp conflict resolution, on page 240
- ip dhcp database, on page 241
- ip dhcp debug ascii-client-id, on page 243
- ip dhcp excluded-address, on page 244
- ip dhcp global-options, on page 246
- ip dhcp limit lease log, on page 247
- ip dhcp limit lease per interface, on page 248
- ip dhcp limited-broadcast-address, on page 249
- ip dhcp ping packets, on page 250

ip arp gratuitous

To enable the gratuitous Address Resolution Protocol (ARP) control on the router, use the **ip arp gratuitous** command in global configuration mode. To disable the ARP control, use the **no** form of this command.

ip arp gratuitous { **local** | **none** | **ignore** }
no ip arp gratuitous

Syntax Description

local	Accepts only local (same subnet) gratuitous arps.
none	Rejects gratuitous arp control.
ignore	Stops processing all received gratuitous arps.

Command Default

Gratuitous ARP control is enabled.

Gratuitous ARP control is disabled by default on the Cisco NCS 4200 Series routers.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Dublin17.10.x	The **ignore** keyword is added.

Examples

The following example shows how to enable the gratuitous ARP control to accept only local (same subnet) gratuitous arp control:

```
Router> enable
Router# configure terminal
Router(config)# ip arp gratuitous local
```

Related Commands

Command	Description
show arp	Display the entries in the ARP table.

ip arp incomplete

To rectify the Address Resolution Protocol (ARP) retry parameters, use the **ip arp incomplete** command in global configuration mode. To disable the correction of the retry parameters, use the **no** form of this command.

ip arp incomplete {**entries** *number-of-IP-addresses* | **retry** *number-of-times*}
no ip arp incomplete {**entries** | **retry**}

Syntax Description

entries	Limits the number of unresolved addresses.
number-of-IP-addresses	Number of IP addresses to resolve. The range is from 1 to 2147483647.
retry	Limits the number of attempts to resolve an address.
number-of-times	Number of times an ARP Request is sent. The range is from 1 to 2147483647.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

An incomplete ARP entry is learned through an ARP request but has not yet been completed with the MAC address of the external host.

Examples

The following example shows how to limit the number of unresolved addresses:

```
Router> enable
Router# configure terminal
Router(config)# ip arp incomplete entries 100
```

Related Commands

Command	Description
show arp	Display the entries in the Address Resolution Protocol (ARP) table.

ip arp inspection filter vlan

To permit ARPs from hosts that are configured for static IP when DAI is enabled and to define an ARP access list and apply it to a VLAN, use the **ip arp inspection filter vlan** command in global configuration mode. To disable this application, use the **no** form of this command.

ip arp inspection filter *arp-acl-name* **vlan** *vlan-range* [**static**]
no ip arp inspection filter *arp-acl-name* **vlan** *vlan-range* [**static**]

Syntax Description

arp-acl-name	Access control list name.
vlan-range	VLAN number or range; valid values are from 1 to 4094.
static	(Optional) Treats implicit denies in the ARP ACL as explicit denies and drops packets that do not match any previous clauses in the ACL.

Command Default

No defined ARP ACLs are applied to any VLAN.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

For *vlan-range*, you can specify the VLAN to which the switches and hosts belong. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma.

When an ARP access control list is applied to a VLAN for dynamic ARP inspection, the ARP packets containing only the IP-to-Ethernet MAC bindings are compared against the ACLs. All other packet types are bridged in the incoming VLAN without validation.

This command specifies that the incoming ARP packets are compared against the ARP access control list, and the packets are permitted only if the access control list permits them.

If the access control lists deny the packets because of explicit denies, the packets are dropped. If the packets are denied because of an implicit deny, they are then matched against the list of DHCP bindings if the ACL is not applied statically.

If you do not specify the **static** keyword, it means that there is no explicit deny in the ACL that denies the packet, and DHCP bindings determine whether a packet is permitted or denied if the packet does not match any clauses in the ACL.

Examples

This example shows how to apply the ARP ACL static-hosts to VLAN 1 for DAI:

```
Router(config)# ip arp inspection filter static-hosts vlan 1
```

Related Commands

Command	Description
arp access-list	Configures an ARP ACL for ARP inspection and QoS filtering and enters the ARP ACL configuration submode.
show ip arp inspection	Displays the status of DAI for a specific range of VLANs.

ip arp inspection limit (interface configuration)

To limit the rate of incoming ARP requests and responses on an interface and prevent DAI from consuming all of the system's resources in the event of a DoS attack, use the **ip arp inspection limit** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

ip arp inspection limit rate *pps* [**burst interval** *seconds* | **none**]
no ip arp inspection limit

Syntax Description

rate *pps*	Specifies the upper limit on the number of incoming packets processed per second; valid values are from 1 to 2048 pps.
burst interval *seconds*	(Optional) Specifies the consecutive interval in seconds over which the interface is monitored for the high rate of the ARP packets; valid values are from 1 to 15 seconds.
none	(Optional) Specifies that there is no upper limit on the rate of the incoming ARP packets that can be processed.

Command Default

The default settings are as follows:

- The **rate** *pps* is set to 15 packets per second on the untrusted interfaces, assuming that the network is a switched network with a host connecting to as many as 15 new hosts per second.
- The rate is unlimited on all the trusted interfaces.
- The **burst interval** *seconds* is set to 1 second.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You should configure the trunk ports with higher rates to reflect their aggregation. When the rate of the incoming packets exceeds the user-configured rate, the interface is placed into an error-disabled state. You can use the error-disable timeout feature to remove the port from the error-disabled state. The rate applies to both the trusted and nontrusted interfaces. Configure appropriate rates on trunks to handle the packets across multiple DAI-enabled VLANs, or use the **none** keyword to make the rate unlimited.

The rate of the incoming ARP packets on the channel ports is equal to the sum of the incoming rate of packets from all the channel members. Configure the rate limit for the channel ports only after examining the rate of the incoming ARP packets on the channel members.

After a switch receives more than the configured rate of packets every second consecutively over a period of burst seconds, the interface is placed into an error-disabled state.

Examples

This example shows how to limit the rate of the incoming ARP requests to 25 packets per second:

```
Router# configur terminal
Router(config)# interface fa6/3
Router(config-if)# ip arp inspection limit rate 25
```

This example shows how to limit the rate of the incoming ARP requests to 20 packets per second and to set the interface monitoring interval to 5 consecutive seconds:

```
Router# configure terminal
Router(config)# interface fa6/1
Router(config-if)# ip arp inspection limit rate 20 burst interval 5
```

Related Commands

Command	Description
show ip arp inspection	Displays the status of DAI for a specific range of VLANs.

ip arp inspection log-buffer

To configure the parameters that are associated with the logging buffer, use the **ip arp inspection log-buffer** command in global configuration mode. To disable the parameters, use the **no** form of this command.

ip arp inspection log-buffer {**entries** *number* | **logs** *number* **interval** *seconds*}
no ip arp inspection log-buffer {**entries** | **logs**}

Syntax Description

entries *number*	Specifies the number of entries from the logging buffer; valid values are from 0 to 1024.
logs *number*	Specifies the number of entries to be logged in an interval; valid values are from 0 to 1024.
interval *seconds*	Specifies the logging rate; valid values are from 0 to 86400 (1 day).

Command Default

The default settings are as follows:

- When dynamic ARP inspection is enabled, denied, or dropped, the ARP packets are logged.
- The **entries** *number* is 32.
- The **logs** *number is*5 per second.
- The **interval** *seconds is*1 second.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

A 0 value for the **logs** *number* indicates that the entries should not be logged out of this buffer.

A 0 value for the **interval** *seconds* keyword and argument indicates an immediate log.

You cannot enter a 0 for both the **logs** *number* and the **interval** *seconds* keywords and arguments.

The first dropped packet of a given flow is logged immediately. The subsequent packets for the same flow are registered but are not logged immediately. Registration for these packets occurs in a log buffer that is shared by all the VLANs. Entries from this buffer are logged on a rate-controlled basis.

Examples

This example shows how to configure the logging buffer to hold up to 45 entries:

```
Router# configure terminal
Router(config)# ip arp inspection log-buffer entries 45
```

This example shows how to configure the logging rate for 10 logs per 3 seconds:

```
Router(config)# ip arp inspection log-buffer logs 10 interval 3
```

Related Commands

Command	Description
arp access-list	Configures an ARP ACL for ARP inspection and QoS filtering and enters the ARP ACL configuration submode.
clear ip arp inspection log	Clears the status of the log buffer.
show ip arp inspection log	Shows the status of the log buffer.

ip arp inspection trust

To set a per-port configurable trust state that determines the set of interfaces where incoming ARP packets are inspected, use the **ip arp inspection trust** command in interface configuration mode. To make the interfaces untrusted, use the **no** form of this command.

ip arp inspection trust
no ip arp inspection trust

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to configure an interface to be trusted:

```
Router# configure terminal
Router(config)# interface fastEthernet 6/3
Router(config-if)# ip arp inspection trust
```

Related Commands

Command	Description
show ip arp inspection	Displays the status of DAI for a specific range of VLANs.

ip arp inspection validate

To perform specific checks for ARP inspection, use the **ip arp inspection validate** command in global configuration mode. To disable ARP inspection checks, use the **no** form of this command.

ip arp inspection validate [**src-mac**] [**dst-mac**] [**ip**]
no ip arp inspection validate [**src-mac**] [**dst-mac**] [**ip**]

Syntax Description

src-mac	(Optional) Checks the source MAC address in the Ethernet header against the sender's MAC address in the ARP body.
dst-mac	(Optional) Checks the destination MAC address in the Ethernet header against the target MAC address in the ARP body.
ip	(Optional) Checks the ARP body for invalid and unexpected IP addresses.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The sender IP addresses are checked in all ARP requests and responses and target IP addresses are checked only in ARP responses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses.

The **src-mac**checks are issued against both ARP requests and responses. The **dst-mac**checks are issued for ARP responses.

Note When enabled, packets with different MAC addresses are classified as invalid and are dropped.

When enabling the checks, specify at least one of the keywords (**src-mac**, **dst-mac**, and **ip**) on the command line. Each command overrides the configuration of the previous command. If a command enables **src** and **dst mac** validations, and a second command enables IP validation only, the **src** and **dst mac** validations are disabled as a result of the second command.

The **no** form of this command disables only the specified checks. If no check options are enabled, all the checks are disabled.

Examples

This example shows how to enable the source MAC validation:

```
Router(config)# ip arp inspection validate src-mac
```

Related Commands

Command	Description
arp access-list	Configures an ARP ACL for ARP inspection and QoS filtering and enters the ARP ACL configuration submode.
show ip arp inspection	Displays the status of DAI for a specific range of VLANs.

ip arp inspection vlan

To enable DAI on a per-VLAN basis, use the **ip arp inspection vlan** command in global configuration mode. To disable DAI, use the **no** form of this command.

ip arp inspection vlan *vlan-range*
no ip arp inspection vlan *vlan-range*

Syntax Description

vlan-range	VLAN number or range; valid values are from 1 to 4094.

Command Default

ARP inspection is disabled on all VLANs.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

For *vlan-range*, you can specify a single VLAN identified by a VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma.

You must specify on which VLANs to enable DAI. DAI may not function on the configured VLANs if the VLAN has not been created or is a private VLAN.

Examples

This example shows how to enable DAI on VLAN 1:

```
Router(config)# ip arp inspection vlan 1
```

Related Commands

Command	Description
arp access-list	Configures an ARP ACL for ARP inspection and QoS filtering and enters the ARP ACL configuration submode.
show ip arp inspection	Displays the status of DAI for a specific range of VLANs.

ip arp inspection vlan logging

To control the type of packets that are logged, use the **ip arp inspection vlan logging**command in global configuration mode. To disable this logging control, use the **no** form of this command.

ip arp inspection vlan *vlan-range* **logging** {**acl-match** {**matchlog** | **none**} | **dhcp-bindings** {**permit** | **all** | **none**}}
no ip arp inspection vlan *vlan-range* **logging** {**acl-match** | **dhcp-bindings**}

Syntax Description

vlan-range	Number of the VLANs to be mapped to the specified instance. The number is entered as a single value or a range; valid values are from 1 to 4094.
acl-match	Specifies the logging criteria for packets that are dropped or permitted based on ACL matches.
matchlog	Specifies that logging of packets matched against ACLs is controlled by the **matchlog** keyword in the permit and deny access control entries of the ACL.
none	Specifies that ACL-matched packets are not logged.
dhcp-bindings	Specifies the logging criteria for packets dropped or permitted based on matches against the DHCP bindings.
permit	Specifies logging when permitted by DHCP bindings.
all	Specifies logging when permitted or denied by DHCP bindings.
none	Prevents all logging of packets permitted or denied by DHCP bindings.

Command Default

All denied or dropped packets are logged.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

By default, the **matchlog** keyword is not available on the ACEs. When you enter the **matchlog** keyword, denied packets are not logged. Packets are logged only when they match against an ACE that has the **matchlog** keyword.

The **acl-match** and **dhcp-bindings** keywords merge with each other. When you set an ACL match configuration, the DHCP bindings configuration is not disabled. You can use the **no** form of this command to reset some of the logging criteria to their defaults. If you do not specify either option, all the logging types are reset to log on when the ARP packets are denied. The two options that are available are as follows:

- **acl-match** --Logging on ACL matches is reset to log on deny.
- **dhcp-bindings** --Logging on DHCP bindings is reset to log on deny.

Examples

This example shows how to configure an ARP inspection on VLAN 1 to add packets to a log that matches the ACLs:

```
Router(config)# ip arp inspection vlan 1 logging acl-match matchlog
```

Related Commands

Command	Description
arp access-list	Configures an ARP ACL for ARP inspection and QoS filtering and enters the ARP ACL configuration submode.
show ip arp inspection	Displays the status of DAI for a specific range of VLANs.

ip arp nat-garp-retry

To enable the efficient mapping of MAC addresses to IP addresses within a local network using the Address Resolution Protocol (ARP) and Gratuitous ARP (GARP), first use the **ip arp nat-garp-retry feature enable** command.

Following this, to request GARP messages, use the 'garp-interface' option along with the 'ip nat inside source static' command on the BD-VIF interface during NAT mapping configuration. For more information, see the **ip nat inside source static** command reference.

ip arp nat-garp-retry feature enable
ip arp nat-garp-retry feature disable

Upon activation, the following parameters can be configured:

- The **'retries'** argument can be added to the **ip arp nat-garp-retry** command to specify the number of NAT GARP Retry messages. The default is 2 times, with a permissible range of 1 to 5 retries for each entry.

  The command for this option is: **ip arp nat-garp-retry entries**

- The **'interval'** argument can be added to the **ip arp nat-garp-retry** command to set the time gap between NAT GARP Retry messages. The default interval is 5 seconds, with an acceptable range of 1 to 30 seconds.

  The command for this option is: **ip arp nat-garp-retry interval**

- The **'entries'** argument can be added to the **ip arp nat-garp-retry** command to define the maximum number of GARP command executions. The maximum number of BD-VIF interfaces for GARP initiation is capped at 3000 to optimize control plane load.

  The command for this option is: **ip arp nat-garp-retry retries**

Syntax Description

nat-garp-retry	Activates the NAT Gratuitous ARP (GARP) retry feature.
entries	(Optional) Defines the limit for GARP command executions. The maximum number of BD-VIF interfaces for GARP initiation is capped at 3000 to optimize control plane load.
interval	(Optional) Sets the time gap between NAT GARP Retry messages. The default is 5 seconds, with a permissible range of 2 to 30 seconds.
retries	(Optional) Determines the number of NAT GARP Retry message attempts. The default is 2 times, with a permissible range of 1 to 5 retries for each entry.

Command Default

By default, the NAT Gratuitous ARP (GARP) retry feature is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 17.13.1a	This command was introduced.

Usage Guidelines

The **ip arp nat-garp retry** command is a fundamental command that controls the parameters of the number of Gratuitous Address Resolution Protocol (GARP) entries, the intervals between the GARP messages, and the number of retries available. This command is specifically designed for use with BD-VIF (Bridge Domain-Virtual Interface) interfaces.

Activation of the **ip arp nat-garp retry** command is initiated with the 'ip arp nat-garp-retry feature enable' argument, effectively enabling this feature. After enabling, the command includes three additional optional arguments that provide further control over its function.

The **ip arp nat-garp-retry entries** argument sets the number of GARP entries. The **ip arp nat-garp-retry interval** argument determines the interval between GARP messages. Finally, the **ip arp nat-garp-retry retries** argument sets the number of retries available.

These optional arguments enable the user to configure the GARP retry mechanism in detail within the BD-VIF interfaces, thereby enhancing the efficiency of MAC to IP address mapping within the network.

By default, this feature is disabled. However, the user can enable it prior to configuring, to activate the GARP retry for IP NAT static inside CLI. This would offer more control over the GARP messages and their retry mechanism.

Examples

Here is an example of how to use the 'ip arp nat-garp retry' command and its optional arguments:

```
Router(config)# ip arp nat-garp-retry feature enable
Router(config)# ip arp nat-garp-retry entries 10
Router(config)# ip arp nat-garp-retry interval 30
Router(config)# ip arp nat-garp-retry retries 5
```

Related Commands

Command	Description
ip nat inside source static	Triggers GARP requests for static NAT mapping configurations on the BD-VIF interface.

ip arp poll

To configure the IP Address Resolution Protocol (ARP) polling for unnumbered interfaces, use the **ip arp poll** command in global configuration mode. To remove the IP ARP polling for unnumbered interfaces, use the **no** form of this command.

ip arp poll {**queue** *queue-size* | **rate** *packet-rate*}
no ip arp poll {**queue** | **rate**}

Syntax Description

queue *queue-size*	Configures the IP ARP polling queue size, in packets. The range is from 0 to 10000. The default is 1000.
rate *packet-rate*	Configures the IP ARP polling packet rate, in packets per second. The range is from 0 to 10000. The default is 1000.

Command Default

IP ARP polling for unnumbered interfaces has a default queue size of 1000 and packet rate of 1000 packets per second.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)SY	This command was introduced.

Examples

The following example shows how to configure the queue size for IP ARP polling for unnumbered interfaces:

```
Device(config)# ip arp poll queue 5000
```

The following example shows how to configure the packet rate for IP ARP polling for unnumbered interfaces:

```
Device(config)# ip arp poll rate 5000
```

Related Commands

Command	Description
show ip arp poll	Displays the IP ARP host polling status.

ip arp proxy disable

To globally disable proxy Address Resolution Protocol (ARP), use the **ip arp proxy disable** command in global configuration mode. To reenable proxy ARP, use the **no** form of this command.

ip arp proxy disable
no ip arp proxy disable

Syntax Description

This command has no arguments or keywords.

Command Default

Proxy ARP is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2 S	This command was introduced.
12.3(11)T	This command was integrated into 12.3(11)T.
12.2 (18)SXE	This command was integrated into 12.2(18)SXE.

Usage Guidelines

The **ip arp proxy disable** command overrides any proxy ARP interface configuration. The **default ip arp proxy** command returns proxy ARP to the default behavior, which is enabled.

Examples

The following example disables proxy ARP:

```
ip arp proxy disable
```

The following example enables proxy ARP:

```
no ip arp proxy disable
```

Related Commands

Command	Description
ip proxy-arp	Enables proxy ARP on an interface.

ip arp queue

To configure the Address Resolution Protocol (ARP) input packet queue size, use the **ip arp queue** command in global configuration mode. To restore the default, use the **no** form of this command.

ip arp queue *queue-size*
no ip arp queue

Syntax Description

queue-size	Size of the ARP input packet queue. Valid values are from 512 to 2147483647.

Command Default

By default, the queue size is configured as 512.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M5	This command was introduced.

Usage Guidelines

You can configure the ARP input packet queue size based on the volume of the incoming traffic. The ARP input queue size can be set by the platform during initialization. The ARP input packet size is configurable at the system level but not at the interface level.

Examples

The following example shows how to configure the ARP input packet queue size as 650:

```
Router(config)# ip arp queue 650
```

ip classless

To enable a router to forward packets, which are destined for a subnet of a network that has no network default route, to the best supernet route possible, use the **ip classless** command in global configuration mode. To disable the functionality, use the **no**form of this command.

ip classless
no ip classless

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
11.3	The default behavior changed from disabled to enabled.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command allows the software to forward packets that are destined for unrecognized subnets of directly connected networks. The packets are forwarded to the best supernet route.

When this feature is disabled, the Cisco IOS software discards the packets when a router receives packets for a subnet that numerically falls within its subnetwork addressing scheme, no such subnet number is in the routing table, and there is no network default route.



Note If the supernet or default route is learned by using Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF), the **no ip classless** configuration command is ignored.

Examples

The following example prevents the software from forwarding packets destined for an unrecognized subnet to the best supernet possible:

```
no ip classless
```

ip ddns update hostname

To enable a host to be used for Dynamic Domain Name System (DDNS) updates of address (A) and pointer (PTR) Resource Records (RRs), use the **ip ddns update hostname**command in interface configuration mode. To disable the dynamic updates, use the **no** form of this command.

ip ddns update hostname *hostname*
no ip ddns update hostname *hostname*

Syntax Description

hostname	Specifies a hostname of the server that will receive updates. **Note** It is expected that the hostname will be an fully qualified domain name (FQDN). Using an FQDN hostname enables the specification of a hostname in a different domain that the default domain of the device.

Command Default

No host is configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(8)YA	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Usage Guidelines

The interface configuration overrides the global configuration.

Examples

The following example shows how to configure the testhost host to update A and PTR RRs:

```
interface ethernet1/0
 ip ddns update hostname testhost
```

Related Commands

Command	Description
ip ddns update method	Specifies a method of DDNS updates of A and PTR RRs and the maximum interval between the updates.

ip ddns update method

To specify a method and method name for updating Dynamic Domain Name System (DDNS) address (A) and pointer (PTR) Resource Records (RRs) and enter DDNS-update-method configuration mode, use the **ip ddns update method**command in global configuration mode. To disable the dynamic updating, use the **no** form of this command.

ip ddns update method *method-name*
no ip ddns update method

Syntax Description

method-name	IETF standardized DDNS update method name.

Command Default

No DDNS update method is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)YA	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Usage Guidelines

The interface configuration overrides the global configuration.

Examples

The following example shows how to assign a DDNS update method name:

```
ip ddns update method unit-test
```

Once you have assigned the method name, you can specify the type of update (DDNS or HTTP) and set a maximum interval. Refer to the **ddns** and **http** commands for more information.

Related Commands

Command	Description
ddns	Specifies DDNS as the update method for A and PTR RRs.
http	Specifies HTTP as the update method for A and PTR RRs.

ip default-gateway

To define a default gateway (router) when IP routing is disabled, use the **ip default-gateway** command in global configuration mode. To disable this function, use the **no** form of this command.

ip default-gateway *ip-address*
no ip default-gateway *ip-address*

Syntax Description

ip-address	IP address of the router.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The Cisco IOS software sends any packets that need the assistance of a gateway to the address you specify. If another gateway has a better route to the requested host, the default gateway sends an Internet Control Message Protocol (ICMP) redirect message back. The ICMP redirectmessage indicates which local router the Cisco IOS software should use.

Examples

The following example defines the router on IP address 192.31.7.18 as the default router:

```
ip default-gateway 192.31.7.18
```

Related Commands

Command	Description
ip redirects	Enables the sending of ICMP redirect messages if the Cisco IOS software is forced to resend a packet through the same interface on which it was received.
show ip redirects	Displays the address of a default gateway (router) and the address of hosts for which an ICMP redirect message has been received.

ip dhcp aaa default username

To specify the default user name for non-virtual routing and forwarding (VRF) address pools that have been configured to obtain subnets through authentication, authorization, and accounting (AAA), use the **ip dhcp aaa default username**command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip dhcp aaa default username *name*
no ip dhcp aaa default username *name*

Syntax Description

name	Name of the address pool.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(15)T	The behavior when the username attribute is sent in the AAA request was changed.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Address pools that are configured with the **vrf** and **origin aaa** commands will set the username attribute in the AAA request to the specified VRF name. If the VPN ID as specified in RFC 2685 is configured for the VRF, the VPN ID will be sent instead.

Address pools that are not configured with the **vrf** command but are configured with the **origin aaa** command, will set the username attribute in the AAA request to the specified name in the **ip dhcp aaa default username** command.

Use the **debug aaa attribute** command to verify the value of the username attribute in the subnet request to the AAA server.

In Cisco IOS Release 12.2(8)T, if this command is not configured, no AAA subnet request from non-VRF ODAPs will be sent.

In Cisco IOS Release 12.2(15)T, if the DHCP pool is not configured with VRF and the **ip dhcp aaa default username** command is not configured, the AAA request will still be sent with the username attribute set to the Dynamic Host Configuration Protocol (DHCP) pool name.

This command is not needed if all on-demand address pools (ODAPs) on the VHG/provider edge (PE) are VRF-associated.

Examples

The following example sets the username attribute in the AAA request to abc:

```
ip dhcp aaa default username abc
```

Related Commands

Command	Description
debug aaa attribute	Verifies the value of the AAA attributes.
origin	Configures an address pool as an on-demand address pool.
vrf	Associates the on-demand address pool with a VPN routing and forwarding instance.

ip dhcp auto-broadcast

To configure a Dynamic Host Configuration Protocol (DHCP) server on your network to respond only with unicast messages instead of automatically switching to broadcast responses, use the **no ip dhcp auto-broadcast** command in global configuration mode. The default behavior is represented by the **ip dhcp auto-broadcast** command.

ip dhcp auto-broadcast
[no] ip dhcp auto-broadcast

Command Default

The default command, **ip dhcp auto-broadcast** allows the DHCP server to send broadcast messages to a client after the server has tried sending two unicast messages. Change this default behavior, so that the DHCP server sends unicast messages to a client, by using the "no" form of the command: **no ip auto-broadcast**.

Command Modes

Global configuration mode.

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S

Usage Guidelines

Usually, when the client requests a unicast response from the DHCPv4 server, the server responds with a unicast message. However, sometimes these unicast responses can get lost or the client does not have the support to handle unicast messages. In such cases, after sending two unicast offer response messages, if the client still sends the same request packet, the server understands that the client is unable to receive unicast messages and automatically responds with a broadcast message.

You can use the **no ip dhcp auto-broadcast** command to change this behavior and ensure that the server continues to send unicast messages to the client.

Examples

The following command specifies that a DHCP server sends unicast messages to the client:

```
no ip dhcp auto-broadcast
```

Related Commands

Command	Description
ip dhcp clientbroadcast-flag	Configures a DHCP client to set or clear the broadcast flag.

ip dhcp bootp ignore

To enable a Dynamic Host Configuration Protocol (DHCP) server to selectively ignore and not reply to received Bootstrap Protocol (BOOTP) request packets, use the **ip dhcp bootp ignore**command in global configuration mode. To return to the default behavior, use the **no** form of this command.

ip dhcp bootp ignore
no ip dhcp bootp ignore

Syntax Description

This command has no arguments or keywords.

Command Default

The default behavior is to service BOOTP requests.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

A DHCP server can forward ignored BOOTP request packets to another DHCP server if the **ip helper-address** command is configured on the incoming interface. If the **ip helper-address** command is not configured, the router will drop the received BOOTP request.

Examples

The following example shows that the router will ignore received BOOTP requests:

```
hostname Router
!
ip subnet-zero
!
ip dhcp bootp ignore
```

Related Commands

Command	Description
ip bootp server	Enables the BOOTP service on routing devices.
ip helper-address	Forwards UDP broadcasts, including BOOTP, received on an interface.

ip dhcp class

To define a Dynamic Host Configuration Protocol (DHCP) class and enter DHCP class configuration mode, use the **ip dhcp class**command in global configuration mode. To remove the class, use the **no** form of this command.

ip dhcp class *class-name*
no ip dhcp class *class-name*

Syntax Description

class-name	Name of the DHCP class.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

DHCP class configuration provides a method to group DHCP clients based on some shared characteristics other than the subnet in which the clients reside.

Examples

The following example defines three DHCP classes and their associated relay agent information patterns. Note that CLASS3 is considered a “match to any” class because it has no relay agent information pattern configured:

```
ip dhcp class CLASS1
 relay agent information
! Relay agent information patterns
  relay-information hex 01030a0b0c02050000000123
  relay-information hex 01030a0b0c02*
  relay-information hex 01030a0b0c02050000000000 bitmask 00000000000000000000FF
ip dhcp class CLASS2
 relay agent information
! Relay agent information patterns
  relay-information hex 01040102030402020102
  relay-information hex 01040101030402020102
ip dhcp class CLASS3
 relay agent information
```

Related Commands

Command	Description
relay agent information	Enters relay agent information option configuration mode.

Command	Description
relay-information hex	Specifies a hexadecimal string for the full relay agent information option.

ip dhcp client

To configure the Dynamic Host Configuration Protocol (DHCP) client to associate any added routes with a specified tracked object number, use the **ip dhcp client**command in interface configuration mode. To restore the default setting, use the **no** form of this command.

ip dhcp client route track *number*
no ip dhcp client route track

Syntax Description

route track *number*	Associates a tracked object number with the DHCP-installed static route. Valid values for the *number* argument range from 1 to 500.

Command Default

No routes are associated with a track number.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)XE	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **ip dhcp client** command must be configured before the **ip address dhcp**command is configured on an interface. The **ip dhcp client**command is checked only when an IP address is acquired from DHCP. If the **ip dhcp client** command is specified after an IP address has been acquired from DHCP, the **ip dhcp client** command will not take effect until the next time the router acquires an IP address from DHCP.

Examples

The following example configures DHCP on an Ethernet interface and associates tracked object 123 with routes generated from this interface:

```
interface ethernet 0/0
 ip dhcp client route track 123
 ip address dhcp
```

Related Commands

Command	Description
ip address dhcp	Acquires an IP address on an Ethernet interface from the DHCP.

ip dhcp client authentication key-chain

To specify the key chain to be used in authenticating a request, use the **ip dhcp client authentication key-chain**command in interface configuration mode. To disable the key-chain authentication, use the **no** form of this command.

ip dhcp client authentication key-chain *name* [**forcerenew**]
no ip dhcp client authentication key-chain

Syntax Description

name	Name of the key chain.
forcerenew	(Optional) Configures DHCP authentication only for FORCERENEW messages.

Command Default

Authentication is not specified.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.1(4)M	This command was modified. The **forcerenew** keyword was added.

Usage Guidelines

Configure the **ip dhcp client authentication key-chain** command to send to the server the authentication messages that are encoded by the secret ID and secret value that were configured using the **key chain** command. When authentication is enabled, all client-server exchanges must be authenticated; the **ip dhcp client authentication mode**and **key chain** commands must be configured.

When the **ip dhcp client authentication key-chain** command is configured, authentication is enabled for all the DHCP messages including FORCERENEW messages that are received through the interface. To configure DHCP authentication only for the FORCERENEW messages, use **forcerenew** keyword.

Examples

The following example shows how to specify a key chain named chain1 for authentication exchanges:

```
Router(config-if)# ip dhcp client authentication key-chain chain1
```

Related Commands

Command	Description
ip dhcp client authentication mode	Specifies the type of authentication to be used in DHCP messages on the interface.
ip dhcp-client forcerenew	Enables FORCERENEW-message handling on the DHCP client when authentication is enabled.
key chain	Identifies a group of authentication keys for routing protocols.

ip dhcp client authentication mode

To specify the type of authentication to be used in DHCP messages on the interface, use the **ip dhcp client authentication mode** command in interface configuration mode. To remove the specification, use the **no** form of this command.

ip dhcp client authentication mode {**md5** | **token**} [**forcerenew**]
no ip dhcp client authentication mode

Syntax Description

md5	Specifies MD5-based authentication.
token	Specifies token-based authentication.
forcerenew	(Optional) Configures DHCP authentication only for FORCERENEW messages.

Command Default

No authentication mode is configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.1(4)M	This command was modified. The **forcerenew** keyword was added.

Usage Guidelines

Token-based authentication is useful only for basic protection against inadvertently instantiated DHCP servers. Tokens are transmitted in plain text; they provide weak authentication and do not provide message authentication. MD5-based authentication provides better message and entry authentication because it specifies the generation of a temporary value by the source.

When the **ip dhcp client authentication key-chain** command is configured, authentication is enabled for all the DHCP messages including FORCERENEW messages that are received through the interface. To configure DHCP authentication only for FORCERENEW messages, use the **forcerenew** keyword.

Examples

The following example shows how to specify chain1 as the key chain and MD5 as the mode for authentication exchanges:

```
Router(config-if)# ip dhcp client authentication key-chain chain1
Router(config-if)# ip dhcp client authentication mode md5
```

Related Commands

Command	Description
ip dhcp client authentication key-chain	Specifies the key chain to be used in DHCP authentication requests.
ip dhcp-client forcerenew	Enables FORCERENEW-message handling on the DHCP client when authentication is enabled.

Command	Description
key chain	Identifies a group of authentication keys for routing protocols.

ip dhcp client broadcast-flag (interface)

To configure a DHCP client to set or clear the broadcast flag, use the **ip dhcp client broadcast-flag** command in interface configuration mode. To disable the configuration, use the **no** form of this command.

ip dhcp client broadcast-flag {**clear** | **set**}
no ip dhcp client broadcast-flag

Syntax Description

clear	Clears the broadcast flag.
set	Sets the broadcast flag.

Command Default

The broadcast flag is set.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

For a DHCP server to work on a Dynamic Multipoint VPN (DMVPN) network, the DHCP client available on the spoke must unicast the DHCP messages from the server to the client. By default, the DHCP client on the spoke broadcasts the DHCP messages. The broadcast flag is set during broadcast. Hence, the DHCP client on the spoke must have an option to clear the DHCP broadcast flag. You can use the **ip dhcp client broadcast-flag** command to configure the DHCP client to set or clear the broadcast flag.

Examples

The following example shows how to configure a DHCP client to clear the broadcast flag:

```
Router(config)# tunnel 1
Router(config-if)# ip dhcp client broadcast-flag clear
```

Related Commands

Command	Description
ip address dhcp	Acquires an IP address on an interface from the DHCP.
ip dhcp support tunnel unicast	Configures a spoke-to-hub tunnel to unicast the DHCP replies over the DMVPN network.

ip dhcp client class-id

To specify the class identifier, use the **ip dhcp client class-id** command in interface configuration mode. To remove the class identifier, use the **no** form of this command.

ip dhcp client class-id {*string* | **hex** *string*}
no ip dhcp client class-id {*string* | **hex** *string*}

Syntax Description

string	A unique ASCII string.
hex *string*	A unique hexadecimal value.

Command Default

No class identifier is specified.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)XF	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The **ip dhcp client class-id** command is checked only when an IP address is acquired from a Dynamic Host Configuration Protocol (DHCP) server. If the command is specified after an IP address has been acquired from the DHCP server, the command will not take effect until the next time the router acquires an IP address from the DHCP server. This means that the new configuration will only take effect after either the **ip address dhcp** command or the **release dhcp** and **renew dhcp**EXECcommandshave been specified.

The class identifier is used by vendors to specify the type of device that is requesting an IP address. For example, docsis 1.0 can be used for a cable modem and Cisco Systems, Inc. IP Phone can be used for a Cisco IP phone.

Examples

The following example configures a class identifier with a hexadecimal string of ABCDEF1235:

```
interface Ethernet 1
 ip dhcp client class-id hex ABCDEF1235
```

Related Commands

Command	Description
ip address dhcp	Acquires an IP address on an interface from DHCP.
release dhcp	Performs an immediate release of a DHCP lease for an interface.
renew dhcp	Performs an immediate renewal of a DHCP lease for an interface.

ip dhcp client client-id

To specify a client identifier and override the default client identifier, use the **ip dhcp client client-id** command in interface configuration mode. To return to the default form, use the **no** form of this command.

ip dhcp client client-id {*interface-name* | **ascii** *string* | **hex** *string* | **reuse-mac**}
no ip dhcp client client-id {*interface-name* | **ascii** *string* | **hex** *string* | **reuse-mac**}

Syntax Description

interface-name	Interface from which the MAC address is used.
ascii *string*	Specifies a unique ASCII string. The default value is cisco-*mac-name* where *mac* is the MAC address of the interface and 'name' is the short form of the interface name.
hex *string*	Specifies a unique hexadecimal value.
reuse-mac	Reuses the MAC address configured by the **atm ether-mac-address** command. **Note** The **reuse-mac** keyword is to be used only on ATM subinterfaces along with the **atm ether-mac-address** command.

Command Default

The client identifier is an ASCII value in the form cisco-*mac-name* where *mac* is the MAC address of the interface and *name* is the short form of the interface name.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)XF	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
15.1(4)M4	This command was modified and integrated into Cisco IOS Release 15.1(4)M4. The **reuse-mac** keyword was added.

Usage Guidelines

The **ip dhcp client client-id** command is specified only when an IP address is acquired from a DHCP server. If the command is specified after an IP address has been acquired from the DHCP server, the command will not take effect until the next time the device acquires an IP address from the DHCP server. This means that the new configuration will only take effect after either the **ip address dhcp** command or the **release dhcp** and **renew dhcp** EXEC commands have been specified.

When the **no** form of this command is specified, the configuration is removed and the system returns to the default form. To configure the system, a client identifier must be included.

Examples

The following example shows how to configure a client identifier named test-client-id:

```
Device> enable
```

```
Device# configure terminal
Device(config)# interface Ethernet 1
Device(config-if)# ip dhcp client client-id ascii test-client-id
```

Related Commands

Command	Description
ip address dhcp	Acquires an IP address on an interface from the DHCP server.
release dhcp	Performs an immediate release of a DHCP lease for an interface.
renew dhcp	Performs an immediate renewal of a DHCP lease for an interface.

ip dhcp client default-router distance

To configure the default Dynamic Host Configuration Protocol (DHCP) administrative distance, use the **ip dhcp client default-router distance** command in interface configuration mode. To disable the configuration, use the **no** form of this command.

ip dhcp client default-router distance *metric-value*
no ip dhcp client default-router distance

Syntax Description

metric-value	Default route metric value. Range: 1 to 255. Default: 254.

Command Default

The default administrative distance is 254.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

While you are adding the default route the administrative distance is calculated as follows:

- Interface configuration is given the highest preference if the metric value is not set to the default value.
- If a metric value is not configured on an interface, then the existing global configuration command will get preference.
- If the administrative distance is not configured in both interface configuration mode and global configuration mode, then the global configuration default distance of 254 is used.

Examples

The following example shows how to configure the DHCP default route metric to 2:

```
Router # configure terminal
Router(config)# interface FastEthernet 0/2
Router(config-if)# ip dhcp client default-router distance 2
```

Related Commands

Command	Description
debug dhcp client	Displays debugging information about the DHCP client activities and monitors the status of DHCP packets.
ip dhcp-client default-router distance	Configures a default DHCP administrative distance for clients in global configuration mode.
show ip route dhcp	Displays the routes added to the routing table by the DHCP server and relay agent.

ip dhcp client hostname

To specify or modify the hostname sent in a Dynamic Host Configuration Protocol (DHCP) message, use the **ip dhcp client hostname** command in interface configuration mode. To remove the hostname, use the **no** form of this command.

ip dhcp client hostname *host-name*
no ip dhcp client hostname *host-name*

Syntax Description

host-name	Name of the host.

Command Default

The hostname is the globally configured hostname of the router.

Command Modes

Interface configuration(config-if)

Command History

Release	Modification
12.3(2)XF	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The **ip dhcp client hostname** command is checked only when an IP address is acquired from a DHCP server. If the command is specified after an IP address has been acquired from DHCP, it will not take effect until the next time the router acquires an IP address from the DHCP server. This means that the new configuration will only take effect after either the **ip address dhcp** command or the **release dhcp** and **renew dhcp**EXECcommandshave been specified.

This command is applicable only for DHCP requests generated by Cisco IOS software. This command is ignored when Cisco IOS software relays requests (for example, from Distributed Route Processor PPP clients).

Examples

The following example shows how to specify the hostname of the DHCP client as hostA:

```
interface Ethernet 1
 ip dhcp client hostname hostA
```

Related Commands

Command	Description
ip address dhcp	Acquires an IP address on an interface from DHCP.
release dhcp	Performs an immediate release of a DHCP lease for an interface.
renew dhcp	Performs an immediate renewal of a DHCP lease for an interface.

ip dhcp client lease

To configure the duration of the lease for an IP address that is requested from a Dynamic Host Configuration Protocol (DHCP) client to a DHCP server, use the **ip dhcp client lease**command in interface configuration mode. To restore to the default value, use the **no** form of this command.

ip dhcp client lease *days* [*hours*] [*minutes*]
no ip dhcp client lease

Syntax Description

days	Specifies the duration of the lease in days.
hours	(Optional) Specifies the number of hours in the lease. A *days* value must be supplied before an *hours* value can be configured.
minutes	(Optional) Specifies the number of minutes in the lease. A *days* value and an *hours* value must be supplied before a *minutes* value can be configured.

Command Default

A default lease time is not included in the DHCP DISCOVER messages sent by the client. The client accepts the lease time that the DHCP server sends.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)XF	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The **ip dhcp client lease**command is checked only when an IP address is acquired from a DHCP server. If the command is specified after an IP address has been acquired from DHCP, it will not take effect until the next time the router acquires an IP address from the DHCP server. This means that the new configuration will only take effect after either the **ip address dhcp** command or the **release dhcp** and **renew dhcp**EXECcommandshave been specified.

Examples

The following example shows a one-day lease:

```
ip dhcp client lease 1
```

The following example shows a one-hour lease:

```
ip dhcp client lease 0 1
```

The following example shows a one-minute lease:

```
ip dhcp client lease 0 0 1
```

Related Commands

Command	Description
ip address dhcp	Acquires an IP address on an interface from DHCP.
lease	Configures the duration of the lease for an IP address that is assigned from a DHCP server to a DHCP client
release dhcp	Performs an immediate release of a DHCP lease for an interface.
renew dhcp	Performs an immediate renewal of a DHCP lease for an interface.

ip dhcp client mobile renew

To configure the number of renewal attempts and the interval between attempts for renewing an IP address acquired by a Dynamic Host Configuration Protocol (DHCP) client, use the **ip dhcp client mobile renew** command in interface configuration mode. To disable the functionality, use the **no** form of this command.

ip dhcp client mobile renew count *number* **interval** *ms*
no ip dhcp client mobile renew count *number* **interval** *ms*

Syntax Description

count *number*	Number of attempts to renew a current IP address before starting the DHCP discovery process. The range is from 0 to 10 attempts. The default is 2 attempts.
interval *ms*	Interval to wait between renewal attempts. The range is from 1 to 1000 ms. The default is 50 ms.

Command Default

count *number* : 2**interval** *ms*: 50

Command Modes

Interface configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Mobile DHCP clients automatically attempt to renew an existing IP address in response to certain events, such as moving between wireless access points. The number of renewal attempts, and the interval between those attempts, depending on network conditions, can be modified by using the **ip dhcp client mobile renew** command.

Examples

In the following example, the DHCP client will make four attempts to renew its current IP address with an interval of 30 milliseconds between attempts :

```
interface FastEthernet0
 ip dhcp client mobile renew count 4 interval 30
```

Related Commands

Command	Description
ip address dhcp	Acquires an IP address on an interface from DHCP.

ip dhcp client request

To configure a Dynamic Host Configuration Protocol (DHCP) client to request an option from a DHCP server, use the **ip dhcp client request**command in interface configuration mode. To remove the request for an option, use the **no** form of this command.

ip dhcp client request *option-name*
no ip dhcp client request *option-name*

Syntax Description

option-name	The option name can be one of the following keywords: • **tftp-server-address** • **sip-server-address** • **netbios-nameserver** • **vendor-specific** • **vendor-identifying-specific** • **static-route** • **classless -static-route** • **domain-name** • **dns-nameserver** • **router** By default, all these options except **sip-server-address**, **vendor-identifying-specific**, and **classless-static-route**are requested.

Command Default

All the options are requested except **sip-server-address**, **vendor-identifying-specific**,and **classless-static-route**.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)XF	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(22)YB	This command was modified. The **sip-server-address**, **vendor-identifying-specific**,and **classless-static-route**keywords were added.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

By default, all options except **sip-server-address**, **vendor-identifying-specific**,and **classless-static-route**are requested, so you must use the **no** form of the **ip dhcp client request**command to disable those default options, and explicitly specify any options that are not enabled by default.

Default options that are specified by the **no** form are removed from the DHCP originated address for the interface. An option can be reinserted in the list of requested options by using the same command without the **no** keyword. Multiple options can be specified on one configuration line. However, each option will appear on a separate line in the running configuration.

The **ip dhcp client request** command is checked only when an IP address is acquired from a DHCP server. If the command is specified after an IP address has been acquired from DHCP, it will not take effect until the next time the router acquires an IP address from the DHCP server. This means that the new configuration will take effect only after either the **ip address dhcp** command or a DHCP lease renewal or termination that is not initiated by a **release dhcp** or a **renew dhcp** command.

Examples

The following example shows how to configure the DHCP client to remove the DNS name server from the options requested from the DHCP server:

```
no ip dhcp client request dns-nameserver
```

Related Commands

Command	Description
ip address dhcp	Acquires an IP address on an interface from DHCP.
ip dhcp-client forcerenew	Enables forcerenew-message handling on the DHCP client when authentication is enabled.
ip dhcp client authentication key-chain	Specifies the authentication key used for the DHCP protocol on the interface.
ip dhcp client authentication mode	Specifies the type of authentication to be used in DHCP messages on the interface.
release dhcp	Performs an immediate release of a DHCP lease for an interface.
renew dhcp	Performs an immediate renewal of a DHCP lease for an interface.

ip dhcp client route

To configure the Dynamic Host Configuration Protocol (DHCP) client to associate any added routes with a specified tracked object number, use the **ip dhcp client** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

ip dhcp client route track *number*
no ip dhcp client route track

Syntax Description

route track *number*	Associates a tracked object number with the DHCP-installed static route. Valid values for the *number* argument range from 1 to 500.

Command Default

No routes are associated with a track number.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)XE	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

The **ip dhcp client** command must be configured before the **ip address dhcp** command is configured on an interface. The **ip dhcp client** command is checked only when an IP address is acquired from DHCP. If the **ip dhcp client** command is specified after an IP address has been acquired from DHCP, the **ip dhcp client** command will not take effect until the next time the router acquires an IP address from DHCP.

Examples

The following example configures DHCP on an Ethernet interface and associates tracked object 123 with routes generated from this interface:

```
interface ethernet 0/0
 ip dhcp client route track 123
 ip address dhcp
```

Related Commands

Command	Description
ip address dhcp	Acquires an IP address on an Ethernet interface from the DHCP.

ip dhcp client update dns

To enable Dynamic Domain Name System (DDNS) updates of address (A) Resource Records (RRs) using the same hostname passed in the hostname and fully qualified domain name (FQDN) options by a client, use the **ip dhcp client update dns** command in interface configuration mode. To disable dynamic updates of A RRs, use the **no** form of this command.

ip dhcp client update dns [**server** {**both** | **none**}]
no ip dhcp client update dns [**server** {**both** | **none**}]

Syntax Description

server	(Optional) Specifies that the client will include an FQDN option specifying the "N" flag. The server will not perform any DDNS updates for the client. The server can, of course, override this configuration and do the updates anyway. • **both** --Enables the DHCP client to perform DDNS updates on both A (forward) and PTR (reverse) RRs in the primary DNS server unless the DHCP server has specified in the DHCP ACK FQDN option that it has overridden the client request and has updated the information previously. **Note** If the **both** keyword is specified, it means that the client will include an FQDN option specifying the S flag. This keyword instructs the server that it should attempt to dynamically update both the A and PTR RRs. • **none** --On the client side, specifies that the DHCP client should include the FQDN option; however, it should not attempt any DDNS updates. **Note** If the **none** keyword is not specified, the FQDN option will result in the server updating the PTR RR and neither the server nor the client will update the A RR.

Command Default

No default behavior.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(8)YA	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Usage Guidelines

Commands that are configured in interface configuration mode override the commands configured using global configuration mode. The **ip dhcp-client update dns** command (hyphenated) is the global configuration command.

If you specify the **both** and **none** keywords in separate configurations, the DHCP client will update both the A and PTR RRs, and the DHCP server will not perform any updates. If you specify the **none** and **both** keywords (in this order), the DHCP client will not perform any updates and the server will update both the A and PTR RRs.

There are two parts to the DDNS update configuration on the client side. First, if the **ip ddns update method** command is configured on the client, which specifies the DDNS-style updates, then the client will be trying to generate or perform A updates. If the **ip ddns update method ddns both** command is configured, then the client will be trying to update both A and PTR RRs.

Second, the only way for the client to communicate with the server, with reference to what updates it is generating or expecting the server to generate, is to include an FQDN option when communicating with the server. Whether or not this option is included is controlled on the client side by the **ip dhcp-client update dns** command in global configuration mode or the **ip dhcp client update dns** command in interface configuration mode.

Even if the client instructs the server to update both or update none, the server can override the client request and do whatever it was configured to do anyway. If there is an FQDN option in the DHCP interaction as above, then the server can communicate to the client that it was overridden, in which case the client will not perform the updates because it knows that the server has done the updates. Even if the server is configured to perform the updates after sending the ACK (the default), it can still use the FQDN option to instruct the client what updates it will be performing and thus the client will not do the same types of updates.

If the server is configured with the **update dns** command with or without any keywords, and if the server does not see an FQDN option in the DHCP interaction, then it will assume that the client does not understand DDNS and will automatically act as though it were configured to update both A and PTR RRs on behalf of the client.

Examples

The following example shows how to configure the DHCP client to perform A and PTR RR updates, but the DHCP server will not perform the updates:

```
ip dhcp client update dns server none
```

Related Commands

Command	Description
ip ddns update method	Specifies a method of DDNS updates of A and PTR RRs and the maximum interval between the updates.

ip dhcp compatibility lease-query client

To configure the Dynamic Host Configuration Protocol (DHCP) client to send a lease query according to RFC 4388, use the **ip dhcp compatibility lease-query client** command in global configuration mode. To disable this configuration, use the **no** form of this command.

ip dhcp compatibility lease-query client {**cisco** | **standard**}
no ip dhcp compatibility lease-query client

Syntax Description

cisco	Configures the DHCP client to use the Cisco standard lease-query message type. This is the default value.
standard	Configures the DHCP client to use the RFC 4388 standard lease-query message type.

Command Default

The DHCP client is configured to use the Cisco standard lease-query message type.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(22)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SCE1	This command was integrated into Cisco IOS Release 12.2(33)SCE1.

Usage Guidelines

Some DHCP servers support only the RFC 4388 standard of lease query. If the DHCP server supports only the RFC 4388 standard, then you must configure the DHCP client to send a lease query according to the RFC 4388 standard.

The Cisco IOS DHCP client sends a lease query with the message type set to 13 and receives either an ACK (acknowledge) or NAK (deny) from the DHCP server. This is the behavior of the DHCP client as per the Cisco standard.

As per the RFC 4388 standard, if a DHCP server receives a lease query with the message type set to 10, it will reply with one of the following message types:

- DHCPLEASEUNASSIGNED 11
- DHCPLEASEUNKNOWN 12
- DHCPLEASEACTIVE 13

By using the **ip dhcp compatibility lease-query client** command, you can switch between the Cisco standard and the RFC 4388 standard implementation.

Examples

The following example shows how to configure the DHCP client to switch from the Cisco standard implementation to the RFC 4388 standard implementation:

```
Router(config)# ip dhcp compatibility lease-query client standard
```

Related Commands

Command	Description
ip dhcp compatibility suboption	Configures DHCP compatibility for a relay-agent suboption.

ip dhcp compatibility suboption link-selection

To configure the Dynamic Host Configuration Protocol (DHCP) client to use private as well as the Internet Assigned Numbers Authority (IANA) standard relay agent suboption numbers, use the **ip dhcp compatibility suboption link-selection** command in global configuration mode. To disable this configuration, use the **no** form of this command.

ip dhcp compatibility suboption link-selection {**cisco** | **standard**}
no ip dhcp compatibility suboption link-selection

Syntax Description

cisco	Configures the DHCP client to use the private Cisco suboption numbers.
standard	Configures the DHCP client to use the standard IANA suboption numbers.

Command Default

Disabled. (The DHCP client is configured to use the private relay agent suboption numbers.)

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Sometimes new features are implemented in advance of standardization. That is, features are developed before the IANA numbers are assigned to the relay agent suboptions. In these cases, the DHCP client uses the private Cisco relay agent suboption numbers. When the IANA numbers are assigned later, the DHCP client must be able to use both the private as well as the IANA relay suboption numbers. You can use the **ip dhcp compatibility suboption link-selection** command to configure the DHCP client to use the IANA relay agent suboption numbers.

Examples

The following example shows how to configure the DHCP client to support the relay agent with the IANA standard suboption numbers:

```
Router(config)# ip dhcp compatibility suboption link-selection standard
```

Related Commands

Command	Description
ip dhcp compatibility lease-query client	Configures the DHCP client to send a lease query according to the RFC 4388 standard.

ip dhcp conflict logging

To enable conflict logging on a Dynamic Host Configuration Protocol (DHCP) server, use the **ip dhcp conflict logging** command in global configuration mode. To disable conflict logging, use the **no** form of this command.

ip dhcp conflict logging
no ip dhcp conflict logging

Syntax Description

This command has no arguments or keywords.

Command Default

Conflict logging is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

A DHCP server database agent should be used to store automatic bindings. If a DHCP server database agent is not used, specify the **no ip dhcp conflict logging** command to disable the recording of address conflicts. By default, the DHCP server records DHCP address conflicts in a log file.

Examples

The following example disables the recording of DHCP address conflicts:

```
no ip dhcp conflict logging
```

Related Commands

Command	Description
clear ip dhcp conflict	Clears an address conflict from the Cisco IOS DHCP server database.
ip dhcp database	Configures a Cisco IOS DHCP server to save automatic bindings on a remote host called a database agent.
show ip dhcp conflict	Displays address conflicts found by a Cisco IOS DHCP server when addresses are offered to the client.

ip dhcp conflict resolution

To configure Dynamic Host Configuration Protocol (DHCP) address conflict resolution, use the **ip dhcp conflict resolution** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ip dhcp conflict resolution [**interval** *minutes*]
no ip dhcp conflict resolution

Syntax Description

interval *minutes*	(Optional) Specifies the time interval, in minutes. Range: 5 to 1440. Default: 60.

Command Default

DHCP address conflict resolution is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

DHCP addresses added to the conflicted address list may become available after some time. This behavior will eventually cause a major chunk of the IP addresses that are actually available to be blocked.

You can use the **ip dhcp conflict resolution** command to configure the DHCP server to periodically audit the conflicted address list and clear the inactive IP addresses.

Examples

The following example shows how to configure address conflict resolution on a DHCP server to take place after 65 minutes:

```
Router # configure terminal
Router(config)# ip dhcp conflict resolution interval 65
```

Related Commands

Command	Description
ip dhcp conflict logging	Enables conflict logging on a DHCP server.

ip dhcp database

To configure a Cisco IOS Dynamic Host Configuration Protocol (DHCP) server and relay agent to save automatic bindings on a remote host called a database agent, use the **ip dhcp database** command in global configuration mode. To remove the database agent, use the no form of this command.

ip dhcp database *url* [**timeout** *seconds* | **write-delay** *seconds* | **write-delay** *seconds* **timeout** *seconds*]
no ip dhcp database *url*



Note When using the **ip dhcp database** command, ensure the correct URL is entered. An incorrect URL may cause the **ip dhcp pool** command to hang the console as the DHCP service attempts to reach the URL multiple times before returning a failure. This is expected behavior from the DHCP side. Additionally, it is crucial to ensure that the file name is included as part of the ftp/tftp URL to prevent this issue.

Syntax Description

url	Specifies the remote file used to store the automatic bindings. The following are acceptable URL file formats: • tftp://host/filename • ftp://user:password@host/filename • rcp://user@host/filename • flash://filename • disk0://filename
timeout *seconds*	(Optional) Specifies how long (in seconds) the DHCP server should wait before aborting a database transfer. Transfers that exceed the timeout period are aborted. By default, DHCP waits 300 seconds (5 minutes) before aborting a database transfer. Infinity is defined as 0 seconds.
write-delay *seconds*	(Optional) Specifies how soon the DHCP server should send database updates. By default, DHCP waits 300 seconds (5 minutes) before sending database changes. The minimum delay is 60 seconds.

Command Default

DHCP waits 300 seconds for both a write delay and a timeout.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

A DHCP database agent is any host (for example, an FTP, TFTP, or rcp server) or storage media on the DHCP server (for example, disk0) that stores the DHCP bindings database. You can configure multiple DHCP database agents, and you can configure the interval between database updates and transfers for each agent.

The DHCP relay agent can save route information to the same database agents to ensure recovery after reloads.

In the following example, the timeout value and write-delay are specified in two separate command lines:

```
ip dhcp database disk0:router-dhcp timeout 60
ip dhcp database disk0:router-dhcp write-delay 60
```

However, the second configuration overrides the first command line and causes the timeout value to revert to the default value of 300 seconds. To prevent the timeout value from reverting to the default value, configure the following on one command line:

```
ip dhcp database disk0:router-dhcp write-delay 60 timeout 60
```

Examples

The following example specifies the DHCP database transfer timeout value as 80 seconds:

```
ip dhcp database ftp://user:password@172.16.1.1/router-dhcp timeout 80
```

The following example specifies the DHCP database update delay value as 100 seconds:

```
ip dhcp database tftp://172.16.1.1/router-dhcp write-delay 100
```

Related Commands

Command	Description
show ip dhcp database	Displays Cisco IOS DHCP Server database agent information.

ip dhcp debug ascii-client-id

To display the client ID in ASCII format in Dynamic Host Configuration Protocol (DHCP) debug output, use the **ip dhcp debug ascii-client-id** command in global configuration mode. To disable To disable display of the client ID in ASCII format in Dynamic Host Configuration Protocol (DHCP) debug output, use the **no** form of this command.

ip dhcp debug ascii-client-id
no ip dhcp debug ascii-client-id

Syntax Description

This command has no arguments or keywords.

Command Default

DHCP debug outputs do not display the client ID in ASCII format.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(1)T	This command was introduced.

Usage Guidelines

Use the **ip dhcp debug ascii-client-id** command to display the client ID in ASCII format in Dynamic Host Configuration Protocol (DHCP) debug output.

Examples

The following example shows how to display the client ID in ASCII format in Dynamic Host Configuration Protocol (DHCP) debug output:

```
Router(config)# ip dhcp debug ascii-client-id
```

Related Commands

Command	Description
odap client	Configures ODAP client parameters.

ip dhcp excluded-address

To specify IP addresses that a Dynamic Host Configuration Protocol (DHCP) server should not assign to DHCP clients, use the **ip dhcp excluded-address** command in global configuration mode. To remove the excluded IP addresses, use the no form of this command.

ip dhcp excluded-address [**vrf** *vrf-name*] *ip-address* [*last-ip-address*]
no ip dhcp excluded-address [**vrf** *vrf-name*] *ip-address* [*last-ip-address*]

Syntax Description

vrf	(Optional) Excludes IP addresses from a virtual routing and forwarding (VRF) space.
vrf-name	(Optional) The VRF name.
ip-address	The excluded IP address, or first IP address in an excluded address range.
last-ip-address	(Optional) The last IP address in the excluded address range.

Command Default

The DHCP server can assign any IP address to the DHCP clients.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.6	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

Use the **ip dhcp excluded-address** command to exclude a single IP address or a range of IP addresses.

The DHCP server assumes that all pool addresses can be assigned to the clients. You cannot use the **ip dhcp excluded-address** command to stop the DHCP server from assigning the pool addresses (assigned to an interface using the **ip address pool** command) to the clients. That is, the **ip dhcp excluded-address** command is not supported for the addresses assigned using the **ip address pool** command.

Examples

The following example shows how to configure an excluded IP address range from 172.16.1.100 through 172.16.1.199:

```
Router> enable
Router# configure terminal
Router(config)#
ip dhcp excluded-address vrf vrf1 172.16.1.100 172.16.1.199
```

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

Command	Description
network (DHCP)	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.
ip address pool	Enables the IP address of an interface to be automatically configured when a DHCP pool is populated with a subnet from IPCP negotiation.

ip dhcp global-options

To enter DHCP global options configuration mode, which is used to configure DHCP-related global configurations, use the **ip dhcp global-options** command in global configuration mode. To remove DHCP-related global configurations, use the **no** form of this command.

ip dhcp global-options
no ip dhcp global-options

Syntax Description

This command has no arguments or keywords.

Command Default

DHCP-related global options are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.

Usage Guidelines

You can configure DHCP options that are common for all pools in DHCP global options configuration mode.

Examples

The following example shows how to enter DHCP global options configuration mode:

```
Router(config)# ip dhcp global-options
Router(config-dhcp-global-options)#
```

Related Commands

Command	Description
dns-server (config-dhcp-global-options)	Configures the DNS IP servers that are available to DHCP clients on request.

ip dhcp limit lease log

To enable DHCP lease violation logging when a DHCP lease limit threshold is exceeded, use the **ip dhcp limit lease log** command in global configuration mode. To disable the lease violation logging of DHCP lease violations, use the **no** form of this command.

ip dhcp limit lease log
no ip dhcp limit lease log

Syntax Description

This command has no arguments or keywords.

Command Default

DHCP lease violation logging is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.

Usage Guidelines

The **ip dhcp limit lease log** command logs violations for global- and interface-level lease violations. If this command is configured, any lease limit violations will display in the output of the **show ip dhcp limit lease** command.

Examples

The following example shows how to enable logging of lease violations:

```
Router(config)# ip dhcp limit lease log
```

Related Commands

Command	Description
ip dhcp limit lease	Limits the number of leases offered to DHCP clients per interface.
show ip dhcp limit lease	Displays the number of times the lease limit threshold has been violated on an interface.

ip dhcp limit lease per interface

To limit the number of leases offered to DHCP clients behind an ATM routed bridge encapsulation (RBE) unnumbered or serial unnumbered interface, use the **ip dhcp limit lease per interface** command in global configuration mode. To remove the restriction on the number of leases, use the **no** form of the command.

ip dhcp limit lease per interface *lease-limit*
no ip dhcp limit lease per interface *lease-limit*

Syntax Description

lease-limit	Number of leases allowed. The range is from 1 to 65535.

Command Default

The number of leases offered is not limited.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.

Usage Guidelines

This command is not supported on numbered interfaces. The lease limit can be applied only to ATM with RBE unnumbered interfaces or serial unnumbered interfaces.

Examples

The following example shows how to allow three DHCP clients to receive IP addresses. If a fourth DHCP client tries to obtain an IP address, the DHCPDISCOVER messages will not be forwarded to the DHCP server.

```
Router(config)# ip dhcp limit lease per interface 3
```

Related Commands

Command	Description
clear ip dhcp limit lease	Clears the stored lease violation entries.
show ip dhcp limit lease	Displays the number of times the lease limit threshold has been violated.

ip dhcp limited-broadcast-address

To override a configured network broadcast and have the Dynamic Host Configuration Protocol (DHCP) server and relay agent send an all networks, all nodes broadcast to a DHCP client, use the **ip dhcp limited-broadcast-address**command in global configuration mode. To disable this functionality, use the no form of this command.

ip dhcp limited-broadcast-address
no ip dhcp limited-broadcast-address

Syntax Description

This command has no arguments or keywords.

Command Default

Default broadcast address: 255.255.255.255 (all ones)

Command Modes

Global configuration

Command History

Release	Modification
12.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When a DHCP client sets the broadcast bit in a DHCP packet, the DHCP server and relay agent send DHCP messages to clients using the all ones broadcast address (255.255.255.255). If the **ip broadcast-address** command has been configured to send a network broadcast, the all ones broadcast set by DHCP is overridden. To remedy this situation, use the **ip dhcp limited-broadcast-address** command to ensure that a configured network broadcast does not override the default DHCP behavior.

Some DHCP clients can only accept an all ones broadcast and may not be able to acquire a DHCP address unless this command is configured on the router interface connected to the client.

Examples

The following example configures DHCP to override any network broadcast:

```
ip dhcp limited-broadcast-address
```

Related Commands

Command	Description
ip broadcast-address	Defines a broadcast address for an interface.

ip dhcp ping packets

To specify the number of packets a Dynamic Host Configuration Protocol (DHCP) server sends to a pool address as part of a ping operation, use the **ip dhcp ping packets** command in global configuration mode. To prevent the server from pinging pool addresses, use the no form of this command. To return the number of ping packets sent to the default value, use the **default** form of this command.

ip dhcp ping packets *number*
no ip dhcp ping packets
default ip dhcp ping packets

Syntax Description

number	The number of ping packets that are sent before the address is assigned to a requesting client. The default value is two packets.

Command Default

Two packets

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The DHCP server pings a pool address before assigning the address to a requesting client. If the ping is unanswered, the DHCP server assumes (with a high probability) that the address is not in use and assigns the address to the requesting client.

Setting the *number* argument to a value of 0 completely turns off DHCP server ping operation .

Examples

The following example specifies five ping attempts by the DHCP server before ceasing any further ping attempts:

```
ip dhcp ping packets 5
```

Related Commands

Command	Description
clear ip dhcp conflict	Clears an address conflict from the Cisco IOS DHCP server database.
ip dhcp ping timeout	Specifies how long a Cisco IOS DHCP Server waits for a ping reply from an address pool.
show ip dhcp conflict	Displays address conflicts found by a Cisco IOS DHCP server when addresses are offered to the client.



ip dhcp ping timeout through ip dhcp-client forcerenew

- ip dhcp ping timeout, on page 253
- ip dhcp pool, on page 254
- ip dhcp relay bootp ignore, on page 256
- ip dhcp relay prefer known-good-server , on page 257
- ip dhcp relay forward spanning-tree, on page 258
- ip dhcp relay information check, on page 259
- ip dhcp relay information check-reply, on page 260
- ip dhcp relay information option, on page 262
- ip dhcp relay information option server-id-override, on page 265
- ip dhcp relay information option subscriber-id, on page 267
- ip dhcp relay information option vpn-id, on page 269
- ip dhcp relay information option-insert, on page 271
- ip dhcp relay information policy, on page 273
- ip dhcp relay information policy-action, on page 275
- ip dhcp relay information trust-all, on page 277
- ip dhcp relay information trusted, on page 278
- ip dhcp-relay source-interface, on page 279
- ip dhcp route connected, on page 280
- ip dhcp server use subscriber-id client-id, on page 281
- ip dhcp smart-relay, on page 282
- ip dhcp snooping, on page 283
- ip dhcp snooping binding, on page 284
- ip dhcp snooping database, on page 285
- ip dhcp snooping detect spurious, on page 287
- ip dhcp snooping detect spurious interval, on page 289
- ip dhcp snooping detect spurious vlan, on page 290
- ip dhcp snooping glean, on page 291
- ip dhcp snooping information option, on page 292
- ip dhcp snooping limit rate, on page 294
- ip dhcp snooping packets, on page 296
- ip dhcp snooping verify mac-address, on page 297

- ip dhcp snooping vlan, on page 298
- ip dhcp subscriber-id interface-name, on page 299
- **ip dhcp support option55-override** , on page 300
- ip dhcp support tunnel unicast, on page 301
- ip dhcp update dns, on page 302
- ip dhcp use, on page 303
- ip dhcp use subscriber-id client-id, on page 305
- ip dhcp-client broadcast-flag, on page 306
- ip dhcp-client default-router distance, on page 307
- ip dhcp-client forcerenew, on page 308

ip dhcp ping timeout

To specify how long a Dynamic Host Configuration Protocol (DHCP) server waits for a ping reply from an address pool, use the **ip dhcp ping timeout** command in global configuration mode. To restore the default number of milliseconds (500) of the timeout, use the no form of this command.

ip dhcp ping timeout *milliseconds*
no ip dhcp ping timeout

Syntax Description

milliseconds	The amount of time (in milliseconds) that the DHCP server waits for a ping reply before it stops attempting to reach a pool address for client assignment. The maximum timeout is 10000 milliseconds (10 seconds). The default timeout is 500 milliseconds.

Command Default

500 milliseconds

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command specifies how long to wait for a ping reply (in milliseconds).

Examples

The following example specifies that a DHCP server will wait 800 milliseconds for a ping reply before considering the ping a failure:

```
ip dhcp ping timeout 800
```

Related Commands

Command	Description
clear ip dhcp conflict	Clears an address conflict from the Cisco IOS DHCP Server database.
ip dhcp ping timeout	Specifies the number of packets a Cisco IOS DHCP Server sends to a pool address as part of a ping operation.
show ip dhcp conflict	Displays address conflicts found by a Cisco IOS DHCP Server when addresses are offered to the client.

ip dhcp pool

To configure a Dynamic Host Configuration Protocol (DHCP) address pool on a DHCP server and enter DHCP pool configuration mode, use the **ip dhcp pool** command in global configuration mode. To remove the address pool, use the no form of this command.

ip dhcp pool *name*
no ip dhcp pool *name*

Note When configuring the **ip dhcp pool** command, note that it can be affected by the **ip dhcp database** command if an incorrect URL is provided. The console may hang due to multiple attempts by the DHCP service to reach the URL before it returns a failure. This is expected behavior. To prevent this issue, ensure that the correct URL, including the file name, is provided when using the **ip dhcp database** command, especially when it includes ftp/tftp.

Syntax Description

name	Name of the pool. Can either be a symbolic string (such as engineering) or an integer (such as 0).

Command Default

DHCP address pools are not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

During execution of this command, the configuration mode changes to DHCP pool configuration mode, which is identified by the (config-dhcp)# prompt. In this mode, the administrator can configure pool parameters, like the IP subnet number and default router list.

Examples

The following example configures pool1 as the DHCP address pool:

```
ip dhcp pool pool1
```

Related Commands

Command	Description
host	Specifies the IP address and network mask for a manual binding to a DHCP client.
ip dhcp excluded-address	Specifies IP addresses that a Cisco IOS DHCP server should not assign to DHCP clients.

Command	Description
network (DHCP)	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.

ip dhcp relay bootp ignore

To configure the Dynamic Host Configuration Protocol (DHCP) relay agent stop forwarding Bootstrap Protocol (BOOTP) packets between the clients and servers, use the **ip dhcp relay bootp ignore** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ip dhcp relay bootp ignore
no ip dhcp relay bootp ignore

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled (Relay agent forwards BOOTP packets from clients and servers).

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

You can use the **ip dhcp relay agent bootp ignore** command in network deployments, where clients send both BOOTP and DHCP packets. When the client sends both type of packets, sometimes the DHCP server or the relay agent will not be able to differentiate between the two types of packets. You can use this command to configure the relay agent stop forwarding the BOOTP packets.

Examples

The following example shows how to configure the relay agent to stop forwarding BOOTP packets:

```
Router# configure terminal
Router(config)# ip dhcp relay bootp ignore
```

Related Commands

Command	Description
ip dhcp relay information	Configures a DHCP server to validate the relay agent information option.
ip dhcp bootp ignore	Configures the DHCP server to stop processing BOOTP packets from clients.

ip dhcp relay prefer known-good-server

To configure the Dynamic Host Configuration Protocol (DHCP) relay agent to forward the client requests to the server that handled the previous request, use the **ip dhcp relay prefer known-good-server** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ip dhcp relay prefer known-good-server
no ip dhcp relay prefer known-good-server

Syntax Description

This command has no arguments or keywords.

Command Default

The relay agent does not forward the requests based on the preference.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

The DHCP servers send addresses to the DHCP clients. Because the DHCP server that responds first cannot be predicted, the client receives different addressees from the servers. This results in unpredictable changes in the address used by the client. Such address changes result in TCP service interruptions. You can configure the **ip dhcp relay prefer known-good-server** command to reduce the frequency with which the DHCP clients change their address and to forward the client requests to the server that handled the previous request.

If the **ip dhcp relay prefer known-good-server** command is configured, and the DHCP client is attached to an unnumbered interface, then the DHCP relay checks if the DHCP client broadcasts the DHCP packets. If the packets are broadcast, the server unicasts the requests to all configured helper addresses, and not just to the server that handled the previous request. If the packets are unicast, the DHCP relay forwards the unicast packets from the client to the DHCP server that had assigned the IP address to the client.

This functionality impacts the DHCPv4 relay, and not the DHCPv6 relay.

Examples

The following example shows how to configure the DHCP relay agent to forward the client requests to the server that handled the previous request:

```
Router# configure terminal
Router(config)# ip dhcp relay prefer known-good-server
```

Related Commands

Command	Description
ip helper-address	Enables the forwarding of UDP broadcasts, including BOOTP, received on an interface.

ip dhcp relay forward spanning-tree

To set the gateway address (giaddr) field in the DHCP packet before forwarding to spanning-tree interfaces, use the **ip dhcp relay forward spanning-tree** command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip dhcp relay forward spanning-tree
no ip dhcp relay forward spanning-tree

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

Prior to Cisco IOS Release 12.1, when the **ip forward-protocol spanning-tree any-local-broadcast** command was configured, DHCP broadcasts were forwarded to all spanning-tree enabled interfaces after setting the giaddr field in the DHCP packet.

The behavior of the DHCP relay agent was modified in release 12.1 such that the DHCP broadcasts were still forwarded to all spanning-tree enabled interfaces but the giaddr field was not set on the packets. This behavior can cause problems in a network because the DHCP server uses the giaddr field to properly allocate addresses when the client is not in the local network.

Use the **ip dhcp relay forward spanning-tree** command to set the giaddr to the IP address of the incoming interface before forwarding DHCP broadcasts to spanning-tree enabled interfaces.

The **ip forward-protocol udp** command is enabled by default and automatically determines that BOOTP client and server datagrams (ports 67 and 68) should be forwarded. This forwarding results in another packet sent to spanning-tree enabled interfaces without the giaddr field set. To avoid these duplicate packets, use the **no ip forward-protocol udp bootpc** and **no ip forward-protocol udp bootps** commands.

Examples

In the following example, the giaddr field in the DHCP packet will be set to the IP address of the incoming interface before forwarding to spanning-tree enabled interfaces:

```
ip dhcp relay forward spanning-tree
ip forward-protocol spanning-tree any-local-broadcast
```

Related Commands

Command	Description
ip forward-protocol	Specifies which protocols and ports the router forwards when forwarding broadcast packets
ip forward-protocol spanning-tree	Permits IP broadcasts to be flooded throughout the internetwork in a controlled fashion.

ip dhcp relay information check

To configure a Dynamic Host Configuration Protocol (DHCP) server to validate the relay agent information option in forwarded BOOTREPLY messages, use the **ip dhcp relay information check** command in global configuration mode. To disable an information check, use the no form of this command.

ip dhcp relay information check
no ip dhcp relay information check

Syntax Description

This command has no arguments or keywords.

Command Default

A DHCP server checks relay information. Invalid messages are dropped.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is used by cable access router termination systems. By default, DHCP checks relay information. Invalid messages are dropped.

Examples

The following example configures the DHCP Server to check that the relay agent information option in forwarded BOOTREPLY messages is valid:

```
ip dhcp relay information check
```

Related Commands

Command	Description
ip dhcp relay information option	Configures a Cisco IOS DHCP Server to insert the DHCP relay agent information option in forwarded BOOTREQUEST messages.
ip dhcp relay information policy	Configures the information reforwarding policy of a DHCP relay agent (what a DHCP relay agent should do if a message already contains relay information).

ip dhcp relay information check-reply

To configure a DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages, use the **ip dhcp relay information check-reply** command in interface or subinterface configuration mode. To disable an information check, use the no form of this command.

ip dhcp relay information check-reply [**none**]
no ip dhcp relay information check-reply [**none**]

Syntax Description

none	(Optional) Disables the command function.

Command Default

A DHCP server checks relay information. Invalid messages are dropped.

Command Modes

Interface configuration Subinterface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

If an **ip dhcp relay information** command is configured in global configuration mode but not configured in interface configuration mode, the global configuration is applied to all interfaces.

If an **ip dhcp relay information** command is configured in both global configuration mode and interface configuration mode, the interface configuration command takes precedence over the global configuration command. However, the global configuration is applied to interfaces without the interface configuration.

If an **ip dhcp relay information** command is not configured in global configuration mode but is configured in interface configuration mode, only the interface with the configuration option applied is affected. All other interfaces are not impacted by the configuration.

The **ip dhcp relay information check-reply none** command option is saved in the running configuration. This command takes precedence over any relay agent information global configuration.

Examples

The following example shows how to configure the DHCP server to check that the relay agent information option in forwarded BOOTREPLY messages received from FastEthernet interface 0 is valid:

```
!
interface FastEthernet 0
 ip dhcp relay information check-reply
```

Related Commands

Command	Description
ip dhcp relay information option-insert	Enables the system to insert a DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.
ip dhcp relay information check	Configures a DHCP server to validate the relay information option in forwarded BOOTREPLY messages in global configuration mode.

Command	Description
ip dhcp relay information policy-action	Configures the information reforwarding policy for a DHCP relay agent.

ip dhcp relay information option

To enable the system to insert a Dynamic Host Configuration Protocol (DHCP) relay agent information option in forwarded BOOTREQUEST messages to a DHCP server, use the **ip dhcp relay information option** command in global configuration mode. To disable inserting relay information into forwarded BOOTREQUEST messages, use the no form of this command.

ip dhcp relay information option [**vpn**]
no ip dhcp relay information option [**vpn**]

Syntax Description

vpn	(Optional) Virtual private network.

Command Default

The DHCP server does not insert relay information.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(4)B	The **vpn** keyword was added.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This functionality enables a DHCP server to identify the user (for example, cable access router) sending a request and initiate appropriate action based on this information. By default, DHCP does not insert relay information.

The **ip dhcp relay information option** command automatically adds the circuit identifier suboption and the remote ID suboption to the DHCP relay agent information option (also called option 82).

The **vpn** optional keyword should be used only when the DHCP server allocates addresses based on VPN identification suboptions.

The **ip dhcp relay information option vpn**command adds the following VPN-related suboptions into the relay agent information option when DHCP broadcasts are forwarded by the relay agent from clients to a DHCP server:

- VPN identifier--Contains the VPN ID if configured or the virtual routing and forwarding (VRF) name if configured on the interface (VPN ID takes precedence over VRF name).
- Subnet selection--Contains the incoming interface subnet address.
- Server identifier override--Contains the incoming interface IP address.

After these suboptions are successfully added, the gateway address is set to the outgoing interface of the router toward the DHCP server IP address that was configured using the **ip helper-address** command.

If only the **ip dhcp relay information option vpn**commandis configured, the VPN identifier, subnet selection, and server identifier override suboptions are added to the relay information option. Note that the circuit identifier suboption and the remote ID suboption are not added to the relay information option. However, if both the **ip dhcp relay information option** command and the **ip dhcp relay information option vpn** command are configured, all five suboptions are added to the relay agent information option.

When the packets are returned from the DHCP server, option 82 is removed before the reply is forwarded to the client.

Even if the **vpn** option is specified, the VPN suboptions are added only to those DHCP or BOOTP broadcasts picked up by the interface that was configured with a VRF name or VPN ID.

For clients from unnumbered ATM or serial interfaces, when this command is enabled, the VPN identifier suboption will contain the VRF name of the unnumbered interface.

Subnet selection and server identifier override suboptions are added from the IP address of the interface from which the unnumbered interface is configured to borrow its IP address. The client host route will be added on the applicable VRF routing tables.

If the **ip dhcp smart-relay** global configuration command is enabled, then the server identifier override and subnet selection suboptions will use the secondary IP address of the incoming interface when the same client retransmits more than three DHCP DISCOVER packets (for both numbered and unnumbered interfaces).

Examples

The following example configures a DHCP server to insert the DHCP relay agent information option, including VPN suboptions, in forwarded BOOTREQUEST messages. In this example, the circuit identifier suboption and the remote ID suboption are not included in the relay information option:

```
ip dhcp relay information option vpn
```

The following example configures a DHCP server to insert the DHCP relay agent information option, including VPN suboptions, the circuit identifier suboption, and the remote ID suboption, in forwarded BOOTREQUEST messages:

```
ip dhcp relay information option vpn
ip dhcp relay information option
```

Cisco 10000 Series Router

The following example enables DHCP option 82 support on the DHCP relay agent by using the **ip dhcp relay information option** command. The **rbe nasip**command configures the router to forward the IP address for Loopback0 to the DHCP server. The value (in hexadecimal) of the agent remote ID suboption is 010100000B0101814058320, and the value of each field is the following:

- Port Type: 0x01
- Version: 0x01
- Reserved: undefined
- NAS IP address: 0x0B010181 (hexadecimal value of 11.1.1.129)
- NAS Port

- Interface (slot/module/port): 0x40 (The slot/module/port values are 01 00/0/000.)
- VPI: 0x58 (hexadecimal value of 88)
- VCI: 0x320 (hexadecimal value of 800)

```
ip dhcp-server 172.16.1.2
!
ip dhcp relay information option
!
interface Loopback0
 ip address 10.1.1.129 255.255.255.192
!
interface ATM4/0
 no ip address
!
interface ATM4/0.1 point-to-point
 ip unnumbered Loopback0
 ip helper-address 172.16.1.2
 atm route-bridged ip
 pvc 88/800
  encapsulation aal5snap
!
interface Ethernet 5/1
 ip address 172.16.1.1 255.255.0.0
!
router eigrp 100
 network 10.0.0.0
 network 172.16.0.0
!
rbe nasip Loopback0
```

In the following example, the DHCP relay receives a DHCP request on Ethernet interface 0/1 and sends the request to the DHCP server located at IP helper address 10.44.23.7, which is associated with the VRF named red.

```
ip dhcp relay information option vpn
!
interface ethernet 0/1
 ip helper-address vrf red 10.44.23.7
```

Related Commands

Command	Description
ip dhcp relay information check	Configures a Cisco IOS DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.
ip dhcp relay information policy	Configures the information reforwarding policy of a DHCP relay agent.
ip dhcp smart-relay	Allows the Cisco IOS DHCP relay agent to switch the gateway address.
ip helper-address	Forwards UDP broadcasts, including BOOTP, received on an interface.

ip dhcp relay information option server-id-override

To enable the system to insert the server ID override and link selection suboptions on a specific interface into the Dynamic Host Configuration Protocol (DHCP) relay agent information option in forwarded BOOTREQUEST messages to a DHCP server, use the **ip dhcp relay information option server-id-override** command in interface configuration mode. To disable inserting the server ID override and link selection suboptions into the DHCP relay agent information option, use the **no** form of this command.

ip dhcp relay information option server-id-override
no ip dhcp relay information option server-id-override

Syntax Description

This command has no arguments or keywords.

Command Default

The server ID override and link selection suboptions are not inserted into the DHCP relay agent information option.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The **ip dhcp relay information option server-id-override** command adds the following suboptions into the relay agent information option when DHCP broadcasts are forwarded by the relay agent from clients to a DHCP server:

- Server ID override suboption
- Link selection suboption

When this command is configured, the gateway address (giaddr) will be set to the IP address of the outgoing interface, which is the interface that is reachable by the DHCP server.

If the **ip dhcp relay information option server-id-override** command is configured on an interface, it overrides the **ip dhcp-relay information option server-override** global configuration on that interface only.

Examples

In the following example, the DHCP relay will insert the server ID override and link selection suboptions into the relay information option on Ethernet interface 0/0:

```
Device(config)# interface Ethernet0/0
Device(config-if)# ip dhcp relay information option server-id-override
```

Related Commands

Command	Description
ip dhcp-relay information option server-override	Enables the system to globally insert the server ID override and link selection suboptions on a specific interface into the DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.

ip dhcp relay information option subscriber-id

To specify that a Dynamic Host Configuration Protocol (DHCP) relay agent add a subscriber identifier suboption to option82, use the **ip dhcp relay information option subscriber-id**command in interface configuration mode. To disable the subscriber identifier, use the no form of this command.

ip dhcp relay information option subscriber-id *string*
no ip dhcp relay information option subscriber-id *string*

Syntax Description

string	Up to a maximum of 50 characters that can be alphanumeric. The string can be ASCII text only. **Note** If more than 50 characters are configured, the string is truncated.

Command Default

Disabled to allow backward capability.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

When the unique subscriber identifier is configured on the relay agent and the interface, the identifier is added to option82 in all of the client DHCP packets to the DHCP server. When the server echoes option82 in the reply packets, the relay agent removes option82 before forwarding the reply packet to the client. When an interface is numbered, all renew packets and release packets are unicast to the server, so option82 is not added.

The unique identifier should be configured for each subscriber and when a subscriber moves from one interface to the other, the configuration of the interface should be changed also.

In case of unnumbered interfaces, all the client packets are sent to the relay. Option82 is added in all the client packets before forwarding the packets to the server. If the server does not echo option82 in the packet, the relay agent tries to validate option82 in the reply packet. If the reply packet does not contain option82, then the validation fails and the packet is dropped by the relay agent. The client cannot get any IP address because of the validation failure. In this case, the existing **no ip dhcp relay information check** command can be used to avoid the option82 invalidation.



Note The configurable string is not an option for network access server (NAS)-IP, because users can move between NAS termination points. When a subscriber moves from one NAS to another, this option does not result in a configuration change on the side of the DHCP server of the ISP.

Examples

The following example shows how to configure an ATM interface for the subscriber identifier suboption.

```
ip dhcp relay information option
!
interface Loopback0
 ip address 10.1.1.129 255.255.255.192
!
interface ATM4/0
 no ip address
!
interface ATM4/0.1 point-to-point
 ip helper-address 10.16.1.2
 ip unnumbered Loopback0
 ip dhcp relay information option subscriber-id newperson123
 atm route-bridged ip
 pvc 88/800
 encapsulation aal5snap
```

Related Commands

Command	Description
ip dhcp relay information check	Configures a Cisco IOS DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.
ip dhcp relay information option	Enables the system to insert the DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.
ip dhcp relay information policy	Configures the information reforwarding policy of a DHCP relay agent (what a DHCP relay agent should do if a message already contains relay information).
ip dhcp smart-relay	Enables the Cisco IOS DHCP relay agent to switch the gateway address (giaddr field of a DHCP packet) to secondary addresses when there is no DHCPOFFER message from a DHCP server
ip helper-address	Forwards UDP broadcasts, including BOOTP, received on an interface.

ip dhcp relay information option vpn-id

To enable the system to insert VPN suboptions into the DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server and set the gateway address to the outgoing interface toward the DHCP server, use the **ip dhcp relay information option vpn-id**command in interface configuration mode. To remove the configuration, use the **no** form of this command.

ip dhcp relay information option vpn-id [**none**]
no ip dhcp relay information option vpn-id

Syntax Description

none	(Optional) Disables the VPN functionality on the interface.

Command Default

The DHCP server does not insert relay information.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

If the **ip dhcp relay information option vpn** global configuration command is configured and the **ip dhcp relay information option vpn-id**interface configuration command is not configured, the global configuration is applied to all interfaces.

If the **ip dhcp relay information option vpn** global configuration command is configured and the **ip dhcp relay information option vpn-id**interface configuration command is also configured, the interface configuration command takes precedence over the global configuration command. However, the global configuration is applied to interfaces without the interface configuration.

If the **ip dhcp relay information option vpn**global configuration command is not configured and the **ip dhcp relay information option vpn-id**interface configuration command is configured, only the interface with the configuration option applied is affected. All other interfaces are not impacted by the configuration.

The **ip dhcp relay information option vpn-id none**option allows you to disable the VPN functionality on the interface. The only time you need to use this option is when the **ip dhcp relay information option vpn** global configuration command is configured and you want to override the global configuration.

The **no ip dhcp relay information option vpn-id** command removes the configuration from the running configuration. In this case, the interface inherits the global configuration, which may or may not be configured to insert VPN suboptions.

Examples

In the following example, the DHCP relay agent receives a DHCP request on Ethernet interface 0/1 and sends the request to the DHCP server located at IP helper address 10.44.23.7, which is associated with the VRF named red. The **ip dhcp relay information option vpn-id** interface configuration command only applies to Ethernet interface 0/1. All other interfaces are not impacted by the configuration:

```
!
interface ethernet 0/1
```

```
ip helper-address vrf red 10.44.23.7
ip dhcp relay information option vpn-id
```

Related Commands

Command	Description
ip dhcp relay information option	Enables the system to insert the DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.

ip dhcp relay information option-insert

To enable the system to insert a DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server, use the **ip dhcp relay information option-insert**command in interface configuration mode or subinterface configuration mode. To disable inserting relay information into forwarded BOOTREQUEST messages, use the no form of this command.

ip dhcp relay information option-insert [**none**]
no ip dhcp relay information option-insert [**none**]

Syntax Description

none	(Optional) Disables the command function.

Command Default

The DHCP server does not insert relay information.

Command Modes

Interface configuration Subinterface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

If an **ip dhcp relay information** command is configured in global configuration mode but not configured in interface configuration mode, the global configuration is applied to all interfaces.

If an **ip dhcp relay information** command is configured in both global configuration mode and interface configuration mode, the interface configuration command takes precedence over the global configuration command. However, the global configuration is applied to interfaces without the interface configuration.

If an **ip dhcp relay information** command is not configured in global configuration mode but is configured in interface configuration mode, only the interface with the configuration option applied is affected. All other interfaces are not impacted by the configuration.

The **ip dhcp relay information option-insert none** command option is saved in the running configuration. This command takes precedence over any relay agent information global configuration.

Examples

The following example shows how to configure the DHCP server to insert the relay agent information option in forwarded BOOTREQUEST messages:

```
!
interface FastEthernet 0
 ip dhcp relay information option-insert
```

Related Commands

Command	Description
ip dhcp relay information check-reply	Configures a DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.
ip dhcp relay information option	Enables the system to insert a DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server in global configuration mode.

Command	Description
ip dhcp relay information policy-action	Configures the information reforwarding policy for a DHCP relay agent.

ip dhcp relay information policy

To configure the information reforwarding policy for a Dynamic Host Configuration Protocol (DHCP) relay agent (what a relay agent should do if a message already contains relay information), use the **ip dhcp relay information policy** command in global configuration mode. To restore the default relay information policy, use the **no** form of this command.

ip dhcp relay information policy {**drop** | **encapsulate** | **keep** | **replace**}
no ip dhcp relay information policy

Syntax Description

drop	Directs the DHCP relay agent to discard messages with existing relay information if the relay information option is already present.
encapsulate	Encapsulates prior relay agent information.
keep	Indicates that existing information is left unchanged on the DHCP relay agent.
replace	Indicates that existing information is overwritten on the DHCP relay agent.

Command Default

The DHCP server replaces existing relay information.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRD	This command was modified. The **encapsulate** keyword was added.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

A DHCP relay agent may receive a message from another DHCP relay agent that already contains relay information. By default, the relay information from the previous relay agent is replaced.

The **ip dhcp relay information policy encapsulate** command option is only needed when the relay agent needs to encapsulate the relay agent information option from a prior relay agent. If this command option is used, the prior option 82 is encapsulated inside the current option 82 and both are forwarded to the DHCP server.

Examples

The following examples show how to configure a DHCP relay agent to drop messages with existing relay information, keep existing information, replace existing information, and encapsulate existing information, respectively:

```
ip dhcp relay information policy drop
ip dhcp relay information policy keep
ip dhcp relay information policy replace
ip dhcp relay information policy encapsulate
```

Related Commands

Command	Description
ip dhcp relay information check	Configures a Cisco IOS DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.
ip dhcp relay information option	Configures a Cisco IOS DHCP server to insert the DHCP relay agent information option in forwarded BOOTREQUEST messages.
ip dhcp relay information policy-action	Configures the information reforwarding policy for a DHCP relay agent in interface configuration mode.

ip dhcp relay information policy-action

To configure the information reforwarding policy for a DHCP relay agent (what a relay agent should do if a message already contains relay information), use the **ip dhcp relay information policy-action** command in interface configuration mode or subinterface configuration mode. To restore the default relay information policy, use the **no** form of this command.

ip dhcp relay information policy-action {**drop** | **encapsulate** | **keep** | **replace**}
no ip dhcp relay information policy-action

Syntax Description

drop	Directs the DHCP relay agent to discard messages with existing relay information if the relay information option is already present.
encapsulate	Encapsulates prior information.
keep	Indicates that existing information is left unchanged on the DHCP relay agent.
replace	Indicates that existing information is overwritten on the DHCP relay agent.

Command Default

The DHCP server replaces existing relay information.

Command Modes

Interface configuration (config-if) Subinterface configuration (config-subif)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SRD	This command was modified. The **encapsulation** keyword was added.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

If an **ip dhcp relay information** command is configured in global configuration mode but not configured in interface configuration mode, the global configuration is applied to all interfaces.

If an **ip dhcp relay information** command is configured in both global configuration mode and interface configuration mode, the interface configuration command takes precedence over the global configuration command. However, the global configuration is applied to interfaces without the interface configuration.

If an **ip dhcp relay information** command is not configured in global configuration mode but is configured in interface configuration mode, only the interface with the configuration option applied is affected. All other interfaces are not impacted by the configuration.

The **ip dhcp relay information policy-action encapsulate** command is only needed when the relay agent needs to encapsulate the relay agent information option from a prior relay agent. If this command option is used, the prior option 82 is encapsulated inside the current option 82 and both are forwarded to the DHCP server.

Examples

The following example shows how to configure a DHCP relay agent to drop messages with existing relay information:

```
Router# configure terminal
Router(config)# interface FastEthernet 0
Router(config-if)# ip dhcp relay information policy-action drop
```

The following example shows how to configure a DHCP relay agent to encapsulate existing relay information:

```
Router# configure terminal
Router(config)# interface Ethernet0/0
Router(config-if)# ip dhcp relay information policy-action encapsulate
```

Related Commands

Command	Description
ip dhcp relay information check-reply	Configures a DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.
ip dhcp relay information option-insert	Enables the system to insert a DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.
ip dhcp relay information policy	Configures the information reforwarding policy for a DHCP relay agent in global configuration mode.

ip dhcp relay information trust-all

To configure all interfaces on a router as trusted sources of the Dynamic Host Configuration Protocol (DHCP) relay agent information option, use the **ip dhcp relay information trust-all** command in global configuration mode. To restore the interfaces to their default behavior, use the **no** form of the command.

ip dhcp relay information trust-all
no ip dhcp relay information trust-all

Syntax Description

This command has no arguments or keywords.

Command Default

All interfaces on the router are considered untrusted.

Command Modes

Global configuration

Command History

Release	Modification
12.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

By default, if the gateway address is set to all zeros in the DHCP packet and the relay information option is already present in the packet, the Cisco IOS DHCP relay agent will discard the packet. If the **ip dhcp relay information trust-all**command is configured globally, the Cisco IOS DHCP relay agent will not discard the packet even if the gateway address is set to all zeros. Instead, the received DHCPDISCOVER or DHCPREQUEST messages will be forwarded to the addresses configured by the **ip helper-address** command as in normal DHCP relay operation.

Examples

In the following example, all interfaces on the router are configured as a trusted source for relay agent information:

```
ip dhcp relay information trust-all
```

Related Commands

Command	Description
ip helper-address	Enables the forwarding of UDP broadcasts, including BOOTP, received on an interface.
show ip dhcp relay information trusted-sources	Displays all interfaces on the router that are configured as a trusted source for the DHCP relay agent information option.

ip dhcp relay information trusted

To configure an interface as a trusted source of the Dynamic Host Configuration Protocol (DHCP) relay agent information option, use the **ip dhcp relay information trusted** command in interface configuration mode. To restore the interface to the default behavior, use the **no** form of the command.

ip dhcp relay information trusted
no ip dhcp relay information trusted

Syntax Description

This command has no arguments or keywords.

Command Default

All interfaces on the router are considered untrusted.

Command Modes

Interface configuration

Command History

Release	Modification
12.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

By default, if the gateway address is set to all zeros in the DHCP packet and the relay information option is already present in the packet, the Cisco IOS DHCP relay agent will discard the packet. If the **ip dhcp relay information trusted**command is configured on an interface, the Cisco IOS DHCP relay agent will not discard the packet even if the gateway address is set to all zeros. Instead, the received DHCPDISCOVER or DHCPREQUEST messages will be forwarded to the addresses configured by the **ip helper-address** command as in normal DHCP relay operation.

Examples

In the following example, interface Ethernet 1 is configured as a trusted source for the relay agent information:

```
interface ethernet 1
 ip dhcp relay information trusted
```

Related Commands

Command	Description
ip helper-address	Enables the forwarding of UDP broadcasts, including BOOTP, received on an interface.
show ip dhcp relay information trusted-sources	Displays all interfaces on the router that are configured as a trusted source for the DHCP relay agent information option.

ip dhcp-relay source-interface

To globally configure the source interface for the relay agent to use as the source IP address for relayed messages, use the **ip dhcp-relay source-interface** command in global configuration mode. To remove the source interface configuration, use the **no** form of this command.

ip dhcp-relay source-interface *type number*
no ip dhcp-relay source-interface *type number*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
number	Interface or subinterface number. For more information about the numbering system for your networking device, use the question mark (?) online help function.

Command Default

The source interface is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The **ip dhcp-relay source-interface** command allows the network administrator to specify a stable, hardware-independent IP address (such as a loopback interface) for the relay agent to use as a source IP address for relayed messages.

If the **ip dhcp-relay source-interface** global configuration command is configured and the **ip dhcp relay source-interface** command is also configured, the **ip dhcp relay source-interface** command takes precedence over the global configuration command. However, the global configuration is applied to interfaces without the interface configuration.

Examples

In the following example, the loopback interface IP address is configured to be the source IP address for the relayed messages:

```
Device(config)# ip dhcp-relay source-interface loopback 0
Device(config)# interface loopback 0
Device(config-if)# ip address 10.2.2.1 255.255.255.0
```

Related Commands

Command	Description
ip dhcp relay source-interface	Configures the source interface for the relay agent to use as the source IP address for relayed messages.

ip dhcp route connected

To specify routes as connected routes, use the **ip dhcp route connected** command in global configuration mode. To return to the default settings, use the **no** form of this command.

ip dhcp route connected
no ip dhcp route connected

Syntax Description

This command has no arguments or keywords.

Command Default

All interfaces on the router are untrusted.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXF	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you enable the **ip dhcp route connected**command, DHCP downloads the route database from a database agent and adds the routes as connected routes, even though they may have been added as static routes previously.

Examples

This example shows how to specify routes as connected routes:

```
Router(config)#
ip dhcp route connected
```

ip dhcp server use subscriber-id client-id

To configure the Dynamic Host Configuration Protocol (DHCP) server to use the subscriber identifier as the client identifier on all incoming DHCP messages on an interface, use the **ip dhcp server use subscriber-id client-id** command in interface configuration mode. To disable this functionality, use the **no** form of this command.

ip dhcp server use subscriber-id client-id
no ip dhcp server use subscriber-id client-id

Syntax Description

This command has no arguments or keywords.

Command Default

DHCP uses the client identifier option in the DHCP packet to identify clients.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(46)SE	This command was introduced.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

This command takes precedence on the interface over the **ip dhcp use subscriber-id client-id** command.

Examples

In the following example, the DHCP server uses the subscriber identifier as the client identifier for all incoming messages received on Ethernet interface 0/0:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# ip dhcp server use subscriber-id client-id
```

Related Commands

Command	Description
ip dhcp use subscriber-id client-id	Configures the DHCP server to globally use the subscriber identifier as the client identifier on all incoming DHCP messages.

ip dhcp smart-relay

To allow the Cisco IOS Dynamic Host Configuration Protocol (DHCP) relay agent to switch the gateway address (giaddr field of a DHCP packet) to secondary addresses when there is no DHCPOFFER message from a DHCP server, use the **ip dhcp smart-relay** command in global configuration mode. To disable this smart-relay functionality and restore the default behavior, use the **no** form of this command.

ip dhcp smart-relay
no ip dhcp smart-relay

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The DHCP relay agent attempts to forward the primary address as the gateway address three times. After three attempts and no response, the relay agent automatically switches to secondary addresses.

Examples

The following example enables the DHCP relay agent to automatically switch to secondary address pools:

```
ip dhcp smart-relay
```

ip dhcp snooping

To globally enable DHCP snooping, use the **ip dhcp snooping**command in global configuration mode. To disable DHCP snooping, use the **no** form of this command.

ip dhcp snooping
no ip dhcp snooping

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.4(3)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

Wireless clients, or mobile nodes, gain access to an untrusted wireless network only if there is a corresponding entry in the DHCP snooping database. Enable DHCP snooping globally by entering the **ip dhcp snooping**command, and enable DHCP snooping on the tunnel interface by entering the **ip dhcp snooping packets** command. After you enable DHCP snooping, the process snoops DHCP packets to and from the mobile nodes and populates the DHCP snooping database.

Examples

This example shows how to enable DHCP snooping:

```
Router(config) # ip dhcp snooping
```

This example shows how to disable DHCP snooping:

```
Router(config) # no ip dhcp snooping
```

Related Commands

Command	Description
ip dhcp snooping packets	Enables DHCP snooping on the tunnel interface.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

ip dhcp snooping binding

To set up and generate a DHCP binding configuration to restore bindings across reboots, use the **ip dhcp snooping binding** command in privileged EXEC mode. To disable the binding configuration, use the **no** form of this command.

ip dhcp snooping binding *mac-address* **vlan** *vlan ip-address* **interface** *type number* **expiry** *seconds*
no ip dhcp snooping binding *mac-address* **vlan** *vlan ip-address* **interface** *type number*

Syntax Description

mac-address	MAC address.
vlan *vlan*	Specifies a valid VLAN number; valid values are from 1 to 4094.
ip-address	IP address.
interface *type*	Specifies the interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet , tengigabitethernet**.
number	Module and port number.
expiry *seconds*	Specifies the interval after which binding is no longer valid; valid values are from 1 to 4294967295 seconds.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When you add or remove a binding using this command, the binding database is marked as changed and a write is initiated.

Examples

This example shows how to generate a DHCP binding configuration on interface gigabitethernet1/1 in VLAN 1 with an expiration time of 1000 seconds:

```
Router# ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface gi1/1 expiry
1000
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

ip dhcp snooping database

To configure the Dynamic Host Configuration Protocol (DHCP)-snooping database, use the **ip dhcp snooping database** command in global configuration mode. To disable the DHCP-snooping database, use the **no** form of this command.

ip dhcp snooping database {**bootflash:** *url* | **ftp:** *url* | **rcp:** *url* | **scp:** *url* | **sup-bootflash:** | **tftp:** *url* | **timeout** *seconds* | **write-delay** *seconds*}
no ip dhcp snooping database {**timeout** *seconds* | **write-delay** *seconds*}

Syntax Description

bootflash: *url*	Specifies the database URL for storing entries using the bootflash.
ftp: *url*	Specifies the database URL for storing entries using FTP.
rcp: *url*	Specifies the database URL for storing entries using remote copy (rcp).
scp: *url*	Specifies the database URL for storing entries using Secure Copy (SCP).
sup-bootflash:	Specifies the database URL for storing entries using the supervisor bootflash.
tftp: *url*	Specifies the database URL for storing entries using TFTP.
timeout *seconds*	Specifies the abort timeout interval; valid values are from 0 to 86400 seconds.
write-delay *seconds*	Specifies the amount of time before writing the DHCP-snooping entries to an external server after a change is seen in the local DHCP-snooping database; valid values are from 15 to 86400 seconds.

Command Default

The DHCP-snooping database is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(18)SXF5	The **sup-bootflash:** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You must enable DHCP snooping on the interface before entering this command. Use the **ip dhcp snooping** command to enable DHCP snooping.

Examples

This example shows how to specify the database URL using TFTP:

```
Router(config)# ip dhcp snooping database tftp://10.90.90.90/snooping-rp2
```

This example shows how to specify the amount of time before writing DHCP snooping entries to an external server:

```
Router(config)# ip dhcp snooping database write-delay 15
```

Related Commands

Command	Description
ip dhcp snooping	Enables DHCP snooping.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

ip dhcp snooping detect spurious

To enable spurious DHCP server detection on a VLAN, use the **ip dhcp snooping detect spurious vlan** command in global configuration mode. To disable spurious DHCP server detection on a VLAN, use the **no** form of this command.

ip dhcp snooping detect spurious vlan *word*
no ip dhcp snooping detect spurious vlan *word*

Syntax Description

word	DHCP snooping VLAN or VLAN range.

Command Default

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SXH6	Support for this command was introduced.

Examples

This example shows how to enable spurious DHCP server detection on a specified VLAN list:

```
Router(config)# ip dhcp snooping detect spurious vlan 3-5
WORD DHCP Snooping vlan list number or vlan range, example: 1,3-5,7,9-11
Router(config)# ip dhcp snooping detect spurious interval ?
<1-65535> Time in minutes
```

Specify the interval between the DHCPDISCOVER messages.

```
Router# show ip dhcp snooping detect spurious ?

entry DHCP snooping detect spurious entry
| Output modifiers
<cr>
```

Provides brief configuration information related to spurious DHCP server detection.

```
Router# show ip dhcp snooping detect spurious entry ?

vlan spurious entry VLAN
| Output modifiers
<cr>
```

Displays all the learnt entries or those from a specific VLAN.

```
Router# clear ip dhcp snooping detect spurious entry ?

vlan Spurious entry VLAN
<cr>
```

Clears either all entries or those from a specific VLAN.

```
Router# show ip dhcp snooping detect spurious
```

```
Spurious DHCP server detection enabled
Detection VLAN list : 13-15,20,30
Detection interval : 10 minutes
Router# sh ip dhcp sn det sp en

Count  MacAddress       IpAddress       VLAN Interface               Last Seen
------ ---------------- --------------- ---- -----------             ------------
1      0004.2322.9dc9   20.0.0.1        20   GigabitEthernet1/25     Sep 21 2009 15:37:50

1      0004.2322.9dc9   10.78.96.194    20   GigabitEthernet1/25     Sep 21 2009 15:37:37

1      0011.955f.067c   30.0.0.1        30   GigabitEthernet1/26     Sep 21 2009 15:37:52
```

Related Commands

Command	Description
clear ip dhcp snooping detect spurious entry	Clears all entries or those from a specific VLAN.
ip dhcp snooping detect spurious interval	Specifies the interval time between DHCPDISCOVER messages.
ip dhcp snooping detect spurious vlan	Enables spurious DHCP server detection on a VLAN.
show ip dhcp snooping detect spurious	Displays the configuration information related to spurious DHCP server detection.
show ip dhcp snooping detect spurious entry	Displays all the learnt entries or those from a specific VLAN.

ip dhcp snooping detect spurious interval

To set the interval time between DHCPDISCOVER messages, use the **ip dhcp snooping detect spurious interval** command in global configuration mode. To reset the time to its default time, use the **no** form of this command.

ip dhcp snooping detect spurious interval *time*
no ip dhcp snooping detect spurious

Syntax Description

time	Time in minutes between DHCPDISCOVER messages; valid values are 1 through 65535.

Command Default

30 minutes is the default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SXH6	Support for this command was introduced.

Examples

This example shows how to set the time interval between DHCPDISCOVER messages to 350 minutes:

```
Router(config)# ip dhcp snooping detect spurious interval 350
Router(config)#
```

Related Commands

Command	Description
clear ip dhcp snooping detect spurious entry	Clears all entries or those from a specific VLAN.
ip dhcp snooping detect spurious vlan	Enables spurious DHCP server detection on a VLAN.
show ip dhcp snooping detect spurious	Displays the configuration information related to spurious DHCP server detection.
show ip dhcp snooping detect spurious entry	Displays all the learnt entries or those from a specific VLAN.

ip dhcp snooping detect spurious vlan

To enable spurious DHCP server detection on a VLAN, use the **ip dhcp snooping detect spurious vlan** command in global configuration mode. To disable spurious DHCP server detection on a VLAN, use the **no** form of this command.

ip dhcp snooping detect spurious vlan *range*
no ip dhcp snooping detect spurious vlan *range*

Syntax Description

range	DHCP snooping VLAN or VLAN range.

Command Default

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SXH6	Support for this command was introduced.

Examples

This example shows how to enable spurious DHCP server detection on a specified VLAN list:

```
Router(config)# ip dhcp snooping detect spurious vlan 3-5
Router(config)#
```

Related Commands

Command	Description
clear ip dhcp snooping detect spurious entry	Clears all entries or those from a specific VLAN.
ip dhcp snooping detect spurious interval	Specifies the interval time between DHCPDISCOVER messages.
show ip dhcp snooping detect spurious	Displays the configuration information related to spurious DHCP server detection.
show ip dhcp snooping detect spurious entry	Displays all the learnt entries or those from a specific VLAN.

ip dhcp snooping glean

To enable DHCP gleaning for a device, use the **ip dhcp snooping glean** command in global configuration mode. To disable DHCP gleaning, use the **no** form of this command.

ip dhcp snooping glean
no ip dhcp snooping glean

Syntax Description

This command has no arguments or keywords.

Command Default

DHCP gleaning is disabled for a device.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.2E	This command was introduced.

Usage Guidelines

DHCP gleaning is a read-only DHCP snooping functionality that allows components to register and glean DHCP version 4 packets. When you enable DHCP gleaning, it does a read-only snooping on all active interfaces on which DHCP snooping is disabled.

To know if DHCP gleaning is enabled on the device, use the **show ip dhcp snooping** command in privileged EXEC mode.

Examples

This example shows how to enable DHCP gleaning on a device and configure an interface as a trusted source for DHCP gleaning:

```
Device> enable
Device# configure terminal
Device(config)# ip dhcp snooping glean
Device(config)# interface gigabitEthernet 1/0/1
Device(config-if)# ip dhcp snooping trust
Device(config-if)# end
```

Related Commands

Command	Description
ip dhcp snooping	Enables DHCP snooping on a device.
show ip dhcp snooping	Displays DHCP snooping configuration information.

ip dhcp snooping information option

To enable Dynamic Host Configuration Protocol (DHCP) option 82 data insertion, use the **ip dhcp snooping information option** command in global configuration mode. To disable DHCP option 82 data insertion, use the **no** form of this command.

ip dhcp snooping information option [**allow-untrusted**]
no ip dhcp snooping information option

Syntax Description

allow-untrusted	(Optional) Enables the switch to accept incoming DHCP snooping packets with option 82 information from the edge switch.

Command Default

DHCP option 82 data insertion is enabled by default. Accepting incoming DHCP snooping packets with option 82 information from the edge switch is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(18)SXF2	The **allow-untrusted** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

DHCP option 82 is part of RFC 3046. DHCP is an application-layer protocol that is used for the dynamic configuration of TCP/IP networks. The protocol allows for a relay agent to pass DHCP messages between the DHCP clients and DHCP servers. By using a relay agent, servers need not be on the same network as the clients. Option 82 (82 is the option's code) addresses the security and scalability issues. Option 82 resides in the relay agent when DHCP packets that originate from the forwarding client are sent to the server. Servers that recognize Option 82 may use the information to implement the IP address or other parameter assignment policies. The DHCP server echoes the option back to the relay agent in its replies. The relay agent strips out the option from the relay agent before forwarding the reply to the client.

When you enter the **ip dhcp snooping information option allow-untrusted** on an aggregation switch that is connected to an edge switch through an untrusted interface, the aggregation switch accepts packets with option 82 information from the edge switch. The aggregation switch learns the bindings for hosts connected through an untrusted switch interface. You can enable the DHCP security features, such as dynamic Address Resolution Protocol (ARP) inspection or IP source guard, on the aggregation switch while the switch receives packets with option 82 information on untrusted input interfaces to which hosts are connected. You must configure the port on the edge switch that connects to the aggregation switch as a trusted interface.



Caution Do not enter the **ip dhcp snooping information option allow-untrusted** command on an aggregation switch that is connected to an untrusted device. If you enter this command, an untrusted device might spoof the option 82 information.

Examples

This example shows how to enable DHCP option 82 data insertion:

```
ip dhcp snooping information option
```

This example shows how to disable DHCP option 82 data insertion:

```
no ip dhcp snooping information option
```

This example shows how to enable the switch to accept incoming DHCP snooping packets with option 82 information from the edge switch:

```
ip dhcp snooping information option allow-trusted
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

ip dhcp snooping limit rate

To configure the number of the DHCP messages that an interface can receive per second, use the **ip dhcp snooping limit rate** command in interface configuration or template configuration mode. To remove the DHCP message rate limit, use the **no** form of this command.

ip dhcp snooping limit rate *rate*
no ip dhcp snooping limit rate

Syntax Description

rate	Number of DHCP messages that a device can receive per second; valid values are from 1 to 4294967294 seconds. When configuring using interface templates in template configuration mode, the range is from 1 to 2048 seconds.

Command Default

The DHCP snooping limit rate is not configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.2(2)E	This command was integrated into Cisco IOS Release 15.2(2)E. This command is supported in template configuration mode.
Cisco IOS XE Release 3.6E	This command was integrated into Cisco IOS XE Release 3.6E. This command is supported in template configuration mode.
15.4(3)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

This command is supported on Layer 2 switch-port and port-channel interfaces only.

Typically, the rate limit applies to the untrusted interfaces. If you want to set up rate limiting for the trusted interfaces, note that the trusted interfaces aggregate all DHCP traffic in the switch, and you will need to adjust the rate limit of the interfaces to a higher value.

Examples

This example shows how to specify the number of DHCP messages that a device can receive per second:

```
Device(config-if)# ip dhcp snooping limit rate 150
```

This example shows how to disable the DHCP message rate limiting:

```
Device(config-if)# no ip dhcp snooping limit rate
```

The following example shows how to specify the number of DHCP messages that a device can receive per second using an interface template:

```
Device# configure terminal
Device(config)# template user-template1
Device(config-template)# ip dhcp snooping limit rate 150
Device(config-template)# end
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

ip dhcp snooping packets

To enable DHCP snooping on the tunnel interface, use the **ip dhcp snooping packets**command in interface configuration mode. To disable DHCP snooping, use the **no** form of this command.

ip dhcp snooping packets
no ip dhcp snooping packets

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on Layer 2 switch-port and port-channel interfaces only.

This command is supported on Cisco 7600 series routers that are configured with a WLSM only.

Wireless clients, or mobile nodes, gain access to an untrusted wireless network only if there is a corresponding entry in the DHCP snooping database. Enable DHCP snooping globally by entering the **ip dhcp snooping** command, and enable DHCP snooping on the tunnel interface by entering the **ip dhcp snooping packets**command. After you enable DHCP snooping, the process snoops DHCP packets to and from the mobile nodes and populates the DHCP snooping database.

Examples

This example shows how to enable DHCP snooping:

```
Router(config-if)# ip dhcp snooping packets
```

This example shows how to disable DHCP snooping:

```
Router(config-if)# no ip dhcp snooping packets
```

Related Commands

Command	Description
ip dhcp snooping	Enables DHCP snooping.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

ip dhcp snooping verify mac-address

To verify that the source MAC address in a DHCP packet matches the client hardware address on an untrusted port, use the **ip dhcp snooping verify mac-address** command in global configuration mode. To disable verification, use the **no** form of this command.

ip dhcp snooping verify mac-address
no ip dhcp snooping verify mac-address

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

For untrusted DHCP snooping ports, DHCP snooping verifies the MAC address on the client hardware address field to ensure that a client is requesting multiple addresses from a single MAC address. You can use the **ip dhcp snooping verify mac-address** command to trust the ports or you can use the **no ip dhcp snooping verify mac-address** command to leave the ports untrusted by disabling the MAC address verification on the client hardware address field.

Examples

This example shows how to verify that the source MAC address in a DHCP packet matches the client hardware address on an untrusted port:

```
Router(config)# ip dhcp snooping verify mac-address
```

This example shows how to turn off the verification of the MAC address on the client hardware address field:

```
Router(config)# no ip dhcp snooping verify mac-address
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

ip dhcp snooping vlan

To enable DHCP snooping on a VLAN or a group of VLANs, use the **ip dhcp snooping vlan** command in global configuration mode. To disable DHCP snooping on a VLAN or a group of VLANs, use the **no** form of this command.

ip dhcp snooping vlan {*numbervlan-list*}
no ip dhcp snooping vlan {*numbervlan-list*}

Syntax Description

number | *vlan-list*	VLAN number or a group of VLANs; valid values are from 1 to 4094. See the "Usage Guidelines" section for additional information.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

DHCP snooping is enabled on a VLAN only if both the global snooping and the VLAN snooping are enabled.

Enter the range of VLANs using this format: 1,3-5,7,9-11.

Examples

This example shows how to enable DHCP snooping on a VLAN:

```
Router(config)# ip dhcp snooping vlan 10
```

This example shows how to disable DHCP snooping on a VLAN:

```
Router(config)# no ip dhcp snooping vlan 10
```

This example shows how to enable DHCP snooping on a group of VLANs:

```
Router(config)# ip dhcp snooping vlan 10,4-8,55
```

This example shows how to disable DHCP snooping on a group of VLANs:

```
Router(config)# no ip dhcp snooping vlan 10,4-8,55
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

ip dhcp subscriber-id interface-name

To automatically generate a subscriber identifier (ID) value based on the short name of the interface, use the **ip dhcp subscriber-id interface-name** command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip dhcp subscriber-id interface-name
no ip dhcp subscriber-id interface-name

Syntax Description

This command has no arguments or keywords.

Command Default

A subscriber ID is not automatically generated.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(46)SE	This command was introduced.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

A subscriber ID configured on a specific interface using the **ip dhcp server use subscriber-id client-id**command takes precedence over the global configuration.

Examples

In the following example, a subscriber ID will be automatically generated based on the short name of the interface (port) specified by the **address client-id** command. The DHCP server will ignore any client identifier fields in the DHCP messages and use this subscriber ID as the client identifier. The DHCP client is preassigned IP address 10.1.1.7.

```
Router(config)# ip dhcp use subscriber-id client-id
Router(config)# ip dhcp subscriber-id interface-name
Router(config)# ip dhcp excluded-address 10.1.1.1 10.1.1.3
Router(config)# ip dhcp pool dhcppool
Router(dhcp-config)# network 10.1.1.0 255.255.255.0
Router(dhcp-config)# address 10.1.1.7 client-id ethernet 1/0 ascii
```

Related Commands

Command	Description
ip dhcp server use subscriber-id client-id	Configures the DHCP server to use the subscriber identifier as the client identifier on all incoming DHCP messages on an interface.

ip dhcp support option55-override

To enable a DHCP server to override multiple option 55 (parameter request list) requests sent by a DHCP client and send a DHCPOFFER message with all the sub-options set in the option 55, use the **ip dhcp support option55-override** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ip dhcp support option55-override
no ip dhcp support option55-override

Syntax Description

This command has no arguments or keywords.

Command Default

A DHCP server accepts the first instance of the option 55 request and ignores the remaining instances. Therefore, the server sends a DHCPOFFER message, which may not contain all the information required by the DHCP client

Command Modes

Global configuration (config)

Command History

Release	Modification
15.3(2)T	This command was introduced.

Examples

The following example shows how to enable a DHCP server to override multiple option 55 requests:

```
Device> enable
Device# configure terminal
Device(config)# ip dhcp support option55-override
```

Related Commands

Command	Description
ip address dhcp	Acquires an interface IP address from the DHCP.
ip dhcp client request	Configures a DHCP client to request an option from a DHCP server.

ip dhcp support tunnel unicast

To configure a spoke-to-hub tunnel to unicast DHCP replies over a Dynamic Multipoint VPN (DMVPN) network, use the **ip dhcp support tunnel unicast** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ip dhcp support tunnel unicast
no ip dhcp support tunnel unicast

Syntax Description

This command has no arguments or keywords.

Command Default

A spoke-to-hub tunnel broadcasts the replies over the DMVPN network.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

By default, the DHCP replies are broadcast from the DMVPN hub to the spoke. The DHCP relay agent must unicast the DHCP messages for a DHCP server to be functional in the DMVPN environment. Hence for the DHCP to be functional in DMVPN environment, you must configure the DHCP relay agent to unicast the DHCP messages.

Use the **ip dhcp support tunnel unicast** command to configure the DHCP relay agent to unicast the DHCP protocol messages from the server (hub) to the client (spoke). The relay agent uses the nonbroadcast multiaccess (NBMA) address to create temporary routes in Next Hop Resolution Protocol (NHRP) to help unicast the DHCPOFFER and DHCPACK messages to the spoke.

Examples

The following example shows how to configure a spoke-to-hub tunnel to unicast the replies over a DMVPN network:

```
Router(config)# ip dhcp support tunnel unicast
```

Related Commands

Command	Description
ip address dhcp	Configures an IP address on an interface acquired through DHCP.
ip dhcp client broadcast-flag	Configures the DHCP client to set or clear the broadcast flag.

ip dhcp update dns

To enable Dynamic Domain Name System (DDNS) updates of address (A) and pointer (PTR) Resource Records (RRs) for most address pools, use the **ip dhcp update dns** command in global configuration mode. To disable dynamic updates, use the **no** form of this command.

ip dhcp update dns [**both**] [**override**] [**before**]
no ip dhcp update dns [**both**] [**override**] [**before**]

Syntax Description

both	(Optional) Enables the Dynamic Host Control Protocol (DHCP) server to perform DDNS updates on both A and PTR RRs unless the DHCP client has specified that the server not perform the updates in the fully qualified domain name (FQDN) option.
override	(Optional) Enables the DHCP server to override the DHCP client specification not to perform DDNS updates for both the A and PTR RRs.
before	(Optional) Enables the DHCP server to perform DDNS updates before sending the DHCP ACK back to the DHCP client.

Command Default

Perform DDNS updates after sending a DHCP ACK.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)YA	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Usage Guidelines

Some address pools are configured using the **update dns** command, and that configuration overrides the global configuration. See the **update dns** command for more information.

If you specify the **both** and **override** keywords, the DHCP server will perform the updates for both A and PTR RRs overriding anything that the DHCP client has specified in the FQDN option.

Examples

The following example shows how to configure the DHCP server to perform A and PTR RR updates and to override the DHCP client FQDN option:

```
ip dhcp update dns both override
```

Related Commands

Command	Description
update dns	Dynamically updates a DNS with A and PTR RRs for some address pools.

ip dhcp use

To control what information the Dynamic Host Configuration Protocol (DHCP) server accepts or rejects during address allocation, use the **ip dhcp use**command in global configuration mode. To disable the use of these parameters during address allocation, use the **no** form of this command.

ip dhcp use {**class** [**aaa**] | **vrf** {**connected** | **remote**}}
no ip dhcp use {**class** [**aaa**] | **vrf** {**connected** | **remote**}}

Syntax Description

class	Specifies that the DHCP server use DHCP classes during address allocation.
aaa	(Optional) Specifies to use the authentication, authorization, and accounting (AAA) server to get class name.
vrf	Specifies whether the DHCP server ignores or uses the receiving VPN routing and forwarding (VRF) interface during address allocation.
connected	Specifies that the server should use the VRF information from the receiving interface when servicing a directly connected client.
remote	Specifies that the server should use the VRF information from the receiving interface when servicing a request forwarded by a relay agent.

Command Default

The DHCP server allocates addresses by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

When the Cisco IOS DHCP server code is allocating addresses, you can use the **ip dhcp use**command to either enable or disable the use of VRF configured on the interface, or to configure DHCP classes. If you use the **no ip dhcp use class**command, the DHCP class configuration is not deleted.

Examples

The following example shows how to configure the DHCP server to use the relay agent information option during address allocation:

```
Router(config)# ip dhcp use class
```

The following example shows how to configure the DHCP server to disable the use of the VRF information option during address allocation:

```
Router(config)# no ip dhcp use vrf connected
```

Related Commands

Command	Description
ip dhcp class	Defines a DHCP class and enters DHCP class configuration mode.

ip dhcp use subscriber-id client-id

To configure the Dynamic Host Configuration Protocol (DHCP) server to globally use the subscriber identifier as the client identifier on all incoming DHCP messages, use the **ip dhcp use subscriber-id client-id** command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip dhcp use subscriber-id client-id
no ip dhcp use subscriber-id client-id

Syntax Description

This command has no arguments or keywords.

Command Default

DHCP uses the client identifier option in the DHCP packet to identify clients.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(46)SE	This command was introduced.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

A subscriber ID value configured on a specific interface using the **ip dhcp server use subscriber-id client-id** command takes precedence over this command.

Examples

In the following example, a subscriber ID will be automatically generated based on the short name of the interface (port) specified by the **address client-id** command. The DHCP server will ignore any client identifier fields in the DHCP messages and use this subscriber ID as the client identifier. The DHCP client is preassigned IP address 10.1.1.7.

```
Router(config)# ip dhcp use subscriber-id client-id
Router(config)# ip dhcp subscriber-id interface-name
Router(config)# ip dhcp excluded-address 10.1.1.1 10.1.1.3
Router(config)# ip dhcp pool dhcppool
Router(dhcp-config)# network 10.1.1.0 255.255.255.0
Router(dhcp-config)# address 10.1.1.7 client-id ethernet 1/0 ascii
```

Related Commands

Command	Description
ip dhcp server use subscriber-id client id	Configures the DHCP server to use the subscriber identifier as the client identifier on all incoming DHCP messages on an interface.

ip dhcp-client broadcast-flag

To configure the Dynamic Host Configuration (DHCP) client to set the broadcast flag, use the **ip dhcp-client broadcast-flag** command in global configuration mode. To disable this feature, use the **no** form of this command.

ip dhcp-client broadcast-flag
no dhcp-client broadcast-flag

Syntax Description

This command has no arguments or keywords.

Command Default

The broadcast flag is on.

Command Modes

Global configuration

Command History

Release	Modification
12.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to set the broadcast flag to 1 or 0 in the DHCP packet header when the DHCP client sends a discover requesting an IP address. The DHCP server listens to this broadcast flag and broadcasts the reply packet if the flag is set to 1.

If the **no ip dhcp-client broadcast-flag** command is entered, the broadcast flag is set to 0 and the DHCP server unicasts the reply packets to the client with the offered IP address.

The DHCP client can receive both broadcast and unicast offers from the DHCP server.

Examples

The following example sets the broadcast flag on:

```
ip dhcp-client broadcast-flag
```

Related Commands

Command	Description
ip address dhcp	Acquires an IP address on an interface via DHCP.
service dhcp	Enables DHCP server and relay functions.

ip dhcp-client default-router distance

To configure a default Dynamic Host Configuration Protocol (DHCP) administrative distance for clients, use the **ip dhcp-client default-router distance**command in global configuration mode. To return to the default, use the **no** form of this command.

ip dhcp-client default-router distance *value*
no ip dhcp-client default-router distance *value*

Syntax Description

distance	DHCP administrative distance. The *value* argument sets the default distance. The range is from 1 to 255.

Command Default

254

Command Modes

Global configuration

Command History

Release	Modification
12.2	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to configure the default admininstrative distance to 25:

```
ip dhcp-client default-router distance 25
```

Related Commands

Command	Description
debug dhcp client	Displays debugging information about the DHCP client activities and monitors the status of DHCP packets.
show ip route dhcp	Displays the routes added to the routing table by the DHCP server and relay agent.

ip dhcp-client forcerenew

To enable forcerenew-message handling on the DHCP client when authentication is enabled, use the **ip dhcp-client forcerenew** command in global configuration mode. To disable the forced authentication, use the **no** form of this command.

ip dhcp-client forcerenew
no ip dhcp-client forcerenew

Syntax Description

This command has no arguments or keywords.

Command Default

Forcerenew messages are dropped.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

DHCP forcerenew handling is not enabled until the CLI is configured.

Examples

The following example shows how to enable DHCP forcerenew-message handling on the DHCP client:

```
Router(config)# ip dhcp-client forcerenew
```

Related Commands

Command	Description
ip dhcp client authentication key-chain	Specifies the key chain to be used in DHCP authentication requests.
ip dhcp client authentication mode	Specifies the type of authentication to be used in DHCP messages on the interface.
key chain	Identifies a group of authentication keys for routing protocols.



ip dhcp-client network-discovery through ip nat sip-sbc

- ip dhcp-client network-discovery, on page 311
- ip dhcp-client update dns, on page 313
- ip dhcp drop-inform, on page 315
- ip dhcp-relay information option server-override, on page 316
- ip dhcp-relay source-interface, on page 318
- ip dhcp-server, on page 319
- ip dhcp-server query lease, on page 321
- ip dns name-list, on page 322
- ip dns primary, on page 324
- ip dns server, on page 326
- ip dns server queue limit, on page 327
- ip dns server view-group, on page 328
- ip dns spoofing, on page 330
- ip dns view, on page 331
- ip dns view-group, on page 335
- ip dns view-list, on page 337
- ip domain list, on page 340
- ip domain lookup, on page 342
- ip domain multicast, on page 344
- ip domain name, on page 345
- ip domain recursive, on page 347
- ip domain retry, on page 348
- ip domain round-robin, on page 349
- ip domain timeout, on page 350
- ip gratuitous-arps, on page 351
- ip host, on page 352
- ip host-list, on page 357
- ip hostname strict, on page 358
- ip local-proxy-arp, on page 360
- ip mobile arp, on page 361
- ip name-server, on page 363

- ip nat, on page 365
- ip nat create flow-entries, on page 367
- ip nat enable, on page 369
- ip nat inside destination, on page 370
- ip nat inside source, on page 372
- ip nat log translations flow-export, on page 378
- ip nat log translations syslog, on page 380
- ip nat outside source, on page 381
- ip nat piggyback-support, on page 385
- ip nat pool, on page 386
- ip nat service, on page 389
- ip nat service dns-reset-ttl, on page 394
- ip nat service enable-sym-port, on page 396
- ip nat service gatekeeper, on page 398
- ip nat service ipsec-esp enable, on page 399
- ip nat service pptp, on page 400
- ip nat settings gatekeeper-size, on page 401
- ip nat settings mode, on page 402
- ip nat settings pap, on page 403
- ip nat settings pool watermark, on page 406
- ip nat settings redundancy optimized-data-sync, on page 407
- ip nat settings scale bind, on page 409
- ip nat settings support mapping outside, on page 410
- ip nat sip-sbc, on page 411

ip dhcp-client network-discovery

To control the sending of Dynamic Host Configuration Protocol (DHCP) Inform and Discover messages, use the **ip dhcp-client network-discovery**command in global configuration mode. To change or disable DHCP message control, use the **no** form of this command.

ip dhcp-client network-discovery informs *number-of-messages* **discovers** *number-of-messages* **period** *seconds*
no ip dhcp-client network-discovery informs *number-of-messages* **discovers** *number-of-messages* **period** *seconds*

Syntax Description

informs *number-of-messages*	Number of DHCP Inform messages. Valid choices are 0, 1, or 2 messages. Default is 0 messages.
discovers *number-of-messages*	Number of DHCP Discover messages. Valid choices are 0, 1, or 2 messages. Default is 0 messages.
period *seconds*	Timeout period for retransmission of DHCP Inform and Discover messages. Valid periods are from 3 to 15 seconds. Default is 15 seconds.

Command Default

0 DHCP Inform and Discover messages (network discovery is disabled when both the **informs** and **discovers**keywords are set to 0); 15-second timeout period.

Command Modes

Global configuration

Command History

Release	Modification
12.2	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **ip dhcp-client network-discovery**command allows peer routers to dynamically discover Domain Name System (DNS) and NetBIOS name server information configured on a DHCP server using PPP IP Control Protocol (IPCP) extensions. Setting the number of DHCP Inform or Discover messages to 1 or 2 determines how many times the system sends a DHCP Inform or Discover message before stopping network discovery, as follows:

- When the number of DHCP Inform messages is set to 1, once the first Inform messages is sent the system waits for a response from the DHCP server for the specified timeout period. If there is no response from the DHCP server by the end of the timeout period, the system sends a DHCP Discover message when the number of Discover messages is not set to 0. If the number of Discover messages is set to 1, network discovery stops. If the number of Discover messages is set to 2, the system waits again for a response from the DHCP server for the specified timeout period. If there is no response from the DHCP server by the end of this second timeout period, the system sends a second DHCP Discover message and stops network discovery.

- When the number of DHCP Inform messages is set to 2, once the first Inform messages is sent, the system waits for a response from the DHCP server for the specified timeout period. If there is no response from the DHCP server by the end of the timeout period, the system sends another DHCP Inform message. If the number of Discover messages is set to 1, network discovery stops. If the number of Discover messages is set to 2, the system waits again for a response from the DHCP server for the specified timeout period. If there is no response from the DHCP server by the end of this second timeout period, the system sends a second DHCP Discover message and stops network discovery.

Network discovery also stops when the DHCP server responds to DHCP Inform and Discover messages before the configured number of messages and timeout period are exceeded.

Setting the number of messages to 0 disables sending of DHCP Inform and Discover messages, and is the same as entering the **no ip dhcp-client network-discovery** command. When the **ip dhcp-client network-discovery**command is disabled, the system falls back to the static configurations made using the **async-bootp dns-server** and **async-bootp nb-server** global configuration commands or, as a last resort, to a DNS server address assigned with the **ip name-server** command.

Examples

The following example sets two DHCP Inform and Discovery messages and a timeout period of 12 seconds:

```
ip dhcp-client network-discovery informs 2 discovers 2 period 12
```

Related Commands

Command	Description
async-bootp	Configures extended BOOTP requests for asynchronous interfaces as defined in RFC 1084.
ip dhcp-server	Specifies which DHCP servers to use on a network, and specifies the IP address of one or more DHCP servers available on the network.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.

ip dhcp-client update dns

To enable Dynamic Domain Name System (DDNS) updates of address (A) Resource Records (RRs) using the same hostname passed in the hostname and fully qualified domain name (FQDN) options by a client, use the **ip dhcp-client update dns** command in global configuration mode. To disable dynamic updates, use the **no** form of this command.

ip dhcp-client update dns [**server** {**both** | **none**}]
no ip dhcp client update dns

Syntax Description

server	(Optional) Enables the Dynamic Host Control Protocol (DHCP) server to perform DDNS updates of forward or A RRs in the primary DNS server, unless the DHCP server reports in the ACK FQDN option that it has overridden the client request and updated this information previously. The keywords are as follows: • **both** --Enables the DHCP server to perform DDNS updates on both A (forward) and PTR (reverse) RRs in the primary DNS server unless the DHCP server has specified in the DHCP ACK FQDN option that it has overridden the client request and has updated the information previously. **Note** If the **both** keyword is specified, it means that the client will include an FQDN option specifying the S flag. This instructs the server that it should attempt to dynamically update both the A and PTR RRs. • **none** --On the client side, specifies that the DHCP client should include the FQDN option, however, it should not attempt any DDNS updates. On the server side, specifies that the client will include an FQDN option specifying the "N" flag. The server will not perform any DDNS updates for the client. The server can, of course, override this and do the updates anyway. **Note** If the **none** keyword is not specified, the FQDN option will result in the server updating the PTR RR and neither the server nor the client will update the A RR.

Command Default

No default behavior.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)YA	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Usage Guidelines

Commands that are configured in interface configuration mode override the commands configured using global configuration mode. The **ip dhcp client update dns** command (no hyphen) is the interface configuration command.

If you specify the **both** and **none** keywords, the DHCP client will update both the A and PTR RRs, and the DHCP server will not perform any updates. The DHCP server can override the DHCP client using the **ip dhcp update dns override** command.

If you specify the **none** and **both** keywords (in this order), the DHCP client will not perform any updates and the server will update both the A and PTR RRs.

There are two parts to the DDNS update configuration on the client side. First, if the **ip ddns update method** command is configured on the client, which specifies the DDNS-style updates, then the client will be trying to generate or perform A updates. If the **ip ddns update method ddns both** command is configured, then the client will be trying to update both A and PTR RRs.

Second, the only way for the client to communicate with the server, with reference what updates it is generating or expecting the server to generate, is to include an FQDN option when communicating with the server. Whether or not this option is included is controlled on the client side by the **ip dhcp-client update dns** command in global configuration mode or the **ip dhcp client update dns** command in interface configuration mode.

If the FQDN option is included in the DHCP interaction, then the client may instruct the server to update "reverse" (the default), "both", or "none." Obviously, if the **ip ddns update method** command is configured with the **ddns both** keyword combination, then the FQDN option configuration should reflect an IP DHCP client update DNS server none, but you have to configure the system correctly.

Even if the client instructs the server to update both or update none, the server can override the client request and do whatever it was configured to do anyway. If there is an FQDN option in the DHCP interaction as above, then the server can communicate to the client that it was overridden, in which case the client will not perform the updates because it knows that the server has done the updates. Even if the server is configured to perform the updates after sending the ACK (the default), it can still use the FQDN option to instruct the client what updates it will be performing and thus the client will not do the same types of updates.

If the server is configured with the update dns command with or without any keywords, and if the server does not see an FQDN option in the DHCP interaction, then it will assume that the client does not understand DDNS and will automatically act as though it were configured to update both A and PTR RRs on behalf of the client.

Examples

The following example shows how to configure the DHCP server to perform A and PTR RR updates:

```
ip dhcp-client update dns server both
```

Related Commands

Command	Description
ip ddns update method	Specifies a method of DDNS updates of A and PTR RRs and the maximum interval between the updates.

ip dhcp drop-inform

To drop DHCPINFORM messages, use the **ip dhcp drop-inform** command in global configuration mode. To send DHCPINFORM messages, use the **no** form of this command.

ip dhcp drop-inform
no ip dhcp drop-inform

Syntax Description

This command has no arguments or keywords.

Command Default

DHCPINFORM messages are not dropped.

Command Modes

Global configuration

Command History

Release	Modification
15.5(2)S	This command was introduced.

Usage Guidelines

This command implements DHCPINFORM as per the specifications given in RFC 2131.

If a client has obtained a network address through some other means (e.g., manual configuration), it may use a DHCPINFORM request message to obtain specific configuration parameters from the server.

Examples

The command in the following example drops DHCPINFORM messages:

```
Router(config)# ip dhcp drop-inform
```

ip dhcp-relay information option server-override

To enable the system to globally insert the server ID override and link selection suboptions into the DHCP relay agent information option in forwarded BOOTREQUEST messages to a Dynamic Host Configuration Protocol (DHCP) server, use the **ip dhcp-relay information option server-override** command in global configuration mode. To disable inserting the server ID override and link selection suboptions into the DHCP relay agent information option, use the **no** form of this command.

ip dhcp-relay information option server-override
no ip dhcp-relay information option server-override

Syntax Description

This command has no arguments or keywords.

Command Default

The server ID override and link selection suboptions are not inserted into the DHCP relay agent information option.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The **ip dhcp-relay information option server-override** command adds the following suboptions into the relay agent information option when DHCP broadcasts are forwarded by the relay agent from clients to a DHCP server:

- Server ID override suboption
- Link selection suboption

When this command is configured, the gateway address (giaddr) will be set to the IP address of the outgoing interface, which is the interface that is reachable by the DHCP server.

If the **ip dhcp relay information option server-id-override** command is configured on an interface, it overrides the global configuration on that interface only.

Examples

In the following example, the DHCP relay will insert the server ID override and link selection suboptions into the relay information option of the DHCP packet. The loopback interface IP address is configured to be the source IP address for the relayed messages.

```
Device(config)# ip dhcp-relay information option server-override
Device(config)# ip dhcp-relay source-interface loopback 0
Device(config)# interface Loopback 0
Device(config-if)# ip address 10.2.2.1 255.255.255.0
```

Related Commands

Command	Description
ip dhcp relay information option server-id-override	Enables the system to insert the server ID override and link selection suboptions on a specific interface into the DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.

ip dhcp-relay source-interface

To globally configure the source interface for the relay agent to use as the source IP address for relayed messages, use the **ip dhcp-relay source-interface** command in global configuration mode. To remove the source interface configuration, use the **no** form of this command.

ip dhcp-relay source-interface *type number*
no ip dhcp-relay source-interface *type number*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
number	Interface or subinterface number. For more information about the numbering system for your networking device, use the question mark (?) online help function.

Command Default

The source interface is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The **ip dhcp-relay source-interface** command allows the network administrator to specify a stable, hardware-independent IP address (such as a loopback interface) for the relay agent to use as a source IP address for relayed messages.

If the **ip dhcp-relay source-interface** global configuration command is configured and the **ip dhcp relay source-interface** command is also configured, the **ip dhcp relay source-interface** command takes precedence over the global configuration command. However, the global configuration is applied to interfaces without the interface configuration.

Examples

In the following example, the loopback interface IP address is configured to be the source IP address for the relayed messages:

```
Device(config)# ip dhcp-relay source-interface loopback 0
Device(config)# interface loopback 0
Device(config-if)# ip address 10.2.2.1 255.255.255.0
```

Related Commands

Command	Description
ip dhcp relay source-interface	Configures the source interface for the relay agent to use as the source IP address for relayed messages.

ip dhcp-server

To use specific Dynamic Host Configuration Protocol (DHCP) servers on your network for address allocation, use the **ip dhcp-server** command in global configuration mode. To remove specific DHCP servers from being used on your network, use the **no** form of this command.

ip dhcp-server [**vrf** *vrf-name*] {*server-ip-address* | *server-name*}
no ip dhcp-server [**vrf** *vrf-name*] {*server-ip-address* | *server-name*}

Syntax Description

vrf *vrf-name*	(Optional) The *vrf-name* argument specifies the virtual routing and forwarding (VRF) instance with which the DHCP server is associated. A VRF must be specified only if the DHCP server interface is associated with a VRF. The **ip dhcp-server vrf** command form can be used only when the device is used as an Intelligent Services Gateway (ISG) for sending lease queries. For basic DHCP client configuration (enabled using the command **ip address dhcp**), the **vrf** keyword is not needed.
server-ip-address	IP address of the DHCP server.
server-name	Name of the DHCP server.

Command Default

The IP limited broadcast address of 255.255.255.255 is used for transactions if no DHCP server is specified. This default setting allows automatic detection of DHCP servers.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.13	This command was integrated into Cisco IOS XE Release 3.13. The **vrf** *vrf-name* keyword-argument pair was added.

Usage Guidelines

A DHCP server temporarily allocates network addresses to clients through the access server on an as-needed basis. While the client is active, the address is automatically renewed in a minimum of 20-minute increments. When the user terminates the session, the interface connection is terminated so that network resources can be quickly reused. You can specify up to ten servers on the network.

In normal situations, if a SLIP or PPP session fails (for example, if a modem line disconnects), the allocated address will be reserved temporarily to preserve the same IP address for the client when dialed back into the server. This way, the session that was accidentally terminated can often be resumed.

To use the DHCP proxy-client feature, enable your access server to be a proxy-client on asynchronous interfaces by using the **ip address-pool dhcp-proxy-client** command. If you want to use specific DHCP servers on your network, use the **ip dhcp-server** command to define up to ten specific DHCP servers.



Note To facilitate transmission, configure intermediary devices (or access servers with router functionality) to use an IP helper address whenever the DHCP server is not on the local LAN and the access server is using broadcasts to interact with the DHCP server.

The **ip address-pool dhcp-proxy-client** command initializes proxy-client status to all interfaces defined as asynchronous on the access server. To selectively disable proxy-client status on a single asynchronous interface, use the **no peer default ip address** interface command.

Examples

The following command specifies a DHCP server with the IP address of 172.24.13.81:

```
ip dhcp-server 172.24.13.81
```

Related Commands

Command	Description
ip address-pool	Enables an address pooling mechanism used to supply IP addresses to dial-in asynchronous, synchronous, or ISDN point-to-point interfaces.
ip helper-address	Forwards UDP broadcasts, including BOOTP, received on an interface.
peer default ip address	Specifies an IP address, an address from a specific IP address pool, or an address from the DHCP mechanism to be returned to a remote peer connecting to this interface.
show cot dsp	Displays information about the COT DSP configuration or current status.

ip dhcp-server query lease

To change the default global retransmission scheme for Dynamic Host Configuration Protocol (DHCP) lease query packets, use the **ip dhcp-server query lease**command in global configuration mode. To remove this retransmission scheme and return to the default behavior, use the **no** form of this command.

ip dhcp-server query lease {**retries** *number* | **timeout** *seconds*}
no ip dhcp-server query lease {**retries** *number* | **timeout** *seconds*}

Syntax Description

retries *number*	The number of times the DHCP lease is transmitted following a timeout for an authoritative reply. The range is from 0 to 5. The default is 2 retries. A value of 0 means no retransmission (a single failure).
timeout *seconds*	The number of seconds to wait for a reply to a query. The range is from 1 to 60 seconds. The default is 5 seconds

Command Default

retries *number* : 2**timeout** *seconds*: 5

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

The DHCP Lease Query protocol is a lightweight mechanism to query a DHCP server for certain information related to IP addresses leased from the DHCP server.

You can specify which DHCP servers to query by using the **ip dhcp-server** global configuration command. You can specify up to 10 servers on the network. Use the **ip dhcp-server query lease**global configuration command to change the default global retransmission scheme for lease query packets.

Examples

In the following example, the time to wait for a reply to a lease query is set to 15 seconds:

```
ip dhcp-server query lease timeout 15
```

In the following example, the retry number is set to 0, which means that only a single DHCP lease query will be transmitted for each DHCP server; no retries will be attempted.

```
ip dhcp-server query lease retries 0
```

Related Commands

Command	Description
ip dhcp-server	Specifies which DHCP server to use on your network.

ip dns name-list

To add a hostname pattern-matching rule to the end of a Domain Name System (DNS) name list, use the **ip dns name-list** command in global configuration mode. To remove a rule from a DNS name list or to remove an entire name-list, use the **no** form of this command.

ip dns name-list *name-list-number* {**deny** | **permit**} *pattern*
no ip dns name-list *name-list-number* [{**deny** | **permit**} *pattern*]

Syntax Description

name-list-number	Integer from 1 to 500 that identifies the DNS name list.
deny	Specifies that any name matching the specified pattern immediately terminates matching the name list with a negative result.
permit	Specifies that any name matching the specified pattern immediately terminates matching the name list with a positive result.
pattern	Regular expression, case-insensitive, to be compared to the a DNS query hostname.

Command Default

No DNS name list is defined or modified. The access list defaults to an implicit **deny .*** clause. The access list is always terminated by an implicit **deny .*** clause.

Command Modes

Global configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command adds a hostname pattern-matching rule to the end of the specified DNS name list. A DNS name list is identified by a unique *name-list-number* value and defines an ordered list of hostname pattern-matching rules that the Cisco IOS software can use to match hostnames in a DNS query.

If the DNS name list does not exist yet, it is automatically created.

When a DNS name list is used to determine if a DNS view list member can be used to handle an incoming DNS query, the individual deny and permit clauses function as follows:

- If the query hostname matches the pattern in a deny clause, the DNS view is rejected; the view-selection process moves on to the next member of the DNS view list.
- If the query hostname matches the pattern in a permit clause, the DNS view is selected to handle the query; the view-selection process is finished.
- There is an implicit deny statement at the end of the access list. If the view-selection process reaches the end of the DNS name list without either a deny clause that causes the view to be rejected or a permit clause that causes the view to be selected, the DNS view is rejected; the view-selection process moves onto the next member of the DNS view list.

For any DNS name list number, the **ip dns name-list** command can be entered multiple times to specify any number of pattern-matching rules in a single name list.

To display a particular DNS name list or all configured name lists, use the **show ip dns name-list** command.

Use of Pattern Matching Characters to Specify the Hostname Pattern

Any rule in a DNS name list can include Cisco regular expression pattern-matching characters in the regular expression that defines the hostname pattern. For a detailed description of regular expressions and regular expression pattern-matching characters, see the *Cisco IOS Terminal Services Configuration Guide* .

Use of a DNS Name List Definition

A DNS name list can be referenced by a DNS view list (accessed by using the **ip dns view-list** command), within a DNS view list member definition (accessed by using the **view** command) that has been configured to deny or permit the use of that DNS view for handling a given DNS query based on whether the destination hostname adheres to a particular DNS name list. To configure this type of usage restriction on the view list member, use the **restrict name-group** command.

Examples

The following example shows how to configure DNS name list number 9 so that the name list will be matched if the query hostname matches either www.example2.com or *.example3.com:

```
Router(config)# ip dns name-list 9 permit www.example2.com

Router(config)# ip dns name-list 9 permit .*.example3.org
```

Related Commands

Command	Description
debug ip dns name-list	Enables debugging output for DNS name list events.
ip dns name-list	Defines a list of pattern-matching rules in which each rule permits or denies the use of a DNS view list member to handle a DNS query based on whether the query hostname matches the specified regular expression.
restrict name-group	Restricts the use of the DNS view list member to DNS queries for which the query hostname matches a particular DNS name list.
show ip dns name-list	Displays a particular DNS name list or all configured name lists.
view	Enters DNS view list member configuration mode so that usage restrictions can be configured for the view list member.

ip dns primary

To configure the router as authoritative for a zone, use the **ip dns primary** command in global configuration mode. To configure the router as nonauthoritative for a zone, use the **no** form of this command.

ip dns primary *domain-name* **soa** *primary-server-name mailbox-name* [*refresh-interval* [*retry-interval* [*expire-ttl* [*minimum-ttl*]]]]
no ip dns primary *domain-name*

Syntax Description

domain-name	Name of the Domain Name System (DNS).
soa	Start of authority record parameters.
primary-server-name	Authoritative name server.
mailbox-name	DNS mailbox of administrative contact.
refresh-interval	(Optional) Refresh time in seconds. This time interval must elapse between each poll of the primary by the secondary name server. The range is from 0 to 4294967295. The default is 21600 (6 hours).
retry-interval	(Optional) Refresh retry time in seconds. This time interval must elapse between successive connection attempts by the secondary to reach the primary name server in case the first attempt failed. The range is from 0 to 4294967295. The default is 900 (15 minutes).
expire-ttl	(Optional) Authority expire time in seconds. The secondary expires its data if it cannot reach the primary name server within this time interval. The range is from 0 to 4294967295. The default is 7776000 (90 days).
minimum-ttl	(Optional) Minimum Time to Live (TTL) in seconds for zone information. Other servers should cache data from the name server for this length of time. The range is from 0 to 4294967295. The default is 86400 (1 day).

Command Default

No authority record parameters are configured for the DNS name server, so queries to the DNS server for locally defined hosts will not receive authoritative responses from this server.

Command Modes

Global configuration

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

Use this command to configure the router as an authoritative name server for the host table, or zone file, of a DNS domain. The primary name server name and a DNS mailbox name are required authority record parameters. Optionally, you can override the default values for the polling refresh interval, the refresh retry interval, the authority expire time, and the minimum TTL for zone information.

To display the authoritative name server configuration for the router, use the **show ip dns primary** command.

Examples

The following example shows how to configure the router as the primary DNS server authoritative for the example.com domain, or zone:

```
Router(config)# ip dns primary example.com soa ns1.example.com mb1.example.com
 10800
 900
 5184000
 172800
```

In the above example, the DNS domain name of the router is ns1.example.com, and the administrative contact for this zone is mb1@example.com. The refresh time is 3 hours, the refresh retry time is 15 minutes, the authority expire time is 60 days, and the minimum TTL is 2 days.

Related Commands

Command	Description
ip dns server	Enables the DNS server on a router.
ip host	Defines static hostname-to-address mappings in the DNS hostname cache for a DNS view.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.
show ip dns primary	Displays the authoritative name server configuration for the router.

ip dns server

To enable the Domain Name System (DNS) server on a router, use the **ip dns server** command in global configuration mode. To disable the DNS server, use the **no** form of the command.

ip dns server
no ip dns server

Syntax Description

This command has no arguments or keywords.

Command Default

The DNS server is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

Use this command to enable the DNS server as needed.

Examples

In the following example, the DNS server is enabled:

```
Router(config)# ip dns server
```

ip dns server queue limit

To configure a limit to the size of the queues used by the Domain Name System (DNS) server processes, use the **ip dns server queue limit**command in global configuration mode. To remove any limit on the queue, use the **no** form of this command.

ip dns server queue limit forwarder *queue-size-limit*
no ip dns server queue limit forwarder

Syntax Description

forwarder	Sets the queue limit for the forwarder queue.
queue-size-limit	Specifies the maximum size to be used for the queue. Valid range is from 0 to 1000000. Value 0 indicates no limit.

Command Default

The queue limit is set to 0, indicating there is no limit on the queue.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.4(24)T	The **director** keyword was removed.

Usage Guidelines

When a DNS query is forwarded to another nameserver for resolution, some memory space is held for the corresponding DNS query until an appropriate response is received or until there is a timeout. If the queries are being received at a very high rate, this may result in the free I/O memory getting exhausted.

Use the **ip dns server queue limit** command to set a limit to the size of the queue.

Examples

The following example shows how to set the limit to the forwarder queue used by the DNS server:

```
Router(config)# ip dns server queue limit forwarder 10
Router(config)#
```

Related Commands

Command	Description
show ip dns statistics	Displays packet statistics for the DNS server.

ip dns server view-group

To specify the default Domain Name System (DNS) server view list for the router, use the **ip dns server view-group** command in global configuration mode. To remove this definition, use the **no** form of this command.

ip dns server view-group *view-list-name*
no ip dns server view-group

Syntax Description

view-list-name	Name of a DNS view list. **Note** If the specified view list does not exist, a warning is displayed but the default view list setting is configured anyway. The specified view list can be defined after the default DNS server view list is configured.

Command Default

No default DNS view list is configured; incoming queries arriving on an interface not assigned a specific DNS view list will be handled using the global default view.

Command Modes

Global configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command configures the router to use the specified DNS server view list as the default DNS view list. The default DNS view list is used to determine which DNS view the router will use to handle a given incoming DNS query that arrives on an interface that is not configured with a DNS view list. The router checks these types of DNS queries against the DNS view list entries (in the order specified in the DNS view list) and uses the first DNS view list member whose restrictions allow the view to handle that query.

To specify that the router uses a particular DNS view list to choose the DNS view to use to handle incoming DNS queries that arrives on a specific interface, use the **ip dns view-group** command.



Note The *view-list-name* argument referenced in this command is configured using the **ip dns view-list** command. The DNS view list is referred to as a "view list" when it is defined and as a "view group" when it is referenced in other commands.

Examples

The following example shows how to configure the DNS name list userlist1 as the default name list:

```
Router(config)# ip dns server view-group userlist1
```

Related Commands

Command	Description
ip dns view-group	Specifies the DNS view list to use to determine which DNS view to use to handle incoming DNS queries that arrive on a specific interface.
ip dns view-list	Enters DNS view list configuration mode so that DNS views can be added to or removed from the ordered list of DNS views.
show ip dns view-list	Displays information about a particular DNS view list or about all configured DNS view lists.

ip dns spoofing

To enable Domain Name System (DNS) spoofing, use the **ip dns spoofing** command in global configuration mode. To disable DNS spoofing, use the **no** form of this command.

ip dns spoofing [*ip-address*]
no ip dns spoofing [*ip-address*]

Syntax Description

ip-address	(Optional) IP address used in replies to DNS queries. **Note** You can specify an IPv4 or IPv6 address for DNS spoofing.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS 12.2(28)SB.
15.4(1)T	This command was modified. An IPv6 address can be specified for the *ip-address* argument.

Usage Guidelines

DNS spoofing allows a device to act as a proxy DNS server and "spoof" replies to any DNS queries using either the configured IP address in the **ip dns spoofing** command or the IP address of the incoming interface for the query. This functionality is useful for devices where the interface toward the ISP is not up. Once the interface to the ISP is up, the device forwards DNS queries to the real DNS servers.

The device will respond to the DNS query with the configured IP address when queried for any host name other than its own but will respond to the DNS query with the IP address of the incoming interface when queried for its own host name.

The host name used in the DNS query is defined as the exact configured host name of the device specified by the **hostname** command, with no default domain appended. For example, consider the following configuration:

```
ip domain name cisco.com
hostname host1
```

Here, the system would respond with a DNS spoofing reply if queried for "host1" but not for "host1.cisco.com".

Examples

In the following example, the device will respond to a DNS query with an IP address of 192.168.15.1:

```
Device(config)# ip dns spoofing 192.168.15.1
```

ip dns view

To access or create the Domain Name System (DNS) view of the specified name associated with the specified VPN routing and forwarding (VRF) instance and then enter DNS view configuration mode so that forwarding and routing parameters can be configured for the view, use the **ip dns view** command in global configuration mode. To remove the definition of the specified DNS view and then return to global configuration mode, use the **no** form of this command.

ip dns view [**vrf** *vrf-name*] {**default***view-name*}
no ip dns view [**vrf** *vrf-name*] {**default***view-name*}

Syntax Description

vrf *vrf-name*	(Optional) The *vrf-name* argument specifies the name of the VRF associated with the DNS view. Default is to associate the DNS view with the global VRF (that is, the VRF whose name is a NULL string). **Note** If the named VRF does not exist, a warning is displayed but the view is created anyway. The specified VRF can be defined after the DNS view is configured. **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.
default	Refers to the unnamed DNS view.
view-name	String (not to exceed 64 characters) that specifies the name of the DNS view. **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.

Command Default

No new DNS view is accessed or created.

Command Modes

Global configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command enters DNS view configuration mode--for the specified DNS view--so that forwarding parameters, resolving parameters, and the logging setting can be configured for that view. If the specified DNS view does not exist yet, it is automatically created.

Note The maximum number of DNS views and view lists supported is not specifically limited but is dependent on the amount of memory on the Cisco router. Configuring a larger number of DNS views and view lists uses more router memory, and configuring a larger number of views in the view lists uses more router processor time. For optimum performance, configure no more views and view list members than needed to support your Split DNS query forwarding or query resolution needs.

The default view associated with the unnamed global VRF exists by default. This is the view that is referenced by using the **ip dns view** command without specifying a VRF and specifying the **default** keyword instead of a *view-name* argument. The default DNS view cannot be removed.

Different DNS views can be associated with the same VRF.

To enable debugging output for DNS view events, use the **debug ip dns view** command.

To display information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used, use the **show ip dns view** command.

When you configure the **ip dns view ezvpn-internal-view** command, the command removes all saved configurations from the running configuration. This is because **ezvpn-internal-view** is a reserved DNS view for use on Easy VPN hardware clients, and is not intended to be modified. The configurations are removed when a Network Extension Mode (NEM) hardware client establishes an IPsec tunnel to the NEM server. The configuration remains until the IPsec tunnel is formed.

Subsequent Operations on a DNS View Definition

After you use the **ip dns view** command to define a DNS view and enter DNS view configuration mode, you can configure DNS forwarder parameters, DNS resolution parameters, and system message logging for the view.

To configure the Cisco IOS DNS forwarder functionality, use the following commands:

- **dns forwarder**
- **dns forwarding**
- **dns forwarding source interface**

To configure the Cisco IOS DNS resolver functionality, use the following commands:

- **domain list**
- **domain lookup**
- **domain multicast**
- **domain name**
- **domain name-server**
- **domain name-server interface**
- **domain retry**
- **domain round-robin**
- **domain timeout**

To enable logging of a system message logging (syslog) message each time the DNS view is used, use the **logging** command.

Use of a DNS View Definition

After a DNS view is configured, the view can be added to a DNS view list (by using the **ip dns view-list** command) and usage restrictions for that view within that view list can configured (by using the **restrict name-group** and **restrict source access-grou**p commands).

Examples

The following example shows how to define the default DNS view in the global address space. This DNS view exists by default, and it is the view that has been in use since before the Split DNS feature was implemented.

```
Router(config)# ip dns view default
```

The following example shows how to define the default DNS view associated with VRF vpn101, creating the view if it does not already exist:

```
Router(config)# ip dns view vrf vpn101 default
```

The following example shows how to define the DNS view user2 in the global address space, creating the view if it does not already exist:

```
Router(config)# ip dns view user2
```

The following example shows how to define the DNS view user2 associated with VRF vpn101, creating the view if it does not already exist:

```
ip dns view vrf vpn101 user2
```

Related Commands

Command	Description
debug ip dns view	Enables debugging output for DNS view events.
dns forwarder	Specifies the ordered list of IP addresses to use when forwarding incoming DNS queries handled using the DNS view.
dns forwarding	Enables forwarding of incoming DNS queries by the DNS view.
dns forwarding source-interface	Specifies the interface to use when forwarding incoming DNS queries handled using the DNS view.
domain list	Defines the ordered list of default domain names to use to complete unqualified hostnames in internally generated DNS queries handled using the DNS view.
domain lookup	Enables the IP DNS-based hostname-to-address translation for internally generated DNS queries handled using the DNS view.
domain multicast	Specifies the IP address to use for multicast lookups handled using the DNS view.
domain name	Specifies a single default domain name to use to complete unqualified hostnames in internally generated DNS queries handled using the DNS view.

Command	Description
domain name-server	Specifies the ordered list of IP addresses to use when resolving internally generated DNS queries handled using the DNS view.
domain name-server interface	Specifies the interface from which the device can learn (through either DHCP or PPP interaction on the interface) a DNS resolving name server address for the DNS view.
domain retry	Specifies the number of times to retry sending or forwarding a DNS query handled using the DNS view.
domain round-robin	Enables round-robin rotation of multiple IP addresses in the global or VRF-specific DNS hostname cache during the TTL of the cache each time DNS lookup is performed to resolve an internally generated DNS query handled using the DNS view.
domain timeout	Specifies the amount of time to wait for a response to a sent or forwarded DNS query handled using the DNS view.
ip dns view-list	Enters DNS view list configuration mode so that DNS views can be added to or removed from the ordered list of DNS views.
logging	Enables logging of a syslog message each time the DNS view is used.
restrict name-group	Restricts the use of the DNS view list member to DNS queries for which the query hostname matches a particular DNS name list.
restrict source access-group	Restricts the use of the DNS view list member to DNS queries for which the query source IP address matches a particular standard ACL.
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

ip dns view-group

To attach a Domain Name System (DNS) view list to the interface, use the **ip dns view-group** command in interface configuration mode. To disable the attachment of a DNS view list to an interface, use the **no** form of this command.

ip dns view-group *view-list-name*
no ip dns view-group *view-list-name*

Syntax Description

view-list-name	Name of an existing DNS view list. **Note** If the specified view list does not exist, a warning is displayed and the view list setting is not configured for the interface.

Command Default

No DNS view list is attached to the interface. If a default DNS view list is configured, that view list is used to handle incoming DNS queries. If no view list has been configured either on this specific interface or for the system, incoming DNS queries are handled using the default global view.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command configures the router to use the specified DNS view list to choose which DNS view to use to handle incoming DNS queries that arrive on the interface.

Only one DNS view list can be assigned to a given interface. However, a single DNS view list can be assigned to any number of interfaces so that the same ordered list of DNS views (along with the restrictions specified in the view list) can be checked by multiple interfaces.

A DNS view list can also be configured as the default DNS view list (by using the **ip dns server view-group** command) to determine which DNS view the router will use to handle a given incoming DNS query that arrives on an interface that is not configured with a DNS view list.



Note The *view-list-name* argument referenced in this command is configured using the **ip dns view-list** command. The DNS view list is referred to as a "view list" when it is defined and as a "view group" when it is referenced in other commands.

When an incoming DNS query is received through the interface, the Cisco IOS software will check the members of the DNS view list--in the order specified in the view list--to determine if the usage restrictions on any view list member allow the view to be used to forward the incoming query:

- Each DNS view list member is checked, in the order specified by the list.

- The first DNS view in the view list with configured usage restrictions (based on the query destination hostname or the query source IP address) that allow its use for the query will be used to forward the incoming query.

If the hostname cache for the view contains the information needed to answer the query, the router will respond to the query with the hostname IP address in that internal cache. Otherwise, provided DNS forwarding is enabled for the DNS view, the router will forward the query to the configured name servers (each in turn, until a response is received), and the response will be both added to the hostname cache and sent back to the originator of the query.

- If no DNS view in the DNS view list is qualified to handle the query, the router drops the query.

Examples

The following example shows how to configure the router so that each time a DNS query arrives through interface ethernet0 the usage restrictions for the members of the DNS view list userlist2 are checked in the order specified by the view list definition. The router uses the first view list member whose usage restrictions allow that DNS view to forward the query.

```
Router(config)# interface ethernet0

Router(config-if)# ip dns view-group userlist2
```

Related Commands

Command	Description
interface	Selects an interface to configure.
ip dns server view-group	Specifies the DNS view list to use to determine which DNS view to use handle incoming queries that arrive on an interface not configured with a DNS view list.
ip dns view	Enters DNS view configuration mode for the specified DNS view so that the logging setting, forwarding parameters, and resolving parameters can be configured for the view.
ip dns view-list	Enters DNS view list configuration mode so that DNS views can be added to or removed from the ordered list of DNS views.
show ip dns view-list	Displays information about a particular DNS view list or about all configured DNS view lists.

ip dns view-list

To access or create the Domain Name System (DNS) view list of the specified name and then enter DNS view list configuration mode so that DNS views can be added to or removed from the ordered list of DNS view members, use the **ip dns view-list** command in global configuration mode. To remove the definition of the specified DNS view list, use the **no** form of this command.

ip dns view-list *view-list-name*
no dns view-list *view-list-name*

Syntax Description

view-list-name	Text string (not to exceed 64 characters) that uniquely identifies the DNS view list to be created.

Command Default

No DNS view list is accessed or created.

Command Modes

Global configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command enters DNS view list configuration mode--for the specified view list--so that individual view list members (DNS views and their order numbers within the view list) can be accessed in, added to, or deleted from that view list. If the specified DNS view list does not exist yet, it is automatically created.

Note The maximum number of DNS views and view lists supported is not specifically limited but is dependent on the amount of memory on the Cisco router. Configuring a larger number of DNS views and view lists uses more router memory, and configuring a larger number of views in the view lists uses more router processor time. For optimum performance, configure no more views and view list members than needed to support your Split DNS query forwarding or query resolution needs.

To display information about a specific DNS view list or all currently configured DNS view lists, use the **show ip dns view-list** command.

Subsequent Operations on a DNS View List

After you use the **ip dns view-list** command to define a DNS view list and enter DNS view list configuration mode, you can use the **view** command to access a view list member or add a DNS view as a new view list member at the end of the list. Each view list member specifies a DNS view and a value that indicates the relative order for checking that view when the DNS view list is used. to determine if it can be used to address a DNS query.

For any DNS view list member, you can use the **restrict authenticated**, **restrict name-group**, and **restrict source access-group** commands to configure usage restrictions for the DNS view list member. These restrictions are based on query source authentication, the query hostname, and the query source host IP address, respectively.

Purpose of a DNS View List

When a DNS view list is used to select a DNS view to use to handle a given DNS query, the Cisco IOS software checks each DNS view in the DNS view list--in the order specified in the view list--to determine if the usage restrictions for that view allow the view to be used to address that particular DNS query.

The first DNS view with configured usage restrictions that allow its use for the DNS query will be used to resolve or forward the query. That is, the router will use the configuration parameters for that DNS view to either respond to the query (by using the name cache belonging to the DNS view) or forward the query to the configured name servers. If no DNS view in the view list is qualified to handle the query, the router does not send or forward the query.



Note Multiple DNS view list definitions enable you to use the same DNS view, but with different restrictions, depending on the source of the DNS query being processed. For example, in one DNS view list a particular DNS view could be used with very few usage restrictions, while in another DNS view list the same DNS view could be used with more usage restrictions.

Use of a DNS View List for DNS Queries Incoming from a Particular Interface

Use the **ip dns view-group** command to configure the router to use a particular DNS view list to determine which DNS view to use to handle incoming DNS queries that arrive on that interface. Only one DNS view list can be assigned to a given interface. However, a single DNS view list can be assigned to any number of interfaces so that the same ordered list of DNS views (along with the restrictions specified in the view list) can be checked by multiple interfaces.

Use of a DNS View List as the Default DNS View List

Use the **ip dns server view-list** command to configure the default DNS view list. The router uses the default DNS view list to determine which DNS view to use to handle incoming DNS queries that arrive on an interface that is not configured with a DNS view list.

Examples

The following example shows how to remove the DNS view user1 from the DNS view list userlist5 and then add the view back to the view list, but with a different position indicator specified for that member within the view list. A usage restriction is also added to the view list member user1.

```
Router(config)# ip dns view-list userlist5

Router(cfg-dns-view-list)# no view user1 30

Router(cfg-dns-view-list)# view user1 10

Router(cfg-dns-view-list)# restrict name-group 7
```

Related Commands

Command	Description
debug ip dns view-list	Enables debugging output for DNS view list events.
ip dns server view-group	Specifies the DNS view list to use to determine which DNS view to use to handle incoming queries that arrive on an interface not configured with a DNS view list.

Command	Description
ip dns view	Enters DNS view configuration mode for the specified DNS view so that the logging setting, forwarding parameters, and resolving parameters can be configured for the view.
ip dns view-group	Specifies the DNS view list to use to determine which DNS view to use to handle incoming DNS queries that arrive on a specific interface.
restrict authenticated	Restricts the use of the DNS view list member to DNS queries for which the DNS query host can be authenticated.
restrict name-group	Restricts the use of the DNS view list member to DNS queries for which the query hostname matches a particular DNS name list.
restrict source access-group	Restricts the use of the DNS view list member to DNS queries for which the query source IP address matches a particular standard ACL.
show ip dns view-list	Displays information about a particular DNS view list or about all configured DNS view lists.
view	Enters DNS view list member configuration mode so that usage restrictions can be configured for the view list member.

ip domain list

To define a list of default domain names to complete unqualified names, use the **ip domain list** command in global configuration mode. To delete a name from a list, use the no form of this command.

ip domain list [**vrf** *vrf-name*] *name*
no ip domain list [**vrf** *vrf-name*] *name*

Syntax Description

vrf *vrf-name*	(Optional) Defines a Virtual Private Network (VPN) routing and forwarding instance (VRF) table. The *vrf-name* argument specifies a name for the VRF table.
name	Domain name. Do not include the initial period that separates an unqualified name from the domain name.

Command Default

No domain names are defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2	The syntax of the command changed from **ip domain-list** to **ip domain list**.
12.4(4)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If there is no domain list, the domain name that you specified with the **ip domain name** global configuration command is used. If there is a domain list, the default domain name is not used. The **ip domain list** command is similar to the **ip domain name** command, except that with the **ip domain list**command you can define a list of domains, each to be tried in turn until the system finds a match.

If the **ip domain list vrf** command option is specified, the domain names are only used for name queries in the specified VRF.

The Cisco IOS software will still accept the previous version of the command, **ip domain-list**.

Examples

The following example shows how to add several domain names to a list:

```
ip domain list company.com
ip domain list school.edu
```

The following example shows how to add several domain names to a list in vpn1 and vpn2:

```
ip domain list vrf vpn1 company.com
ip domain list vrf vpn2 school.edu
```

Related Commands

Command	Description
ip domain list	Defines a list of default domain names to complete unqualified hostnames.
ip domain lookup	Enables the IP DNS-based hostname-to-address translation.
ip domain retry	Specifies the number of times to retry sending DNS queries.
ip domain timeout	Specifies the amount of time to wait for a response to a DNS query.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.

ip domain lookup

To enable IP Domain Name System (DNS)-based hostname-to-address translation, use the **ip domain lookup** command in global configuration mode. To disable DNS-based hostname-to-address translation, use the **no** form of this command.

ip domain lookup [**nsap** | **recursive** | [**vrf** *vrf-name*] [**source-interface** *interface-type interface-number*]]
no ip domain lookup [**nsap** | **recursive** | [**vrf** *vrf-name*] [**source-interface** *interface-type interface-number*]]

Syntax Description

nsap	(Optional) Enables IP DNS queries for Connectionless Network Service (CLNS) and Network Service Access Point (NSAP) addresses.
recursive	(Optional) Enables IP DNS recursive lookup.
vrf *vrf-name*	(Optional) Defines a Virtual Routing and Forwarding (VRF) table. The *vrf-name* argument specifies a name for the VRF table.
source-interface	(Optional) Specifies the source interface for the DNS resolver.
interface-type interface-number	(Optional) The type of interface and the interface number.

Command Default

IP DNS-based hostname-to-address translation is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2	This command was modified. The syntax of the command changed from **ip domain-lookup** to **ip domain lookup**.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(1)M	This command was modified. The **nsap** keyword was added.
Cisco IOS XE Release 3.10S	This command was modified. The **vrf** keyword and the *vrf-name* argument were added.

Release	Modification
Cisco IOS XE Dublin 17.12.1	In previous releases, the **ip domain lookup source-interface** configuration would be removed if the configured source-interface went down or if the interface experienced flap. The removal of the configuration was done programmatically without admin notification. Starting from the Cisco IOS XE Dublin 17.12.x release, the configuration remains intact when the configured interface goes down or experiences a flap.

Usage Guidelines

If the **ip domain lookup** command is enabled on a device, and you execute the **show tcp brief** command, the output may be displayed very slowly. With both IP and ISO CLNS enabled on a device, the **ip domain lookup nsap** command allows you to discover a CLNS address without having to specify a full CLNS address, given a hostname. The **ip domain lookup** command is useful for the **ping** (ISO CLNS) command, and for CLNS Telnet connections.

When configuring the **ip domain lookup source-interface** command, the user must ensure that the interface is in an up state for DNS functionality to work correctly. If the interface is in a down state or if the interface is removed, DNS queries that rely on this configuration will not work as expected.

Examples

The following example shows how to configure IP DNS-based hostname-to-address translation:

```
Device> enable
Device# configure terminal
Device(config)# ip domain lookup
Device(config)# end
```

The following example shows how to configure IP DNS-based hostname-to-address translation for a specified VRF and interface:

```
Device> enable
Device# configure terminal
Device(config)# ip domain lookup vrf RED source-interface ethernet 1/2
Device(config)# end
```

Related Commands

Command	Description
ip domain list	Defines a list of default domain names to complete unqualified hostnames.
ip domain retry	Specifies the number of times to retry sending DNS queries.
ip domain timeout	Specifies the amount of time to wait for a response to a DNS query.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.
show tcp brief	Displays a concise description of TCP connection endpoints.

ip domain multicast

To create a domain prefix for Domain Name Service (DNS)-based Source Specific Multicast (SSM) mapping, use the **ip domain multicast** command in global configuration mode. To revert to the default domain prefix, use the **no** form of this command.

ip domain multicast *domain-prefix*
no ip domain multicast *domain-prefix*

Syntax Description

domain-prefix	Name of the domain prefix to be used for DNS-based SSM mapping.

Command Default

By default, the ip-addr.arpa domain is used as the domain prefix.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18) SXD3	This command was integrated into Cisco IOS Release 12.2(18)SXD3.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.

Usage Guidelines

When a device attempts DNS-based SSM mapping for an IP group address (G = G1.G2.G3.G4), the device queries the domain name server for IP address resource records (DNS record type ‘A’) for the domain G4.G3.G2.G1 *domain-prefix*.

Examples

The following example shows you how to create a domain prefix for DNS-based SSM mapping:

```
ip domain multicast ssm-map.cisco.com
```

Related Commands

Command	Description
ip igmp ssm-map enable	Enables SSM mapping for groups in a configured SSM range.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.

ip domain name

To define a default domain name that the Cisco IOS software uses to complete unqualified hostnames (names without a dotted-decimal domain name), use the **ip domain name** command in global configuration mode. To disable use of the Domain Name System (DNS), use the noform of this command.

ip domain name [**vrf** *vrf-name*] *name*
no ip domain name [**vrf** *vrf-name*] *name*

Syntax Description

vrf *vrf-name*	(Optional) Defines a Virtual Private Network (VPN) routing and forwarding instance (VRF) table. The *vrf-name* argument specifies a name for the VRF table.
name	Default domain name used to complete unqualified hostnames. Do not include the initial period that separates an unqualified name from the domain name.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2	The syntax of the command changed from **ip domain-name**to **ip domain name**.
12.4(4)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Any IP hostname that does not contain a domain name (that is, any name without a dot) will have the dot and cisco.com appended to it before being added to the host table.

If the **ip domain name vrf** command option is specified, the domain names are only used for name queries in the specified VRF.

The Cisco IOS software will still accept the previous version of the command, which is **ip domain-name**.

Examples

The following example shows how to define cisco.com as the default domain name:

```
ip domain name cisco.com
```

The following example shows how to define cisco.com as the default domain name for vpn1:

```
ip domain name vrf vpn1 cisco.com
```

Related Commands

Command	Description
ip domain list	Defines a list of default domain names to complete unqualified hostnames.
ip domain lookup	Enables the IP DNS-based hostname-to-address translation.
ip domain retry	Specifies the number of times to retry sending DNS queries.
ip domain timeout	Specifies the amount of time to wait for a response to a DNS query.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.

ip domain recursive

To enable recursive DNS querying for a device, use the **ip domain recursive** command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip domain recursive {**allow-soa** | **retry** *maximum-referral-value*}
no ip domain recursive {**allow-soa** | **retry** *maximum-referral-value*}

Syntax Description

allow-soa	Treats a recursive DNS query response from an authoritative name server containing a start of authority (SOA) record as a referral.
retry *maximum-referral-value*	Configures the maximum number of retries for a DNS recursive query. The default value is 10.

Command Default

Recursive DNS querying is disabled for a device.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.12S	This command was introduced in a release earlier than Cisco IOS XE Release 3.12S.

Usage Guidelines

Examples

The following example shows you how to enable recursive DNS querying for a device and set a value for the maximum number of retries for a DNS recursive query:

```
Device> enable
Device# configure terminal
Device(config)# ip domain recursive retry 11
Device(config)# end
```

Related Commands

Command	Description
ip domain list	Defines a list of default domain names to complete unqualified hostnames.
ip domain lookup	Enables the IP DNS-based hostname-to-address translation.
ip domain multicast	Creates a domain prefix for DNS-based SSM mapping.
ip domain retry	Specifies the number of times to retry sending DNS queries.

ip domain retry

To specify the number of times to retry sending Domain Name System (DNS) queries, use the **ip domain retry**command in global configuration mode. To return to the default behavior, use the no form of this command.

ip domain retry *number*
no ip domain retry *number*

Syntax Description

number	Number of times to retry sending a DNS query to the DNS server. The range is from 0 to 100; the default is 2.

Command Default

number : 2 times

Command Modes

Global configuration

Command History

Release	Modification
12.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the **ip domain retry** command is not configured, the Cisco IOS software will only send DNS queries out twice.

Examples

The following example shows how to configure the router to send out 10 DNS queries before giving up:

```
ip domain retry 10
```

Related Commands

Command	Description
ip domain list	Defines a list of default domain names to complete unqualified host names.
ip domain lookup	Enables the IP DNS-based host name-to-address translation.
ip domain retry	Specifies the number of times to retry sending DNS queries.
ip domain timeout	Specifies the amount of time to wait for a response to a DNS query.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.

ip domain round-robin

To enable round-robin functionality on DNS servers, use the **ip domain round-robin**command in global configuration mode. To disable round-robin functionality, use the no form of the command.

ip domain round-robin
no ip domain round-robin

Syntax Description

This command has no arguments or keywords.

Command Default

Round robin is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

In a multiple server configuration without the DNS round-robin functionality, the first host server/IP address is used for the whole time to live (TTL) of the cache, and uses the second and third only in the event of host failure. This behavior presents a problem when a high volume of users all arrive at the first host during the TTL time. The network access server (NAS) then sends out a DNS query; the DNS servers reply with a list of the configured IP addresses to the NAS. The NAS then caches these IP addresses for a given time (for example, five minutes). All users that dial in during the five minute TTL time will land on one host, the first IP address in the list.

In a multiple server configuration with the DNS round-robin functionality, the DNS server returns the IP address of all hosts to rotate between the cache of host names. During the TTL of the cache, users are distributed among the hosts. This functionality distributes calls across the configured hosts and reduces the amount of DNS queries.

Examples

The following example allows a Telnet to www.company.com to connect to each of the three IP addresses specified in the following order: the first time the Telnet command is given, it would connect to 10.0.0.1; the second time the command is given, it would connect to 10.1.0.1; and the third time the command is given, it would connect to 10.2.0.1. In each case, the other two addresses would also be tried if the first one failed; this is the normal operation of the Telnet command.

```
ip host www.server1.com 10.0.0.1 10.1.0.1 10.2.0.1
ip domain round-robin
```

ip domain timeout

To specify the amount of time to wait for a response to a DNS query, use the **ip domain timeout**command in global configuration mode. To return to the default behavior, use the no form of this command.

ip domain timeout *seconds*
no ip domain timeout *seconds*

Syntax Description

seconds	Time, in seconds, to wait for a response to a DNS query. The range is from 0 to 3600; the default is 3.

Command Default

seconds : 3 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the **ip domain timeout** command is not configured, the Cisco IOS software will only wait 3 seconds for a response to a DNS query.

Examples

The following example shows how to configure the router to wait 50 seonds for a response to a DNS query:

```
ip domain timeout 50
```

Related Commands

Command	Description
ip domain list	Defines a list of default domain names to complete unqualified host names.
ip domain lookup	Enables the IP DNS-based host name-to-address translation.
ip domain retry	Specifies the number of times to retry sending DNS queries.
ip domain timeout	Specifies the amount of time to wait for a response to a DNS query.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.

ip gratuitous-arps

To enable the transmission of gratuitous Address Resolution Protocol (ARP) messages for an address in an address pool if the transmission has been disabled, use the **ip gratuitous-arps** command in global configuration mode. To disable the transmission, use the **no**form of this command.

ip gratuitous-arps [**non-local**]
no ip gratuitous-arps

Syntax Description

non-local	(Optional) Sends gratuitous ARP messages if a client receives an IP address from a non-local address pool. Gratuitous ARP messages for locally originated peer addresses are not sent by default.

Command Default

Gratuitous ARP messages are not sent out when the client receives the address from the local address pool.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2T	The **non-local** keyword was added and the default behavior of the command changed.
12.4(2)T	The name of this command was changed from **no ip gratuitous-arps** to **ip gratuitous-arps**.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

A Cisco router will send out a gratuitous ARP message out of all interfaces when a client connects and negotiates an address over a PPP connection. However, by default, gratuitous ARP messages are not sent out when the client receives the address from the local address pool. The **ip gratuitous-arps non-local** command option is the default form and is not saved in the running configuration.

Cisco 10000 Series Router

To maximize the performance of the router, disable gratuitous ARP requests using the **no ip gratuitous-arps** command.

Examples

The following example enables the sending of gratuitous ARP messages if the transmission has been disabled:

```
ip gratuitous-arps
```

ip host

To define static hostname-to-address mappings in the Domain Name System (DNS) hostname cache for a DNS view, use the **ip host** command in global configuration mode. If the hostname cache does not exist yet, it is automatically created. To remove a hostname-to-address mapping, use the **no** form of this command.

ip host [**vrf** *vrf-name*] [**view** *view-name*] {*hostname* | **t** *modem-telephone-number*} [*tcp-port-number*] {*ip-address1* [*ip-address2* . . . *ip-address8*] | **additional** *ip-address9* [*ip-address10* . . . *ip-addressn*] | [**mx** *preference mx-server-hostname* | **ns** *nameserver-hostname* | **srv** *priority weight port target*]}
no ip host [**vrf** *vrf-name*] [**view** *view-name*] {*hostname* | **t** *modem-telephone-number*} [*tcp-port-number*] {*ip-address1* [*ip-address2* . . . *ip-address8*] **additional** *ip-address9* [*ip-address10* . . . *ip-addressn*] | [**mx** *preference mx-server-hostname* | **ns** *nameserver-hostname* | **srv** *priority weight port target*]}

Syntax Description

vrf *vrf-name*	(Optional) The *vrf-name* argument specifies the name of the Virtual Private Network (VRF) routing and forwarding (VRF) instance associated with the DNS view whose hostname cache is to store the mappings. Default is the global VRF (that is, the VRF whose name is a NULL string) with the specified or default DNS view. **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.
view *view-name*	(Optional) The *view-name* argument specifies the name of the DNS view whose hostname cache is to store the mappings. Default is the default DNS view associated with the specified or global VRF. **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.
hostname	Name of the host. The first character can be either a letter or a number. If you use a number, the types of operations you can perform (such as ping) are limited.
t *modem-telephone-number*	Modem telephone number that is mapped to the IP host address for use in Cisco modem user interface mode. You must enter the letter "t" before the telephone number. **Note** This argument is not relevant to the Split DNS feature.
tcp-port-number	(Optional) TCP port number to connect to when using the defined hostname in conjunction with an EXEC connect or Telnet command. The default is Telnet (port 23).
ip-address1	Associated host IP address. **Note** You can specify an IPv4 or IPv6 address for the host IP address and additional IP addresses.

ip-address2 ...ip-address8	(Optional) Up to seven additional associated IP addresses, delimited by a single space. **Note** The ellipses in the syntax description are used to indicate a range of values. Do not use ellipses when entering host IP addresses.
additional *ip-address9*	The *ip-address9* argument specifies an additional IP address to add to the hostname cache. **Note** The use of the optional additional keyword enables the addition of more than eight IP addresses to the hostname cache.
ip-address10 ...ip-addressn	(Optional) Additional associated IP addresses, delimited by a single space. **Note** The ellipses in the syntax description are used to indicate a range of values. Do not use ellipses when entering host IP addresses.
mx *preference mx-server-hostname*	(Optional) Mail Exchange (MX) resource record settings for the host: • *preference* --The order in which mailers select MX records when they attempt mail delivery to the host. The lower this value, the higher the host is in priority. Range is from 0 to 65535. • *mx-server-hostname* --The DNS name of the Simple Mail Transfer Protocol (SMTP) server where the mail for a domain name should be delivered. An MX record specifies how you want e-mail to be accepted for the domain specified in the *hostname* argument. **Note** You can have several MX records for a single domain name, and they can be ranked in order of preference.
ns *nameserver-hostname*	(Optional) Name Server (NS) resource record setting for the host: • *nameserver-hostname* --The DNS name of the machine that provides domain service for the particular domain. Machines that provide name service do not have to reside in the named domain. An NS record lists the name of the machine that provides domain service for the domain indicated by the *hostname* argument. **Note** For each domain you must have at least one NS record. NS records for a domain must exist in both the zone that delegates the domain and in the domain itself.

srv *priority weight port target*	(Optional) Server (SRV) resource record settings for the host: • *priority* --The priority to give the record among the owner SRV records. Range is from 0 to 65535. • *weight* --The load to give the record at the same priority level. Range is from 0 to 65535. • *port* --The port on which to run the service. Range is from 0 to 65535. • *target* --Domain name of host running on the specified port. The use of SRV records enables administrators to use several servers for a single domain, to move services from host to host with little difficulty, and to designate some hosts as primary servers for a service and others as backups. Clients ask for a specific service or protocol for a specific domain and receive the names of any available servers.

Command Default

No static hostname-to-address mapping is added to the DNS hostname cache for a DNS view.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(3)T	The **mx** keyword and the *preference* and *mx-server-hostname* arguments were added.
12.0(7)T	The **srv** keyword and the *priority*, *weight*, *port*, and *target* arguments were added.
12.2(1)T	The **ns** keyword and the *nameserver-hostname* argument were added.
12.4(4)T	The capability to map a modem telephone number to an IP host was added for the Cisco modem user interface feature.
12.4(4)T	The **vrf** keyword and *vrf-name* argument were added.
12.4(9)T	The **view** keyword and *view-name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS 12.2(33)SRA.
12.2SX	This command is integrated into Cisco IOS 12.2SX.
15.4(1)T	This command was modified. An IPv6 address can be specified for the *ip-address* argument, and the **additional** *ip-address* keyword-argument pair.

Usage Guidelines

This command adds the specified hostname-to-IP address mappings as follows:

- If no VRF name and no DNS view name is specified, the mappings are added to the global hostname cache.
- Otherwise, the mappings are added to the DNS hostname cache for a specific DNS view:
  - If only a DNS view name is specified, the specified mappings are created in the view-specific hostname cache.

- If only a VRF name is specified, the specified mappings are created in the VRF-specific hostname cache for the default view.
- If both a VRF name and a DNS view name are specified, the specified mappings are created in the VRF-specific hostname cache for the specified view.

If the specified VRF does not exist yet, a warning is displayed and the entry is added to the hostname cache anyway.

If the specified view does not exist yet, a warning is displayed and the entry is added to the hostname cache anyway.

If the hostname cache does not exist yet, it is automatically created.

To specify the machine that provides domain service for the domain, use the **ns** keyword and the *nameserver-hostname* argument

To specify where the mail for the host is to be sent, use the **mx** keyword and the *preference* and *mx-server-hostname* arguments.

To specify a host that offers a service in the domain, use the **srv** keyword and the *priority*, *weight*, *port*, and *target* arguments.

To display the display the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views, use the **show hosts** command.



Note If a global or VRF-specific DNS hostname cache contains hostnames that are associated with multiple IP addresses, round-robin rotation of the returned addresses can be enabled on a DNS view-specific basis (by using the **domain round-robin** command).

Examples

The following example shows how to add three mapping entries to the global hostname cache and then remove one of those entries from the global hostname cache:

```
Device(config)# ip host www.example1.com 192.0.2.141 192.0.2.241

Device(config)# ip host www.example2.com 192.0.2.242

Device(config)# no ip host www.example1.com 192.0.2.141
```

The following example shows how to add three mapping entries to the hostname cache for the DNS view user3 that is associated with the VRF vpn101 and then remove one of those entries from that hostname cache:

```
Device(config)# ip host vrf vpn101 view user3 www.example1.com 192.0.2.141 192.0.2.241

Device(config)# ip host vrf vpn101 view user3 www.example2.com 192.0.2.242

Device(config)# no ip host vrf vpn101 view user3 www.example1.com 192.0.2.141
```

Related Commands

Command	Description
clear host	Removes static hostname-to-address mappings from the hostname cache for the specified DNS view or all DNS views.
domain round-robin	Enables round-robin rotation of multiple IP addresses in the global or VRF-specific DNS hostname cache during the TTL of the cache each time DNS lookup is performed to resolve an internally generated DNS query handled using the DNS view.
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views.

ip host-list

To specify a list of hosts that will receive Dynamic Domain Name System (DDNS) updates of address (A) and pointer (PTR) Resource Records (RRs) and to enter host-list configuration mode, use the **ip host-list**command in global configuration mode. To disable the host list, use the **no** form of this command.

ip host-list *host-list-name* [**vrf** *vrf-name*]
no ip host-list *host-list-name* [**vrf** *vrf-name*]

Syntax Description

host-list-name	List of servers that will receive DDNS updates.
vrf *vrf-name*	(Optional) Identifies the virtual routing and forwarding (VRF) table. The *vrf-name* argument identifies the address pool to which the VRF is associated.

Command Default

No IP host list is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)YA	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Usage Guidelines

The interface configuration overrides the global configuration.

Examples

The following example shows how to configure a list of hosts:

```
ip host-list test
 host vrf testgroup
```

Related Commands

Command	Description
host (host-list)	Specifies a list of hosts that will receive DDNS updates of A and PTR RR.

ip hostname strict

To ensure that Internet hostnames comply with Section 2.1 of RFC 1123, use the **ip hostname strict** command in global configuration mode. To remove the restriction on hostnames, use the **no** form of this command.

ip hostname strict
no ip hostname strict

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default, that is, characters that are not specified in Section 2.1 of RFC 1123 are allowed in hostnames.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2SR	This command was introduced.

Usage Guidelines

Section 2.1 of RFC 1123 specifies the following rules for hostnames:

- A hostname is composed of one or more labels, separated by periods.
- Each label is composed of one or more of the following characters: letters (A-Z, a-z), digits (0-9), and the hyphen (-). No other characters are allowed.
- Alphabetic characters in hostnames can be either uppercase or lowercase, in any combination.
- A hyphen cannot be the first character of any label.
- The most significant label (also described as the top-level domain or TLD), that is, the group of characters that follow the final dot of the domain name, must contain at least one letter or hyphen, and must have least two characters.
- A hostname, including the periods, cannot have more than 255 characters. However, hostnames should not exceed 63 characters because conforming applications might be unable to handle hostnames longer than that.

The following hostnames comply with Section 2.1 of RFC 1123:

- • Name.Example.COM
  • XX
  • 3.example.org
  • 4-.5.9.1.6.US

The following hostnames do not comply with Section 2.1 of RFC 1123:

- • Name.Example.a The TLD “a” is too short.
  • Name.-e.com A label cannot start with “-”.
  • Name_Example.Example.COM “_” is not a valid character.
  • Name.Example..com A label must be at least one character.
  • Example.com. A label must be at least one character.

When the **ip hostname strict** command is configured on a router, any hostname configured on the router must comply with Section 2.1 of RFC 1123, including the following configurations:

- • Router(config)# **hostname router1**
  • Router(config)# **ip domain name domainname1.com**
  • Router(config)# **ip domain list list1.com**
  • Router(config)# **ip host host.example.com 10.0.0.1**
  • Router(config)# **ipv6 host a.example.com 1000::1**

When the **ip hostname strict** command is not configured on a router, characters that are not specified in Section 2.1 of RFC 1123 are allowed in hostnames.

Examples

The following example shows how to specify compliance with Section 2.1 of RFC 1123 for hostnames.

```
Router(config)# ip hostname strict
```

Related Commands

Command	Description
hostname	Defines the hostname for a network server.
ip domain list	Defines a list of default domain names to complete unqualified hostnames.
ip domain name	Defines a default domain name to complete unqualified hostnames.
ip host	Defines static hostname-to-address mappings in the Domain Name System (DNS) hostname cache for a DNS view.
ipv6	Defines a static hostname-to-address mapping in the hostname cache.

ip local-proxy-arp

To enable the local proxy Address Resolution Protocol (ARP) feature, use the **ip local-proxy-arp** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ip local-proxy-arp
no ip local-proxy-arp

Syntax Description

This command has no arguments or keywords.

Command Default

This command is not enabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(5c)EX	This command was introduced on the Catalyst 6500 series switches.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E on the Catalyst 6500 series switches.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines

The local proxy ARP feature allows the Multilayer Switching Feature Card (MSFC) to respond to ARP requests for IP addresses within a subnet where normally no routing is required. With the local proxy ARP feature enabled, the MSFC responds to all ARP requests for IP addresses within the subnet and forwards all traffic between hosts in the subnet. Use this feature only on subnets where hosts are intentionally prevented from communicating directly to the Catalyst 6500 series switch on which they are connected.

Before the local proxy ARP feature can be used, the IP proxy ARP feature must be enabled. The IP proxy ARP feature is enabled by default.

Internet Control Message Protocol (ICMP) redirects are disabled on interfaces where the local proxy ARP feature is enabled.

Examples

The following example shows how to enable the local proxy ARP feature:

```
ip local-proxy-arp
```

ip mobile arp

To enable local-area mobility, use the **ip mobile arp** command in interface configuration mode. To disable local-area mobility, use the **no** form of this command.

ip mobile arp [**timers** *keepalive hold-time*] [**access-group** *access-list-numbername*]
no ip mobile arp

Syntax Description

timers	(Optional) Sets local-area mobility timers.
keepalive	(Optional) Frequency, in minutes, at which the Cisco IOS software sends unicast Address Resolution Protocol (ARP) messages to a relocated host to verify that the host is present and has not moved. The default value is 5.
hold-time	(Optional) Hold time, in minutes. This is the length of time the software considers that a relocated host is present without receiving some type of ARP broadcast or unicast from the host. Normally, the hold time should be at least three times greater than the keepalive time. The default value is 15.
access-group	(Optional) Indicates that you are applying an access list. This access list applies only to local-area mobility.
access-list-number	(Optional) Number of a standard IP access list. The range is from 1 to 99. Only hosts with addresses permitted by this access list are accepted for local-area mobility.
name	(Optional) Name of an IP access list. The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists.

Command Default

Local-area mobility is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
XE 2.5.1	This command was integrated into Cisco IOS XE Release 2.5.1. VRF-awareness for local-area mobility is available in this release.

Usage Guidelines

Local-area mobility is supported on Ethernet, Token Ring, and FDDI interfaces only.

To create larger mobility areas, you must first redistribute the mobile routes into your Interior Gateway Protocol (IGP). The IGP must support host routes. You can use Enhanced IGRP, Open Shortest Path First (OSPF), or

Intermediate System-to-Intermediate System (IS-IS); you can also use Routing Information Protocol (RIP), but RIP is not recommended. The mobile area must consist of a contiguous set of subnets.

Using an access list to control the list of possible mobile nodes is strongly encouraged. Without an access list, misconfigured hosts can be mistaken for mobile nodes and disrupt normal operations.

Examples

The following example shows how to configure local-area mobility on Ethernet interface 0:

```
access-list 10 permit 10.92.37.114
 interface ethernet 0
 ip mobile arp access-group 10
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
default-metric (BGP)	Sets default metric values for the BGP, OSPF, and RIP routing protocols.
default-metric (OSPF)	Sets default metric values for OSPF.
default-metric (RIP)	Sets default metric values for RIP.
network (BGP)	Specifies the list of networks for the BGP routing process.
network (IGRP)	Specifies a list of networks for the IGRP or Enhanced IGRP routing process.
network (RIP)	Specifies a list of networks for the RIP routing process.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
router eigrp	Configures the IP Enhanced IGRP routing process.
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process for IP.
router ospf	Configures an OSPF routing process.

ip name-server

To specify the address of one or more name servers to use for name and address resolution, use the **ip name-server**command in global configuration mode. To remove the addresses specified, use the **no** form of this command.

ip name-server [**vrf** *vrf-name*] *server-address1* [*server-address2...server-address6*]
no ip name-server [**vrf** *vrf-name*] *server-address1* [*server-address2...server-address6*]

Syntax Description

vrf *vrf-name*	(Optional) Defines a Virtual Private Network (VPN) routing and forwarding instance (VRF) table. The *vrf-name* argument specifies a name for the VRF table.
server-address1	IPv4 or IPv6 addresses of a name server.
server-address2...server-address6	(Optional) IP addresses of additional name servers (a maximum of six name servers).

Command Default

No name server addresses are specified.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(2)T	Support for IPv6 addresses was added.
12.0(21)ST	Support for IPv6 addresses was added.
12.0(22)S	Support for IPv6 addresses was added.
12.2(14)S	Support for IPv6 addresses was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.4(4)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Examples

The following example shows how to specify IPv4 hosts 172.16.1.111 and 172.16.1.2 as the name servers:

```
ip name-server 172.16.1.111 172.16.1.2
```

This command will be reflected in the configuration file as follows:

```
ip name-server 172.16.1.111
ip name-server 172.16.1.2
```

The following example shows how to specify IPv4 hosts 172.16.1.111 and 172.16.1.2 as the name servers for vpn1:

```
Router(config)# ip name-server vrf vpn1 172.16.1.111 172.16.1.2
```

The following example shows how to specify IPv6 hosts 3FFE:C00::250:8BFF:FEE8:F800 and 2001:0DB8::3 as the name servers:

```
ip name-server 3FFE:C00::250:8BFF:FEE8:F800 2001:0DB8::3
```

This command will be reflected in the configuration file as follows:

```
ip name-server 3FFE:C00::250:8BFF:FEE8:F800
ip name-server 2001:0DB8::3
```

Related Commands

Command	Description
ip domain-lookup	Enables the IP DNS-based hostname-to-address translation.
ip domain-name	Defines a default domain name to complete unqualified hostnames (names without a dotted decimal domain name).

ip nat

To designate that traffic originating from or destined for the interface is subject to Network Address Translation (NAT), to enable NAT logging, or to enable static IP address support, use the **ip nat**command in interface configuration mode. To prevent the interface from being able to translate or log, use the **no** form of this command.

ip nat [{**inside** | **outside**} | **log** | **translations** | **syslog** | **allow-static-host**]
no ip nat [{**inside** | **outside**} | **log** | **translations** | **syslog** | **allow-static-host**]

Syntax Description

inside	(Optional) Indicates that the interface is connected to the inside network (the network subject to NAT translation).
outside	(Optional) Indicates that the interface is connected to the outside network.
log	(Optional) Enables NAT logging.
translations	(Optional) Enables NAT logging translations.
syslog	(Optional) Enables syslog for NAT logging translations.
allow-static-host	(Optional) Enables static IP address support for NAT translation.

Command Default

Traffic leaving or arriving at this interface is not subject to NAT.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.3(2)XE	The **allow-static-host** keyword was added.
12.3(7)T	This command was implemented in Cisco IOS Release 12.3(7)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

Only packets moving between inside and outside interfaces can be translated. You must specify at least one inside interface and outside interface for each border router where you intend to use NAT.

When static IP address support is enabled with the **ip nat allow-static-host**command, Cisco IOS software will provide a working IP address within the Public Wireless LAN to users configured with a static IP address.

Examples

The following example translates between inside hosts addressed from either the 192.168.1.0 or 192.168.2.0 network to the globally unique 171.69.233.208/28 network:

```
ip nat pool net-208 172.69.233.208 171.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
 ip address 172.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

The following example enables static IP address support for the router at 192.168.196.51:

```
interface ethernet 1
 ip nat inside
ip nat allow-static-host
ip nat pool pool1 172.1.1.1 171.1.1.10 netmask 255.255.255.0 accounting WLAN-ACCT
ip nat inside source list 1 pool net-208
access-list 1 deny ip 192.168.196.51
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
debug ip nat	Displays information about IP packets translated by NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Enables a port other than the default port.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip nat create flow-entries

To enable flow cache entries in Network Address Translation (NAT), use the **ip nat create flow-entries** command in global configuration mode. To disable flow cache entries in NAT, use the **no** form of this command.

ip nat create flow-entries
no ip nat create flow-entries

Syntax Description

This command has no arguments or keywords.

Command Default

Flow cache entries are enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.10S	This command was introduced.

Usage Guidelines

Note Disabling flow cache entries will result in lesser performance as this functionality does multiple database searches to find the most specific translation to use.

By default, Network Address Translation (NAT) creates a session (which is a 5-tuple entry) for every translation. A session is also called a flow cache entry.

Standard NAT and carrier-grade NAT (CGN) translation modes support the disabling of flow cache entries. You can disable flow cache entries in dynamic and static NAT/CGN configurations. Instead of creating sessions, dynamic and static NAT translations can translate a packet from the binding (or bindings, if both inside and outside bindings are available). A binding or a half entry is an association between a local IP address and a global IP address.

Disabling flow cache entries for dynamic and static translations saves memory usage and provides more scalability for your NAT translations.

Note Port Address Translation (PAT) or interface overload does not support disabling of flow cache entries.

Examples

The following example shows how to disable flow cache entries in a dynamic NAT configuration:

```
Device# configure terminal
Device(config)# ip nat pool net-208 172.16.233.208 172.16.233.223 prefix-length 28
Device(config)# access-list 1 permit 192.168.34.0 0.0.0.255
Device(config)# ip nat inside source list 1 pool net-208
Device(config)# no ip nat create flow-entries
```

The following example shows how to enable flow cache entries in a static CGN configuration:

```
Device# configure terminal
Device(config)# ip nat settings mode cgn
Device(config)# ip nat inside source static 192.168.2.1 192.168.34.2
Device(config)# ip nat create flow-entries
```

Related Commands

Command	Description
access-list (IP Extended)	Defines an extended IP access list.
access-list (IP Standard)	Defines a standard IP access list.
ip nat inside source	Enables NAT of the inside source address.
ip nat settings mode cgn	Enables CGN operating mode.

ip nat enable

To configure an interface connecting Virtual Private Networks (VPNs) and the Internet for Network Address Translation (NAT), use the **ip nat enable**command in interface configuration mode.

ip nat enable
no ip nat enable

Syntax Description

This command has no arguments or keywords.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Examples

The following example show how to configure an interface connecting VPNs and the Internet for NAT translation:

```
interface Ethernet0/0
 ip vrf forwarding vrf1
 ip address 192.168.122.1 255.255.255.0
 ip nat enable
```

Related Commands

Command	Description
ip nat pool	Defines a pool of IP addresses for Network Address Translation.
ip nat source	Enables Network Address Translation on a virtual interface without inside or outside specification.

ip nat inside destination

To enable the Network Address Translation (NAT) of a globally unique outside host address to multiple inside host addresses, use the **ip nat inside destination**command inglobal configuration mode. This command is primarily used to implement TCP load balancing by performing destination address rotary translation. To remove the dynamic association to a pool, use the **no** form of this command.

ip nat inside destination list {*access-list-numbername*} **pool** *name* [**redundancy** *redundancy-id* **mapping-id** *map-id*]
no ip nat inside destination list

Syntax Description

list *access-list-number*	Specifies the standard IP access list number. Packets with destination addresses that pass the access list are translated using global addresses from the named pool.
list *name*	Specifies the name of a standard IP access list. Packets with destination addresses that pass the access list are translated using global addresses from the named pool.
pool *name*	Specifies the name of the pool from which global IP addresses are allocated during dynamic translation.
redundancy *redundancy-id*	Specifies the NAT redundancy operation.
mapping-id *map-id*	(Optional) Specifies whether the local Stateful NAT Translation (SNAT) router will distribute a particular set of locally created entries to a peer SNAT router.

Command Default

No inside destination addresses are translated.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
12.3(7)T	This command was modified. The **mapping-id** *map-id* keyword and argument combination was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.4S	This command was modified. The **redundancy** *redundancy-id* keyword and argument pair was added.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

To implement TCP load balancing, you must configure NAT to use rotary pools as specified with the **ip nat pool** command and the **rotary** keyword.

Packets from addresses that match the standard access list are translated using global addresses allocated from the pool named with the **ip nat pool** command.

Examples

The following example shows how to define a virtual address with connections that are distributed among a set of real hosts. The rotary pool defines the addresses of the real hosts. The access list defines the virtual address. If a translation does not already exist, TCP packets from serial interface 0 (the outside interface) whose destination matches the access list are translated to an address from the rotary pool.

```
ip nat pool real-hosts 192.168.15.2 192.168.15.15 prefix-length 28 type rotary
ip nat inside destination list 2 pool real-hosts
!
interface serial 0/0/0
 ip address 192.168.15.129 255.255.255.240
 ip nat outside
!
interface GigabitEthernet 0/0/1
 ip address 192.168.15.17 255.255.255.240
 ip nat inside
!
access-list 2 permit 192.168.15.1
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Enables a port other than the default port.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip nat inside source

To enable Network Address Translation (NAT) of the inside source address, use the **ip nat inside source** command in global configuration mode. To remove the static translation, or the dynamic association to a pool, use the **no** form of this command.

Dynamic NAT

ip nat inside source {**list** {*access-list-number access-list-name*} | **route-map** *name*} {**interface** *type number* | **pool** *name* [**redundancy** *rg-id* **mapping-id** *mapping-id*]} [**no-payload**] [**overload**] [**c**] [**vrf** *name* [**match-in-vrf**]] [**oer**] [**portmap** *name*]

no ip nat inside source {**list** {*access-list-number access-list-name* } | **route-map** *name*} {**interface** *type number* | **pool** *name* [**redundancy** *rg-id* **mapping-id** *mapping-id*]} [**no-payload**] [**overload**] [**reversible**] [**vrf** *name* [**match-in-vrf**]] [**oer**] [**portmap** *name*]

Static NAT

ip nat inside source static {**esp** *local-ip* **interface** *type number* | *local-ip global-ip*} [**extendable**] [**no-alias**] [**no-payload**] [**route-map** *name* [**reversible**]] [**redundancy** {*group-name* | *rg-id* **mapping-id** *mapping-id*}] [**reversible**][**vrf** *name* [**match-in-vrf**] [**forced**] [**garp-interface**]]

no ip nat inside source static {**esp** *local-ip* **interface** *type number* | *local-ip global-ip*} [**extendable**] [**no-alias**] [**no-payload**] [**route-map** *name* [**reversible**]] [**redundancy** {*group-name* | *rg-id* **mapping-id** *mapping-id*}] [**vrf** *name* [**match-in-vrf**] [**forced**] [**garp-interface**]]

Port Static NAT

ip nat inside source static {**tcp** | **udp**} {*local-ip local-port global-ip global-port* [**extendable**] [**forced**] [**no-alias**] [**no-payload**] [**redundancy** {*group-name* | *rg-id* **mapping-id** *mapping-id*}] [**route-map** *name* [**reversible**]] [**vrf** *name* [**match-in-vrf**]] | **interface** *global-port*}

no ip nat inside source static {**tcp** | **udp**} {*local-ip local-port global-ip global-port* [**extendable**] [**forced**] [**no-alias**] [**no-payload**] [**redundancy** {*group-name* | *rg-id* **mapping-id** *mapping-id*}] [**route-map** *name* [**reversible**]] [**vrf** *name* [**match-in-vrf**]] | **interface** *global-port*}

Network Static NAT

ip nat inside source static network *local-network global-network mask* [**extendable**] [**forced**] [**no-alias**] [**no-payload**] [**redundancy** {*group-name* | *rg-id* **mapping-id** *mapping-id*}] [**vrf** *name* [**match-in-vrf**]]

no ip nat inside source static network *local-network global-network mask* [**extendable**] [**forced**] [**no-alias**] [**no-payload**] [**redundancy** {*group-name* | *rg-id* **mapping-id** *mapping-id*}] [**vrf** *name* [**match-in-vrf**]]

Syntax Description

list *access-list-number*	Specifies the number of a standard IP access list. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
list *access-list-name*	Specifies the name of a standard IP access list. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
route-map *name*	Specifies the named route map.
interface	Specifies an interface for the global address.

type	Interface type. For more information, use the question mark (?) online help function.
number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
pool *name*	Specifies the name of the pool from which global IP addresses are allocated dynamically.
no-payload	(Optional) Prohibits the translation of an embedded address or port in the payload.
redundancy	(Optional) Establishes NAT redundancy.
group-name	(Optional) Redundancy group name.
rg-id	(Optional) Redundancy group ID.
mapping-id *mapping-id*	(Optional) Specifies the mapping ID to be associated to NAT high-availability redundancy.
overload	(Optional) Enables the device to use one global address for many local addresses. When overloading is configured, the TCP or UDP port number of each inside host distinguishes between the multiple conversations using the same local IP address.
reversible	(Optional) Enables outside-to-inside initiated sessions to use route maps for destination-based NAT.
vrf *name*	(Optional) Associates the NAT translation rule with a particular VPN routing and forwarding (VRF) instance.
match-in-vrf	(Optional) Enables NAT inside and outside traffic in the same VRF.
oer	(Optional) Allows Optimized Edge Routing (OER) to operate NAT and control traffic class routing.
portmap *name*	(Optional) Specifies the port map to be associated for NAT.
static	Sets up a single static translation.
esp *local-ip*	Establishes the IPsec Encapsulating Security Payload (ESP) (tunnel mode) support.
local-ip	Local IP address assigned to a host on the inside network. The address could be randomly chosen, allocated from RFC 1918, or obsolete.
global-ip	Globally unique IP address of an inside host as it appears to the outside network.
extendable	(Optional) Extends the translation.
forced	(Optional) Forcefully deletes an entry and its children from the configuration.
no-alias	(Optional) Prohibits an alias from being created for the global address.
tcp	Establishes the TCP protocol.

udp	Establishes the UDP protocol.
local-port	Local TCP or UDP port. The range is from 1 to 65535.
global-port	Global TCP or UDP port. The range is from 1 to 65535.
network *local-network*	Specifies the local subnet translation.
global-network	Global subnet translation.
mask	IP network mask to be used with subnet translations.
garp-interface	Initiates GARP messages request.

Command Default

No NAT translation of inside source addresses occurs.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
12.2(4)T	This command was modified to include the ability to use route maps with static translations, and the **route-map** *name* keyword-argument pair was added. This command was modified to include static translation with Hot Standby Routing Protocol (HSRP), and the **redundancy** *group-name* keyword-argument pair was added. This command was modified to enable the translation of the IP header address only, and the **no-payload** keyword was added.
12.2(13)T	This command was modified. The **interface** keyword was added for static translations. The **vrf** *name* keyword-argument pair was added.
12.4(3)T	This command was modified. The **reversible** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(15)T	This command was modified. The **oer** keyword was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRE	This command was modified. The **vrf** *name* keyword-argument pair was removed from Cisco 7600 series routers.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.3(2)T	This command was modified. The *rg-id* argument and the **mapping-id** *mapping-id* keyword-argument pair were added.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Release	Modification
Cisco IOS XE Fuji Release 16.7.1	This command was modified. The **reversible** keyword was added to Static NAT configuration.
Cisco IOS XE 17.13.1a	This command was modified. The **garp-interface** keyword was added to Static NAT configuration to initiate GARP messages on the BD-VIF interface.

Usage Guidelines

The optional keywords of the **ip nat inside source** command can be entered in any order.

For information about the limitations when the **ip nat inside source** command was integrated into Cisco IOS XE Release 2.5, see the Cisco IOS XE 2 Release Notes.

This command has two forms: the dynamic and the static address translation. The form with an access list establishes the dynamic translation. Packets from addresses that match the standard access list are translated using global addresses allocated from the pool named with the **ip nat pool** command.

Packets that enter the device through the inside interface and packets sourced from the device are checked against the access list for possible NAT candidates. The access list is used to specify which traffic is to be translated.

Alternatively, the syntax form with the keyword **static** establishes a single static translation.

Note When a session is initiated from outside with the source IP as the outside global address, the device is unable to determine the destination VRF of the packet. Use the **match-in-vrf** keyword to enable the IP alias installation to work correctly when routing NAT inside and outside traffic in the same VRF.

Note When you configure NAT with a VRF-enabled interface address that acts as the global address, you must configure the **ip nat inside source static no-alias** command. If the **no-alias** keyword is not configured, Telnet to the VRF-enabled interface address fails.

Note Enabling or Initiating GARP for NAT Mapping as a feature using the **ip nat inside source static** command with the '**garp-interface**' option is only applicable to BD-VIF (Bridge Domain-Virtual Interface) interfaces. These interfaces bridge virtualized networks to the ACI fabric, offering essential connectivity for NAT mapping configuration and GARP notifications.

Examples

The following example shows how to translate between inside hosts addressed from either the 192.0.2.0 or the 198.51.100.0 network to the globally unique 203.0.113.209/28 network:

```
ip nat pool net-209 203.0.113.209 203.0.113.222 prefix-length 28
ip nat inside source list 1 pool net-209
!
interface ethernet 0
 ip address 203.0.113.113 255.255.255.240
 ip nat outside
!
```

```
interface ethernet 1
 ip address 192.0.2.1 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.0.2.1 255.255.255.0
access-list 1 permit 198.51.100.253 255.255.255.0
```

The following example shows how to translate the traffic that is local to the provider's edge device running NAT (NAT-PE):

```
ip nat inside source list 1 interface ethernet 0 vrf vrf1 overload
ip nat inside source list 1 interface ethernet 0 vrf vrf2 overload
!
ip route vrf vrf1 10.0.0.1 10.0.0.1 192.0.2.1
ip route vrf vrf2 10.0.0.1 10.0.0.1 192.0.2.1
!
access-list 1 permit 10.1.1.1 0.0.0.255
!
ip nat inside source list 1 interface ethernet 1 vrf vrf1 overload
ip nat inside source list 1 interface ethernet 1 vrf vrf2 overload
!
ip route vrf vrf1 10.0.0.1 10.0.0.1 198.51.100.1 global
ip route vrf vrf2 10.0.0.1 10.0.0.1 198.51.100.1 global
access-list 1 permit 10.1.1.0 0.0.0.255
```

The following example shows how to translate sessions from outside to inside networks:

```
ip nat pool POOL-A 10.1.10.1 10.1.10.126 255.255.255.128
ip nat pool POOL-B 10.1.20.1 10.1.20.126 255.255.255.128
ip nat inside source route-map MAP-A pool POOL-A reversible
ip nat inside source route-map MAP-B pool POOL-B reversible
!
ip access-list extended ACL-A
 permit ip any 10.1.10.128 0.0.0.127
ip access-list extended ACL-B
 permit ip any 10.1.20.128 0.0.0.127
!
route-map MAP-A permit 10
 match ip address ACL-A
!
route-map MAP-B permit 10
 match ip address ACL-B
!
```

The following example shows how to configure the route map R1 to allow outside-to-inside translation for static NAT:

```
ip nat inside source static 10.1.1.1 10.2.2.2 route-map R1 reversible
!
ip access-list extended ACL-A
 permit ip any 10.1.10.128 0.0.0.127
route-map R1 permit 10
 match ip address ACL-A
```

The following example shows how to configure NAT inside and outside traffic in the same VRF:

```
interface Loopback1
 ip vrf forwarding forwarding1
 ip address 192.0.2.11 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
```

```
interface Ethernet0/0
 ip vrf forwarding forwarding2
 ip address 192.0.2.22 255.255.255.0
 ip nat outside
 ip virtual-reassembly
ip nat pool MYPOOL 192.0.2.5 192.0.2.5 prefix-length 24
ip nat inside source list acl-nat pool MYPOOL vrf vrf1 overload
!
!
ip access-list extended acl-nat
 permit ip 192.0.2.0 0.0.0.255 any
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
clear ip nat translation	Clears dynamic NAT translations from the translation table.
interface	Configures an interface type and enters interface configuration mode.
ip access-list	Defines an IP access list or object group access control list by name or number.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Enables a port other than the default port.
ip route vrf	Establishes static routes for a VRF instance.
ip vrf forwarding	Associates a VRF instance with a diameter peer.
match ip-address	Distributes any routes that have a destination network number address that is permitted by a standard access list, an extended access list, or a prefix list, or performs policy routing on packets.
permit	Sets conditions in a named IP access list or object group access control list that will permit packets.
route-map	Defines the conditions for redistributing routes from one routing protocol into another routing protocol, or enables policy routing.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip nat log translations flow-export

To enable the high-speed logging of Network Address Translation (NAT) translations by using a flow exporter, use the **ip nat log translations flow-export** command in global configuration mode. To disable the logging of NAT translations by using a flow exporter, use the **no** form of this command.

ip nat log translations flow-exportv9 udp {**destination** *IPv4address-port* | **ipv6-destination** *ipv6address-port*}[**vrf** *vrf-name* | **source** *interface-name interface-number* | **bind-only**]
no ip nat log translations flow-export

Syntax Description

v9	Specifies the flow exporter Version 9 format.
udp	Specifies the UDP protocol.
destination	Specifies the destination IPv4 address for which translations will be logged.
ipv6-destination	Specifies the destination address for which translations will be logged.
hostname	Name or IPv4 address of the destination.
local-udp-port	Local UDP port number. Valid values are from 1 to 65335.
bind-only	(Optional) Logs only NAT binding translations.
source *interface-type interface-number*	(Optional) Specifies the source interface for which translations will be logged.
vrf *vrf-name*	(Optional) Specifies the destination VRF for which translations will be logged.

Command Default

Logging is disabled for all NAT translations.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was modified. The **bind-only** keyword was added.

Release	Modification
Cisco IOS XE Everest Release 16.6.1	This command was modified. The following keywords were added: • **ipv6-destination** • **vrf**

Usage Guidelines

The volume of data that is logged for NAT bindings translations is significantly reduced when you enable the **bind-only** keyword.

NAT binding is a one-to-one association between a local IP address and a global IP address. When you configure the **ip nat log translations flow-export** command without the **bind-only** keyword, translations for both NAT bindings and NAT sessions are logged. Sessions are identified by the 5-tuple (the source IP address, the destination IP address, the protocol, the source port, and the destination port) information. Sessions are normally created and destroyed at a much faster rate than bindings and, as a result, configuring the **bind-only** keyword can significantly reduce the volume of translation logs.

The **bind-only** keyword is most useful for dynamic NAT configurations without the overload configuration. Overload configurations (also known as Port Address Translation [PAT]) generally produce only sessions and no bindings. Thus, configuring the **bind-only** keyword is not very useful for PAT users.

Examples

The following example shows how to enable translation logging for a specific destination and source interface:

```
Device(config)# ip nat log translations flow-export v9 udp destination 10.10.0.1 1020 source
 gigabithethernet 0/0/1
```

This example shows how to enable high-speed logging using an IPv6 address

```
Device(config)# ip nat log translations flow-export v9 udp ipv6-destination 2001::06 5050
source GigabitEthernet 0/0/0
```

This example shows how to enable high-speed logging using an IPv6 address for a VRF

```
Device(config)# ip nat log translations flow-export v9 udp ipv6-destination 2001::06 5050
vrf hslvrf source GigabitEthernet 0/0/0
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
show ip nat translations	Displays active NAT translations.

ip nat log translations syslog

To enable the high-speed logging of Network Address Translation (NAT) translations to the syslog, use the **ip nat log translation syslog** command in global configuration mode. To disable the logging of NAT translations, use the **no** form of this command.

ip nat log translations syslog [**bind-only**]
no ip nat log translations

Syntax Description

bind-only	(Optional) Logs only NAT binding translations.

Command Default

Logging is disabled for all NAT translations.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was modified. The **bind-only** keyword was added.

Usage Guidelines

The volume of data that is logged for NAT bindings translations is significantly reduced when you enable the **bind-only** keyword.

NAT binding is a one-to-one association between a local IP address and a global IP address. When you configure the **ip nat log translations syslog** command without the **bind-only** keyword, translations for both NAT bindings and NAT sessions are logged. Sessions are identified by the 5-tuple (the source IP address, the destination IP address, the protocol, the source port, and the destination port) information. Sessions are normally created and destroyed at a much faster rate than bindings and, as a result, configuring the **bind-only** keyword can significantly reduce the volume of translation logs.

The **bind-only** keyword is most useful for dynamic NAT configurations without the overload configuration. Overload configurations (also known as Port Address Translation [PAT]) generally produce only sessions and no bindings. Thus, configuring the **bind-only** keyword is not very useful for PAT users.

Examples

The following example shows how to log only NAT bindings translations to the syslog:

```
Device(config)# ip nat log translations syslog bind-only
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
show ip nat translations	Displays active NAT translations.

ip nat outside source

To enable Network Address Translation (NAT) of the outside source address, use the **ip nat outside source** command in global configuration mode. To remove the static entry or the dynamic association, use the **no** form of this command.

Dynamic NAT
ip nat outside source {**list** {*access-list-number access-list-name*} | **route-map** *name*} **pool** *pool-name* [**redundancy** *rg-id* **mapping-id** *mapping-id*] [**vrf** *name*] [**add-route**] [**no-payload**]
no ip nat outside source {**list** {*access-list-number access-list-name*} | **route-map** *name*} **pool** *pool-name* [**redundancy** *rg-id* **mapping-id** *mapping-id*] [**vrf** *name*] [**add-route**] [**no-payload**]

Static NAT
ip nat outside source static *global-ip local-ip* [**vrf** *name* [**match-in-vrf**]] [**add-route**] [**extendable**] [**no-alias**] [**no-payload**] [**redundancy** {*group-name* | *rg-id* **mapping-id** *mapping-id*}]
no ip nat outside source static *global-ip local-ip* [**vrf** *name* [**match-in-vrf**]] [**add-route**] [**extendable**] [**no-alias**] [**no-payload**] [**redundancy** {*group-name* | *rg-id* **mapping-id** *mapping-id*}]

Port Static NAT
ip nat outside source static {**tcp** | **udp**} *global-ip global-port local-ip local-port* [**vrf** *name* [**match-in-vrf**]] [**add-route**] [**extendable**] [**no-alias**] [**no-payload**] [**redundancy** {*group-name* | *rg-id* **mapping-id** *mapping-id*}]
no ip nat outside source static {**tcp** | **udp**} *global-ip global-port local-ip local-port* [**vrf** *name* [**match-in-vrf**]] [**add-route**] [**extendable**] [**no-alias**] [**no-payload**] [**redundancy** {*group-name* | *rg-id* **mapping-id** *mapping-id*}]

Network Static NAT
ip nat outside source static network *global-network local-network mask* [**vrf** *name* [**match-in-vrf**]] [**add-route**] [**extendable**] [**no-alias**] [**no-payload**] [**redundancy** {*group-name* | *rg-id* **mapping-id** *mapping-id*}]
no ip nat outside source static network *global-network local-network mask* [**vrf** *name* [**match-in-vrf**]] [**add-route**] [**extendable**] [**no-alias**] [**no-payload**] [**redundancy** {*group-name* | *rg-id* **mapping-id** *mapping-id*}]

Syntax Description

list *access-list-number*	Specifies the number of a standard IP access list. Packets with source addresses that pass the access list are translated using global addresses from the named pool.
list *access-list-name*	Specifies the name of a standard IP access list. Packets with source addresses that pass the access list are translated using global addresses from the named pool.
route-map *name*	Specifies a named route map.
pool *pool-name*	Specifies the name of the pool from which global IP addresses are allocated.
add-route	(Optional) Adds a static route for the outside local address.
no-payload	(Optional) Prohibits the translation of an embedded address or port in the payload.
vrf *name*	(Optional) Associates the NAT rule with a particular VPN routing and forwarding (VRF) instance.

static	Sets up a single static translation.
global-ip	Globally unique IP address assigned to a host on the outside network by its owner. The address was allocated from the globally routable network space.
local-ip	Local IP address of an outside host as it appears to the inside network. The address was allocated from the address space routable on the inside (RFC 1918, *Address Allocation for Private Internets*).
match-in-vrf	(Optional) Matches the incoming VRF.
extendable	(Optional) Extends the transmission.
no-alias	(Optional) Prohibits an alias from being created for the local address.
redundancy	(Optional) Enables the NAT redundancy operation.
group-name	(Optional) Redundancy group name.
rg-id	(Optional) Redundancy group ID.
mapping-id *mapping-id*	(Optional) Specifies the mapping ID to be associated to NAT high-availability redundancy.
tcp	Establishes the TCP.
udp	Establishes the UDP.
global-port	Port number assigned to a host on the outside network by its owner.
local-port	Port number of an outside host as it appears to the inside network.
static network	Sets up a single static network translation.
global-network	Globally unique network address assigned to a host on the outside network by its owner. The address is allocated from a globally routable network space.
local-network	Local network address of an outside host as it appears to the inside network. The address is allocated from an address space that is routable on the inside network.
mask	Subnet mask for the networks that are translated.

Command Default

No translation of source addresses coming from the outside to the inside network occurs.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.

Release	Modification
12.2(4)T	This command was modified to include static translation with Hot Standby Routing Protocol (HSRP), and the **redundancy** *group-name* keyword-argument pair was added. This command was modified to enable the translation of the IP header address only, and the **no-payload** keyword was added.
12.2(13)T	This command was modified. The **vrf** *name* keyword-argument pair was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.3(2)T	This command was modified. The *rg-id* argument and the **mapping-id** *mapping-id* keyword-argument pair were added.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

The optional keywords of the **ip nat outside source** command except for the **vrf** *name* keyword can be entered in any order.

For information about the limitations when this command was integrated into Cisco IOS XE Release 2.5, see the Cisco IOS XE 2 Release Notes.

You can use NAT to translate inside addresses that overlap with outside addresses. Use this command if your IP addresses in the stub network happen to be legitimate IP addresses belonging to another network, and you need to communicate with those hosts or devices.

This command has two general forms: dynamic and static address translation. The form with an access list establishes dynamic translation. Packets from addresses that match the standard access list are translated using global addresses allocated from the pool that is named by using the **ip nat pool** command.

Alternatively, the syntax form with the **static** keyword establishes a single static translation.

The **match-in-vrf** keyword is supported with the **ip nat outside source static** command. The **match-in-vrf** keyword is not supported with the dynamic NAT configuration.

When you configure the **ip nat outside source static** command to add static routes for static outside local addresses, there is a delay in the translation of packets and packets are dropped. To avoid dropped packets, configure either the **ip nat outside source static add-route** command or the **ip route** command.

Examples

The following example shows how to translate between inside hosts addressed from the 10.114.11.0 network to the globally unique 10.69.233.208/28 network. Further, packets from outside hosts addressed from the 10.114.11.0 network (the true 10.114.11.0 network) are translated to appear to be from the 10.0.1.0/24 network.

```
ip nat pool net-208 10.69.233.208 10.69.233.223 prefix-length 28
ip nat pool net-10 10.0.1.0 10.0.1.255 prefix-length 24
ip nat inside source list 1 pool net-208
ip nat outside source list 1 pool net-10
!
interface ethernet 0
 ip address 10.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 10.114.11.39 255.255.255.0
 ip nat inside
!
access-list 1 permit 10.114.11.0 0.0.0.255
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
clear ip nat translation	Clears dynamic NAT from the translation table.
interface	Configures an interface type and enters interface configuration mode.
ip address	Sets a primary or secondary IP address for an interface.
ip nat	Designates the traffic originating from or destined for the interface as subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Enables a port other than the default port.
ip route	Establishes static routes.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NATs.

ip nat piggyback-support

To enable a Network Address Translation (NAT) optimized Session Initiation Protocol (SIP) media path, use the **ip nat piggyback-support** commandinglobal configuration mode.

ip nat piggyback-support sip {**all-messages** | **sdp-only**} **router** *router-id* [**authentication** *authentication-key*]
no ip nat piggyback-support sip {**all-messages** | **sdp-only**} **router** *router-id* [**authentication** *authentication-key*]

Syntax Description

sip	SIP protocol algorithm.
all-messages	Establishes piggybacking in all messages except Session Description Protocol (SDP).
sdp-only	Establishes piggybacking in SDP only.
router *router-id*	Piggyback router ID number.
authentication *authentication-key*	(Optional) Specifies the MD5 authentication key.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced.

Examples

The following example shows how to configure a NAT optimized SIP media path with SDP:

```
ip nat piggyback-support sip sdp-only router 100 authentication md5-key
```

Related Commands

Command	Description
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Changes the amount of time after which NAT translations time out.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip nat pool

To define a pool of IP addresses for Network Address Translation (NAT) translations, use the **ip nat pool** command in global configuration mode. To remove one or more addresses from the pool, use the **no** form of this command.

ip nat pool *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*} [**add-route**] [**type** {**match-host** | **rotary**}] [**accounting** *list-name*] [**arp-ping**] [**no-alias**] [**nopreservation**]
no ip nat pool *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*} [**add-route**] [**type** {**match-host** | **rotary**}] [**accounting** *list-name*] [**arp-ping**] [**no-alias**] [**nopreservation**]

Syntax Description

name	Name of the pool.
start-ip	Starting IP address that defines the range of addresses in the address pool.
end-ip	Ending IP address that defines the range of addresses in the address pool.
netmask *netmask*	Specifies the network mask that indicates the address bits that belong to the network and subnetwork fields and the ones that belong to the host field. • Specify the network mask of the network to which the pool addresses belong.
prefix-length *prefix-length*	Specifies the number that indicates how many bits of the address is dedicated for the network.
add-route	(Optional) Specifies that a route is added to the NAT Virtual Interface (NVI) for the global address.
type	(Optional) Indicates the type of pool.
match-host	(Optional) Specifies that the host field of an IP address must remain the same after translation.
rotary	(Optional) Specifies that the range of addresses in the address pool identifies the real inside hosts among which TCP load distribution will occur.
accounting *list-name*	(Optional) Specifies the RADIUS profile name that matches the RADIUS configuration in the router.
arp-ping	(Optional) Determines static IP client instances and restarts the NAT entry timer.
no-alias	(Optional) Specifies to not create an alias for the address pool.
nopreservation	(Optional) Enables all IP addresses in the pool to be used for dynamic translation.

Command Default No pool of addresses is defined.

Command Modes Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
12.3(2)XE	This command was modified. The **accounting** keyword and the *list-name* argument were added.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.3(14)T	This command was modified. The **add-route** keyword was added.
12.4(6)T	This command was modified. The **arp-ping** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified. The **nopreservation** keyword was added.
Cisco IOS XE Release 3.6S	This command was modified. The **accounting** keyword and the *list-name* argument were removed.
15.2(4)M	This command was modified. The **no-alias** keyword was added.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines This command defines a pool of addresses by specifying the start address, the end address, and either network mask or prefix length.

When you enable the **no-alias** keyword, IP aliases are not created for IP addresses mentioned in the NAT pool.

Using the **nopreservation** keyword with the **prefix-length** or the **netmask** keyword disables the default behavior, which is known as IP address reservation. The **no** form of the command with the **nopreservation** keyword enables the default behavior and reserves the first IP address in the NAT pool, making the IP address unavailable for dynamic translation.

Examples The following example shows how to translate between inside hosts addressed from either the 192.168.1.0 or 192.168.2.0 network to the globally unique 10.69.233.208/28 network:

```
ip nat pool net-208 10.69.233.208 10.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
```

```
!
interface ethernet 0
 ip address 10.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

The following example shows how to add a route to the NVI interface for the global address:

```
ip nat pool NAT 192.168.25.20 192.168.25.30 netmask 255.255.255.0 add-route
ip nat source list 1 pool NAT vrf group1 overload
```

Related Commands

Command	Description
access-list	Defines a standard IP access list.
clear ip nat translation	Clears dynamic NAT translations from the translation table.
debug ip nat	Displays information about IP packets translated by NAT.
interface	Configures an interface and enters interface configuration mode.
ip address	Sets a primary or secondary IP address for an interface.
ip nat	Designates that traffic originating from or destined for an interface is subject to NAT.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat service	Enables a port other than the default port.
ip nat source	Enables NAT on a virtual interface without inside or outside specification.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip nat service

To specify a port other than the default port, use the **ip nat service**command in global configuration mode. To disable the port, use the **no** form of this command.

ip nat service dns-v6 {**H225** | **allow-h323-even-rtp-ports** | **allow-h323-keepalive** | **allow-sip-even-rtp-ports** | **allow-skinny-even-rtp-ports** | **fullrange** {**tcp** | **udp**} **port** *port-number* | **list** {*access-list-numberaccess-list-name*} {**ESP spi-match** | **IKE preserve-port** | **ftp tcp port** *port-number*} | **alg** {**tcp** | **udp**} **dns** | **allow-multipart** | **mgcp** | **enable-mib** | **nbar** | **port-randomization** | **ras** | **rtsp** | **sip** {**tcp** | **udp**} **port** *port-number* | **skinny tcp port** *port-number*}
no ip nat service dns-v6 {**H225** | **allow-h323-even-rtp-ports** | **allow-h323-keepalive** | **allow-sip-even-rtp-ports** | **allow-skinny-even-rtp-ports** | **fullrange** {**tcp** | **udp**} **port** *port-number* | **list** {*access-list-numberaccess-list-name*} {**ESP spi-match** | **IKE preserve-port** | **ftp tcp port** *port-number*} | **alg** {**tcp** | **udp**} **dns** | **allow-multipart** | **mgcp** | **enable-mib** | **nbar** | **port-randomization** | **ras** | **rtsp** | **sip** {**tcp** | **udp**} **port** *port-number* | **skinny tcp port** *port-number*}

Syntax Description

H225	Specifies the H.323 to H.225 protocol.
allow-h323-even-rtp-ports	Specifies the even-numbered Real-time Transport Protocol (RTP) ports for the H.323 protocol.
allow-h323-keepalive	Specifies the H.323 keepalive.
allow-sip-even-rtp-ports	Specifies the even-numbered RTP ports for the Session Initiation Protocol (SIP).
allow-skinny-even-rtp-ports	Specifies the even-numbered RTP ports for the skinny protocol.
fullrange	Specifies all the available ports. The range is from 1024 to 65535.
tcp	Specifies the TCP protocol. A maximum of 16 TCP ports can be configured.
udp	Specifies the UDP protocol. A maximum of 16 UDP ports can be configured.
port *port-number*	Specifies the port other than the default port in the range from 1 to 65533.
list *access-list-number*	Specifies the standard access list number in the range from 1 to 199.
access-list-name	Name of a standard IP access list.
ESP	Specifies the Security Parameter Index (SPI) matching IPsec pass-through.
spi-match	Specifies the SPI matching IPsec pass-through. The ESP endpoints must also have SPI matching enabled.
IKE	Preserves the Internet Key Exchange (IKE) port, as required by some IPsec servers.
preserve-port	Preserves the UDP port in IKE packets.
ftp	Specifies FTP.

alg {**tcp** | **upd**} **dns**	Enables Domain Name System (DNS) processing with an Application-Level Gateway (ALG) for either TCP or UDP.
allow-multipart	Enables SIP multipart processing.
mgcp	Specifies the Media Gateway Control Protocol (MGCP).
enable-mib	Enables NAT MIB support.
nbar	Enables network-based application recognition (NBAR).
port-randomization	Specifies that ports are allocated randomly for Network Address Translation (NAT), instead of sequentially.
ras	Specifies the H.323-Registration, Admission, and Status (RAS) protocol.
rtsp	Specifies the Real Time Streaming Protocol (RTSP). This protocol is enabled by default on port 554 and requires NBAR.
sip	Specifies SIP. This protocol is enabled by default on port 5060.
skinny	Specifies the skinny protocol.
dns-v6	Specifies if IPv6 DNS packets should be processed by ALG.

Command Default

DNS ALG processing is enabled for TCP and UDP. H.323 even-numbered RTP port allocation is enabled. Port randomization is disabled. RTSP is enabled and requires NBAR. Skinny even-numbered RTP port allocation is enabled. UDP SIP even-numbered RTP port allocation is enabled. UDP SIP is enabled on port 5060. UDP SIP multipart processing is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3	This command was introduced.
12.1(5)T	This command was modified. The **skinny** keyword was added.
12.2(8)T	This command was modified. The **sip** keyword was added.
12.2(15)T	This command was modified. The **ESP**and **spi-match**keywords were added to enable SPI matching on outside IPsec gateways. The **ike** and **preserve-port** keywords were added to enable outside IPsec gateways that require IKE source port 500.
12.3(7)T	This command was modified. The **rtsp** and **mgcp** keywords were added.
12.3(11)T	This command was modified. The **allow-sip-even-rtp-ports**keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4	This command was modified. The **nbar** keyword was added.

Release	Modification
12.4(24)T	This command was modified. The **port-randomization** keyword was added.
15.0(1)M	This command was modified. The **alg**, **dns**, and **allow-multipart** keywords were added.
15.0(1)M2	This command was modified. The **enable-mib** keyword was added.
15.1(1)T2	This command was modified. The **tcp** keyword used along with the **sip** keyword was removed.
15.0(1)M3	This command was modified. The **enable-mib** keyword was removed.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.
16.7.1	This command was modified. The **dns-v6** keyword is added.
16.8.1	This command was modified. The **fullrange** keyword is enhanced to configure the local port with a global port in the high range (1024-65535).

Usage Guidelines

A host with an FTP server using a port other than the default port can have an FTP client using the default FTP control port. When a port other than the default port is configured for an FTP server, Network Address Translation (NAT) prevents FTP control sessions that are using port 21 for that particular server. If an FTP server uses the default port and a port other than the default port, both ports need to be configured using the **ip nat service** command.

NAT listens on the default port of the Cisco CallManager to translate the skinny messages. If the Cisco CallManager uses a port other than the default port, that port needs to be configured using the **ip nat service** command.

Use the **no ip nat service H225** command to disable support of H.225 packets by NAT.

Use the **no ip nat service allow-h323-even-rtp-ports**command to force odd-numbered RTP port allocation for H.323.

Use the **no ip nat service allow-sip-even-rtp-ports**command to force odd-numbered RTP port allocation for SIP.

Use the **no ip nat service allow-skinny-even-rtp-ports**command to force odd-numbered RTP port allocation for the skinny protocol.

Use the **no ip nat service rtsp** command to disable support of RTSP packets by NAT. RSTP uses port 554.

By default SIP is enabled on port 5060; therefore NAT-enabled devices interpret all packets on this port as SIP call messages. If other applications in the system use port 5060 to send packets, the NAT service may corrupt the packet as it attempts to interpret the packet as a SIP call message.

A NAT-enabled Cisco device that is running Cisco IOS Release 12.3(7)T or a later release may experience an increase in CPU usage when upgrading from a previous release. RTSP and MGCP NAT ALG support was added in Cisco IOS Release 12.3(7)T, which requires NBAR. You can use the **no ip nat service nbar** command to disable NBAR processing, which can decrease the CPU utilization rate.



Note If the **no ip nat service nbar** command is not specified during the startup of the router, results in the crashing of the router, when loading the configuration from the TFTP during the booting process.

The **port-randomization** keyword can be used to prevent a security threat caused by the possibility of of predicting the next port number that NAT will allocate. This security threat is described in the Cisco Security Advisory titled Multiple Cisco Products Vulnerable to DNS Cache Poisoning Attacks . Port randomization has the following limitations:

- It cannot be used with certain other NAT features, including port map, full-range, and Secure Network Address Translation (SNAT).
- It is supported only for the port in the Layer 4 header of the packet.

Use the **ip nat service allow-multipart** command to enable the processing of SIP multipart Session Description Protocol (SDP) packets.

NAT MIB support is turned off by default to avoid breakpoint exception crashes. To enable NAT MIB support, use the **enable-mib** keyword.

Examples

The following example shows how to configure the nonstandard port 2021:

```
ip nat service list 10 ftp tcp port 2021
access-list 10 permit 10.1.1.1
```

The following example shows how to configure the standard FTP port 21 and the nonstandard port 2021:

```
ip nat service list 10 ftp tcp port 21
ip nat service list 10 ftp tcp port 2021
access-list 10 permit 10.1.1.1
```

The following example shows how to configure the 20002 port of the Cisco CallManager:

```
ip nat service skinny tcp port 20002
```

The following example shows how to configure TCP port 500 of the third-party concentrator:

```
ip nat service list 10 IKE preserve-port
```

The following example shows how to configure SPI matching on the endpoint routers:

```
ip nat service list 10 ESP spi-match
```

The following example shows how to configure local port translating to the global port in the high range:

```
ip nat service fullrange udp port 53
ip nat service fullrange udp port 123
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.

Command	Description
ip nat outside source	Enables NAT of the outside source address.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip nat service dns-reset-ttl

To reset the time-to-live (TTL) value of Domain Name System (DNS) resource records that pass through Network Address Translation (NAT) to zero, use the **ip nat service dns-reset-ttl** command in global configuration mode. To prevent the TTL value of DNS resource records (RRs) from being set to zero, use the **no** form of this command.

ip nat service dns-reset-ttl
no ip nat service dns-reset-ttl

Syntax Description

This command has no arguments or keywords.

Command Default

The TTL value is set to zero for DNS RRs that pass through NAT.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 3.6S	This command was integrated into Cisco IOS XE Release 3.6S.

Usage Guidelines

RFC 2694, *DNS extensions to Network Address Translators (DNS_ALG)*, states that the TTL value supplied in original RRs for static address assignments is left unchanged. For dynamic address assignments, the DNS application-level gateway (ALG) modifies the TTL value to zero, so that RRs are used only for transactions in progress and are not cached. RFC 2181, *Clarifications to the DNS Specification*, requires all RRs in an RRset (RRs with the same name, class, and type, but with different RDATA) to have the same TTL value. If the TTL value of an RR is set to zero, all other RRs within the same RRset are adjusted by the DNS ALG to be zero.

The **ip nat service dns-reset-ttl** command allows you to modify the behavior of the DNS ALG. The TTL values of all DNS RRs that pass through NAT are set to zero by default, and DNS servers or clients cannot cache temporarily assigned RRs. Use the **no ip nat service dns-reset-ttl** command to prevent the TTL value from being set to zero.

Use a TTL value of zero to prevent nonauthoritative servers from caching DNS RRs, when changing the IP address of a server. A nonzero value for DNS RRs enables remote name servers to cache the DNS RR information for a longer period of time, thereby reducing the number of queries for the RR and lengthening the amount of time required to proliferate RR changes simultaneously.

Examples

The following example shows how to prevent DNS RRs that pass through NAT from having their TTL values set to zero:

```
Router(config)# no ip nat service dns-reset-ttl
```

The following example shows how to set the value of DNS RRs that pass through NAT to zero:

```
Router(config)# ip nat service dns-reset-ttl
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
debug ip nat	Displays information about IP packets translated by NAT.
ip dns primary	Configures the router as authoritative for a zone.
ip dns server	Enables a DNS server on a router.
ip host	Defines static hostname-to-address mappings in the DNS hostname cache for a DNS view.
ip name-server	Specifies the address of one or more name servers to be used for name and address resolution.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT; enables NAT logging; or enables static IP address support.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Specifies a port other than the default port for NAT.
show ip dns primary	Displays the authority record parameters configured for the DNS server.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip nat service enable-sym-port

To enable the endpoint agnostic port allocation, use the **ip nat service enable-sym-port** command in global configuration mode. To disable the endpoint agnostic port allocation, use the no form of this command.

ip nat service enable-sym-port
no ip nat service enable-sym-port

Syntax Description

This command has no arguments or keywords.

Command Default

If you do not issue this command, the endpoint agnostic port allocation is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

Use the **ip natserviceenable-sym-port** command to enable the endpoint agnostic port allocation, which is also known as symmetric port allocation.

Note Use this command before you enable Network Address Translation (NAT). If you enable the symmetric port database after creating entries in the NAT database, then corresponding entries are not added to the symmetric port database.

Examples

In the following example, an access list is created and the inside source address is translated using NAT. The endpoint agnostic port allocation is enabled after the inside source address is translated.

```
Router(config)# interface Ethernet 0/0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# access list 1 permit 172.18.192.0 0.0.0.255
Router(config)# ip nat inside source list 1 interface Ethernet 0/0
Router(config)# ip nat service enable-sym-port
Router(config)# end
```

Following are the list of entries which are made to the SymmetricPort (Sym Port) table, debugs, and Symmetric DB (Sym DB) when the command is issued and when the command is not entered:

```
NAT Symmetric Port Database: 1 entries
public ipaddr:port [tableid] | port# [refcount][syscount] | localaddr:localport [flags]
172.18.192.69:1024 [0] | 1025 [1] [0] | 172.18.192.69:1024 [0]
Sample SymPort Debugs:
If SymDB is not enabled or initiated:
NAT-SymDB: DB is either not enabled or not initiated.
If an entry needs to be inserted into SymDB:
NAT-SymDB: insert 172.18.192.69 1024 0
172.18.192.69 is the local address, 1024 is the local port, and 0 is the tableid
If SymDB lookup found an entry:
NAT-SymDB: [0] Entry was found for 172.18.192.69 -> 10.10.10.1: wanted 1024 got 1025
```

```
172.18.192.69 is the local address, 10.10.10.1 is the global address, 1024 is the requested
 port, and 1025 is the allocated port
If entry was deleted from SymDB:
NAT-SymDB: deleting entry 172.18.192.69:1024
172.18.192.69 is the local address, 1024 is the local port.
```

Related Commands

Command	Description
show ip nat translations	Displays the list of translations entries.
show ip nat statistics	Displays the entries in the symmetric port database

ip nat service gatekeeper

To prevent non-NAT packet flows from using excessive CPU for NAT translation, use the **ip nat service gatekeeper** command in global configuration mode. To disable the gatekeeper, use the **no** form of this command.

ip nat service gatekeeper
no ip nat service gatekeeper

Syntax Description

This command has no arguments or keywords.

Command Default

NAT gatekeeper is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)	This command was introduced from Cisco IOS Release 12.2.

Examples

The following example shows how to configure the gatekeeper for NAT:

```
Device(config)# ip nat service gatekeeper
Device(config)# end
Gatekeeper on
```

The following example shows how to disable the gateekeeper for NAT:

```
Device(config)# no ip nat service gatekeeper
Device(config)# end
Gatekeeper off
```

ip nat service ipsec-esp enable

To enable IPsec packet processing using ESP, use the **ip nat service ipsec-esp enable** command in global configuration mode. To disable IPsec packet processing using ESP, use the **no** form of this command.

ip nat service ipsec-esp enable
noip nat service ipsec-esp enable

Syntax Description

This command has no arguments or keywords.

Command Default

By default IPsec packet processing using ESP is turned off.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.5(2)S	This command was introduced.

Examples

The following example shows how to use this command to enable IPsec packet processing using ESP:

```
Router(config)#  ip nat service ipsec-esp enable
```

ip nat service pptp

To enable Point-to-Point Tunneling Protocol (PPTP) application-layer gateway (ALG) translation for an application, use the **ip nat service pptp** command in global configuration mode. To disable the PPTP ALG translation for an application, use **no** form of this command.

ip nat service pptp
no ip nat service pptp

Syntax Description

This command has no arguments or keywords.

Command Default

PPTP ALG translation is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.

Usage Guidelines

PPTP ALG translation is enabled by default, when Network Address Translation (NAT) is configured.

Only Port Address Translation (PAT), also known as overload, uses the PPTP ALG. In static and dynamic NAT translations, the PPTP traffic is translated without the requirement of an ALG. PAT maps multiple unregistered internal addresses to only one or a few external addresses by using port numbers.

The following example shows how to disable PPTP ALG translation:

```
Device(config)# no ip nat service pptp
```

Related Commands

ip nat service	Specifies a port other than the default port.

ip nat settings gatekeeper-size

To configure cache for NAT, use **ip nat settings** *gatekeeper-size* command in global configuration mode. To disable the mode, use the **no** form of this command.

ip nat settings gatekeeper-size *gatekeeper-size*
no ip nat settings gatekeeper-size *gatekeeper-size*

Syntax Description

gatekeeper-size	Specifies the cache size.

Command Default

NAT gatekeeper is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2 SRA	This command was introduced from Cisco IOS Release 12.2 SRA.

Usage Guidelines

The extended mode for NAT allows the NAT gatekeeper to cache the source and the destination addresses. You can specify the required cache size based on the requirement when there is a non-NAT traffic on a NAT interface.

Examples

The following example shows how to configure the cache size for NAT gatekeeper:

```
Device(config)# ip nat settings gatekeeper-size 1024
Device(config)# end
```

ip nat settings mode

To enable the Network Address Translation (NAT) operating mode, use the **ip nat settings mode** command in global configuration mode. To disable the NAT operating mode, use the **no** form of this command.

ip nat settings mode {**cgn** | **default**}
no ip nat settings mode

Syntax Description

cgn	Enables the Carrier Grade NAT (CGN) operating mode.
default	Enables the default NAT operating mode.

Command Default

The default NAT operating mode is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.6S	This command was introduced.

Usage Guidelines

In CGN mode, the **ip nat inside destination** command is not supported.

Note We recommend the use of CGN mode for environments in which outside mapping translations are not required, but a large number of inside mappings are required.

Examples

The following example shows how to enable the CGN mode:

```
Router(config)# ip nat settings mode cgn
```

Related Commands

Command	Description
ip nat inside destination	Enables NAT of a globally unique outside host address to multiple inside host addresses.
ip nat settings support mapping outside	Configures NAT outside mapping support.

ip nat settings pap

To configure Network Address Translation (NAT) paired-address-pooling configuration mode, use the **ip nat settings pap** command in global configuration mode. To remove NAT paired-address-pooling configuration mode, use the **no** form of this command.

ip nat settings pap [**limit** {**1000** | **120** | **250** | **30** | **500** | **60**}] [**bpa**] [**set-size** *set-size*] [**step-size** *step-size*] [**single-set**]
no ip nat settings pap

Syntax Description

limit	(Optional) Limits the number of local addresses that you can use per global address.
1000	(Optional) Configures a limit of 1000 local addresses per global address by using an average of 64 ports.
120	(Optional) Configures a limit of 120 local addresses per global address by using an average of 512 ports. This is the default.
250	(Optional) Configures a limit of 250 local addresses per global address by using an average of 256 ports.
30	(Optional) Configures a limit of 30 local addresses per global address by using an average of 2048 ports.
500	(Optional) Configures a limit of 500 local addresses per global address by using an average of 128 ports.
60	(Optional) Configures a limit of 60 local addresses per global address by using an average of 1024 ports.
bpa	(Optional) Configures bulk logging and port-block allocation for carrier-grade NAT (CGN).
set-size *set-size*	(Optional) Configures the number of ports in each port block. Valid values for the *set-size* argument are 1024, 128, 2048, 256, 512, and 64. The default is 512.
step-size *step-size*	(Optional) Configures the step size for a port block. Valid values for the *step-size* argument are 1, 2, 4, and 8.
single-set	(Optional) Configures a single port set.

Command Default

Standard NAT configuration mode is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.
Cisco IOS XE Release 3.10S	This command was modified. The **bpa** and **single-set** keywords and the **set-size** *set-size* and **step-size** *step-size* keyword-argument pairs were introduced.

Usage Guidelines

The ability of NAT to consistently represent a local IP address as a single global IP address is termed paired-address pooling. A local address is any address that appears on the inside of a network and a global address is any address that appears on the outside of the network.

If you change NAT configuration mode to paired-address-pooling configuration mode and vice versa, all existing NAT sessions are removed.

Paired-address pooling is supported only on Port Address Translation (PAT).

When you use the **no** form of this command, both paired-address pooling and bulk logging and port-block allocation modes are removed.

Bulk logging and port-block allocation mode allocates a block of ports for translation instead of allocating individual ports. This reduces the volume of messages logged through high-speed logging (HSL). The reduction of HSL messages is accomplished by dynamically allocating (based on data traffic) a block of global ports instead of a single global port to users.



Note Bulk logging and port-block allocation mode can be enabled only in carrier-grade NAT (CGN) mode. When you change any bulk logging and port-block allocation commands, all existing translations are torn down.

Bulk logging and port-block allocation uses a scattered port set method where a start port, a step value, and number of ports are used for bulk allocation of ports. For example, if the starting port number is 4000, the step value is 4,and the number of ports is 512, then the step value of 4 is added to 4000 to get the second port, again 4 is added to 4004 to get the third port and so on, till you have 512 ports in the port-set.

Port-set size determines the number of ports allocated in each port block. The step size is the number that is added to the previous port in a block to get the next port. The **single-set** keyword limits the number of port-sets to one per user

The default port size can differ based on the paired-address pooling limit that is configured .The following table provides information of the default port size when various paired-address pooling limit is configured:

Table 3: Default Port Size based on Paired-Address Pooling Support

Paired-Address Pooling	Default Port Set Size	Maximum Port Step Size
1000	64 ports	16
120	512 ports	8
250	256 ports	4
30	2048 ports	2
500	128 ports	8
60	1024 ports	4

Valid values available for the *set-size* argument are based on the configured paired-address pooling limit. The following table provides the paired-address pooling limit and the available set sizes:

Table 4: Paired-Address Pooling Limit and Available Set Sizes

Paired-Address Pooling Limit	Set Size
1000	1024, 128, 2048, 256, 512, and 64
120	1024, 2048, and 512
250	1024, 2048, 256, and 512
30	2048
500	1024, 128, 2048, 256, and 512
60	1024 and 2048

Valid values available for the *step-size* argument are based on the configured set-size. The following table provides the set size and the available step sizes:

Table 5: Port-Set Sizes and Available Step Sizes

Set-size	Step Size
1024	1, 2, and 4
2048	1 and 2
512	1, 2, 4, and 8

Examples

The following example shows how to configure paired-address-pooling mode:

```
Device# configure terminal
Device(config)# ip nat settings pap
```

The following example shows how to configure paired-address pooling limit and bulk logging and port-block allocation:

```
Device# configure terminal
Device(config)# ip nat settings mode cgn
Device(config)# ip nat settings mode pap limit 1000 2048 step-size 2 single-set
```

Related Commands

Command	Description
ip nat settings mode	Enables the default NAT operating mode.
ip nat settings mode cgn	Enables CGN operating mode.

ip nat settings pool watermark

To enable the configuration of threshold limits for address pool, use the **ip nat settings pool watermark** command in global configuration mode. To disable the threshold limit, use the **no** form of this command..

ip nat settings pool watermark high*number in percentage*
[low*number in percentage*]
no ip nat settings scale bind

Syntax Description:

This command has no arguments or keywords

Command Default

If the threshold limits are not configured, syslogs are generated after the address pool is exhausted.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.8 Release	This command was introduced.

Examples

The following example shows how to enable threshold levels:

```
Device# configure terminal
Device(config)# ip nat settings pool watermark high 80 low 50
```

ip nat settings redundancy optimized-data-sync

To enable optimization of NAT entries synchronization in a high-availability setup, use the **ip nat settings redundancy optimized-data-sync** command in global configuration mode.

To disable the optimization of data synchronization, use the **no** form of this command.

ip nat settings redundancy optimized-data-sync
no ip nat settings redundancy optimized-data-sync

Note The feature enabled by the **ip nat settings redundancy optimized-data-sync** command is supported in Autonomous mode and is compatible with both classic NAT and CGN operational modes, but not in SD-WAN environments.

Syntax Description

redundancy optimized-data-sync	Specifies the optimization of data synchronization for NAT entries in high-availability configurations to reduce system load during the synchronization process.

Command Default

By default, the optimization of NAT entries synchronization in a redundant setup is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 17.15.1a	This command was introduced.

Usage Guidelines

This command is applicable specifically for B2B (box-to-box) high-availability deployments and is used to reduce the system load during the synchronization process of NAT entries between two high-availability peers.

To maintain service continuity and data integrity, it is critical to ensure full synchronization of control and data TCP connections to the standby router before performing a switchover.

After applying optimized data synchronization, it is important to verify that active and standby sessions are consistent, especially for redundancy group 1, and address any discrepancies promptly to maintain the accuracy of NAT session states.

The cooperation of this feature with the NAT gatekeeper is necessary to manage the NAT resources and synchronization correctly.

The **preempt** CLI option within the redundancy group configuration should be avoided with NAT, as it can lead to unpredictable behavior without providing any tangible benefits.

Even during standby reloads, redundancy sessions are expected to sync, maintaining consistency in redundancy capabilities.

Any inconsistencies between active and standby sessions, particularly after a reload with the optimized data sync feature, need to be promptly addressed to ensure the accurate state of NAT sessions. When the data link

on the standby router is shut down, sessions should not falsely display as synced, to prevent misinterpretation of the redundancy state.

Furthermore, upon the removal of the optimized-data-sync configuration, the synced sessions should become visible on the active router, confirming that the optimization feature has been deactivated.



Note For the feature to function correctly from the Cisco IOS XE 17.15.1a release, the **ip nat settings redundancy optimized-data-sync** command must be configured on both the active and standby routers. It is not supported to configure this command on only one router in a redundant pair. Furthermore, a system reload may be required for the command to take effect if it is configured or changed.

Examples

The following example shows how to enable optimized data synchronization for NAT entries in a high-availability setup:

```
Device# configure terminal
Device(config)# ip nat settings redundancy optimized-data-sync
```

ip nat settings scale bind

To configure CGN NAT to scale to a higher number of translations on ESP200, use the **ip nat settings scale bind** command in global configuration mode. To remove increased scaling on ESP200, use the **no** form of this command.

ip nat settings scale bind
no ip nat settings scale bind

Syntax Description:

This command has no arguments or keywords

Command Default

This command is disabled by default.

Command Modes

Global configuration (config)

Usage Guidelines

The **ip nat settings scale bind** command must be configured before NAT is configured. If the **ip nat settings scale bind** is configured after NAT is configured, the router must be restarted for the changes to take effect.

Note We recommend the use of CGN mode for environments in which outside mapping translations are not required, but a large number of inside mappings are required.

Command History

Release	Modification
Cisco IOS XE Polaris 16.8	This command was introduced.

Examples

The following example shows how to use **ip nat settings scale bind** command:

```
Device# configure terminal
Device(config)# ip nat settings scale bind
```

ip nat settings support mapping outside

To configure the Network Address Translation (NAT) outside mapping support, use the **ip nat settings support mapping outside** command in global configuration mode. To remove all existing outside mapping configuration, use the **no** form of this command.

ip nat settings support mapping outside
no ip nat settings support mapping outside

Syntax Description

This command has no arguments or keywords.

Command Default

NAT outside mapping is supported by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.6S	This command was introduced.

Usage Guidelines

If you have configured NAT in the default mode, use the **ip nat settings mode cgn** command to change your NAT configuration to Carrier Grade NAT (CGN) mode. While changing your NAT configuration to CGN mode, use the **ip nat settings support mapping outside** command to remove all existing outside mapping configurations and to prevent the addition of outside mappings to the configuration.

Examples

The following example shows how to configure NAT outside mapping:

```
Router(config)# ip nat settings support mapping outside
```

Related Commands

Command	Description
ip nat settings mode	Enables the NAT operating mode.

ip nat sip-sbc

To configure a Cisco IOS hosted Network Address Translation (NAT) traversal for Session Border Controller (SBC), use the **ip nat sip-sbc** command in global configuration mode. To disable the Cisco IOS hosted NAT traversal for SBC, use the **no** form of this command.

Syntax Description

proxy	Configures the address or port which the inside phones refer to, and configures the outside proxy's address or port that the NAT SBC translates the destination IP address or port.
inside-address	Sets the Proxy's private IP address, which is configured on the inside phones.
inside-port	Sets the Proxy's private port.
outside-address	Sets the Proxy's public address, which is the actual proxy's address that NAT SBC changes the destination address to.
outside -port	Sets the Proxy's port.
tcp	Establishes the Transmission Control Protocol.
udp	Establishes the User Datagram Protocol.
call-id-pool *pool-name*	(Optional) Specifies a dummy pool name from which the inside to outside SIP signaling packets' call ID is translated to a 1:1 maintained association rather than using the regular NAT pool.
override address	(Optional) Specifies the default override address mode.
override none	(Optional) Specifies that no override will be configured.
override port	(Optional) Specifies override port mode.
mode allow -flow-around	(Optional) Configures Real-Time Transport Protocol (RTP) for flow around for traffic between phones in the inside domain.
mode allow-flow-through *pool-name*	(Optional) Configures Real-Time Transport Protocol (RTP) for flow through for traffic between phones in the inside domain.
session -timeout *seconds*	(Optional) Configures the timeout duration for NAT entries pertaining to SIP signaling flows.
session-timeout nat-default	(Optional) Allows the default timeout to return to the NAT default timeout value of 5 minutes.
none	(Optional) Prevents modification of the out > in destination L3/L4 to the L3/L4 as saved in the sbc_appl_data of the door or NAT entry.
vrf -list vrf-name	(Optional) Defines SIP SBC VPN Routing and Forwarding (VRF) list names.
no	(Optional) Removes a name from the VRF list.

registration-throttle	(Optional) Defines the registration throttling parameter.
inside-timeout *seconds*	Timeout in seconds in the range of 1-536870.
outside-timeout *seconds*	Timeout in seconds in the range of 1-536870.
exit	(Required) Exit from SBC VRF configuration mode.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.4(15)T	The **allow-flow-through** and **registration-throttle** sub commands were added.

Usage Guidelines

The **proxy** keyword configures the address or port, which the inside phones refer to, and it configures the outside proxy's address or port that the NAT SBC translates the destination IP address or port. This keyword installs an outside static port half-entry with OL as the inside address or port and OG as the outside address or port.

The **mode allow-flow-around** keyword enables the RTP to be flow around. This keyword is only applicable for traffic between phones in the inside domain.

The mode **allow-flow-through** keyword enables the RTP to be flow through. This keywordd is only applicable for traffic between phones in the inside domain.

The optional **vrf-list** keyword must be followed by a list of VRF names. After the outside static port entry is created, a static route is installed wit the destination IP address as OL and next hop as OG. The NAT entry created is associated with appropriate VRFs as configured by this command.

Examples

The following example shows how to configure a Cisco IOS hosted NAT traversal for SBC:

```
interface ethernet1/1
 ip nat inside
 ip forwarding A
!
interface ethernet1/2
 ip nat inside
 ip forwarding B
!
interface ethernet1/3
 ip nat outside
!
ip nat pool call-id-pool 1.1.1.1 1.1.1.100
ip nat pool outside-pool 2.2.2.1.1.1 2.2.2.1.1.10
ip nat pool inside-pool-A 169.1.1.1 169.1.1.10
ip nat pool inside-pool-B 170.1.1.1 170.1.1.10
ip nat inside source list 1 pool inside-pool-A vrf A overload
ip nat inside source list 2 pool inside-pool-B vrf B overload
ip nat outside list 3 pool outside-pool
ip nat inside source list 4 pool call-id-pool
!
access-list for VRF-A inside-phones
```

```
access-list 1 permit 10.1.1.0 0.0.0.255
access-list 2 permit 172.1.1.0 0.0.0.255
!
access-=list for call-id-pool
access-list 4 permit 10.1.1.0 0.0.0.255
access-list 4 permit 20.1.1.0 0.0.0.255
!
ip nat sip-sbc
 proxy 200.1.1.1 5060 192.1.1.1 5060 protocol udp
 vrf-list
  vrf-name A
  vrf-name B
 call-id-pool call-id-pool
 session-timeout 300
 mode allow-flow-around
 override address
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
debug ip nat	Displays information about IP packets translated by NAT.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside source	Enables NAT of the inside destination address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Enables a port other than the default port.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.



ip nat source through iterate-ip-addrs

- ip nat settings gatekeeper-size, on page 417
- ip nat settings high-performance, on page 418
- ip nat settings nonpatdrop, on page 420
- ip nat source, on page 421
- ip nat stateful id, on page 423
- ip nat switchover replication http, on page 425
- ip nat translation, on page 426
- ip nat translation (timeout), on page 427
- ip nat translation max-entries, on page 430
- ip nat translation max-entries cpu, on page 433
- ip netmask-format, on page 434
- ip nhrp authentication, on page 435
- ip nhrp group, on page 436
- ip nhrp holdtime, on page 438
- ip nhrp interest, on page 439
- ip nhrp map, on page 440
- ip nhrp map group, on page 442
- ip nhrp map multicast, on page 444
- ip nhrp map multicast dynamic, on page 445
- ip nhrp max-send, on page 447
- ip nhrp multicast, on page 449
- ip nhrp network-id, on page 450
- ip nhrp nhs, on page 451
- ip nhrp record, on page 454
- ip nhrp redirect, on page 455
- ip nhrp registration, on page 457
- ip nhrp registration no-unique, on page 459
- ip nhrp responder, on page 460
- ip nhrp resolution refresh base, on page 461
- ip nhrp send-routed, on page 463
- ip nhrp server-only, on page 464
- ip nhrp shortcut, on page 465
- ip nhrp trigger-svc, on page 466

- ip nhrp use, on page 467
- ip options, on page 469
- ip proxy-arp, on page 471
- ip route, on page 472
- ip route vrf, on page 477
- ip routing, on page 481
- ip source binding, on page 482
- ip source-route, on page 484
- ip sticky-arp (global configuration), on page 485
- ip sticky-arp (interface configuration), on page 487
- ip subnet-zero, on page 488
- ip unnumbered, on page 489
- IP Unnumbered Ethernet Polling Support, on page 492
- ip verify source vlan dhcp-snooping, on page 493
- ipv4-prefix, on page 494
- ipv6 address autoconfig, on page 495
- ipv6 address dhcp, on page 497
- ipv6 address dhcp client request, on page 498
- ipv6 dhcp binding track ppp, on page 499
- ipv6 dhcp client information refresh minimum, on page 500
- ipv6 dhcp client pd, on page 501
- ipv6 dhcp database, on page 503
- ipv6 dhcp debug redundancy, on page 505
- ipv6 dhcp framed password, on page 506
- ipv6 dhcp guard attach-policy, on page 507
- ipv6 dhcp guard policy, on page 509
- ipv6 dhcp iana-route-add, on page 510
- ipv6 dhcp iapd-route-add, on page 511
- **ipv6 dhcp-ldra** , on page 512
- ipv6 dhcp-ldra attach-policy, on page 513
- ipv6 dhcp ldra attach-policy (VLAN), on page 515
- ipv6 dhcp ping packets, on page 516
- ipv6 dhcp pool, on page 517
- ipv6 dhcp relay destination, on page 520
- ipv6 dhcp-relay source-interface, on page 523
- ipv6 dhcp-relay bulk-lease, on page 524
- ipv6 dhcp-relay option vpn, on page 525
- ipv6 dhcp-relay show bindings, on page 526
- ipv6 dhcp-relay source-interface, on page 527
- ipv6 dhcp server, on page 528
- ipv6 dhcp server vrf enable, on page 530
- ipv6 inspect tcp finwait-time, on page 531
- ipv6 nd managed-config-flag, on page 532
- ipv6 nd other-config-flag, on page 534
- ipv6-prefix, on page 536
- iterate-ip-addrs, on page 537

ip nat settings gatekeeper-size

To modify gatekeeper cache size, use the **ip nat settings gatekeeper-size** command. This command allows allocating gatekeeper cache in the power of two based on the number of entries configured.

ip nat settings gatekeeper-size *number of entries*
no ip nat settings gatekeeper *number of entries*

Syntax Description

number of entries	Number of entries that can be stored in gatekeeper cache. Each entry has source and destination ip address of the packet.

Command Default

If gatekeeper service is enabled, gatekeeper cache size is allocated with default value. The default value is based on the platform.

Command Modes

Global configuration mode

Command History

Release	Modification
Cisco IOS XE Dublin 17.11.1a	This command was introduced in 3.13 MCP release. Maximum entries allowed for gatekeeper was 256k. In 17.11 release, maximum number of entries supported has been extended to 1 million entries.

Usage Guidelines

When a device is sending both NAT mode and non-NAT mode traffic, increase gatekeeper cache size to skip nat processing for non-NAT mode traffic.

Examples

The following example shows how to enable the **ip nat settings gatekeeper size** command on the device.

```
Router(config)#ip nat settings gatekeeper-size 1048576
Router(config)#end
```

Related Commands

Command	Description
ip nat service gatekeeper	Enables gatekeeper service to tag non-NAT mode traffic to skip NAT processing.

ip nat settings high-performance

To allow high connection setup rate for non-ALG NAT traffic, use the **ip nat settings high- performance** command. This command only supports pool overload configuration. To disable high connection set up rate, use the **no** form of this command.

ip nat settings high-performance
no ip nat settings high-performance

Syntax Description

This command has no arguments or keywords.

Command Default

This command is not enabled.

Command Modes

CGN operating mode and Global configuration mode

Command History

Release	Modification
Cisco IOS XE 17.2 Amsterdam	This command was introduced for ASR 1000 platform.

Usage Guidelines

Before enabling this command ensure that the following prerequisites are met:

- The paired address pooling is disabled using **no ip nat settings pap** command
- The end-point mapping is not configurable
- The application level gateways are disabled
- Reload the router after using this command

Examples

The following example shows how to enable the **ip nat settings high performance** command on the device.

```
!
Router(config)# ip nat settings high-performance
Router(config)# exit
Router(config-if)# reload
```

Examples

The following example shows how to verify if **ip nat settings high performance** command is working.

```
!
Router# show platform hardware qfp active feature nat datapath basecfg
```

Related Commands

Command	Description
ip dhcp limit lease per interface	Limits the number of DHCP leases offered to DHCP clients behind an ATM RBE unnumbered or serial unnumbered interface.
show ip dhcp limit lease	Displays the number of times the lease limit threshold has been violated on an interface.

ip nat settings nonpatdrop

This command enables the behavior related to non-PATable NAT translations. To configure this setting, use the **ip nat settings nonpatdrop** command in global configuration mode. To disable or remove this setting, use the **no** form of this command.

ip nat settings nonpatdrop
no ip nat settings nonpatdrop

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
16.4.1	This command was introduced.

Usage Guidelines

Using the **ip nat settings nonpatdrop** command, the router drops packets that cause Non-Pattable NAT translation attempts, which are traffic types without port numbers, instead of creating one-to-one bindings. This helps conserve NAT pool addresses and prevents address exhaustion from such traffic.

Examples

The following example shows how to enable the **ip nat settings nonpatdrop** command to control the behavior of non-PATable NAT translations:

```
Router(config)# ip nat settings nonpatdrop
```

ip nat source

To enable Network Address Translation (NAT) on a virtual interface without inside or outside specification, use the **ip nat source** command in global configuration mode.

Dynamic NAT
ip nat source {**list** {*access-list-numberaccess-list-name*} **interface** *type number* | **pool** *name*} [**overload** | **vrf** *name*]

Static NAT
ip nat source static {**esp** *local-ip* **interface** *type number* | *local-ip global-ip*} [**extendable** | **no-alias** | **no-payload** | **vrf** *name*]
no ip nat source static {**esp** *local-ip* **interface** *type number* | *local-ip global-ip*} [**extendable** | **no-alias** | **no-payload** | **vrf** *name*]

Port Static NAT

Network Static NAT
ip nat source static network *local-network global-network mask* [**extendable** | **no-alias** | **no-payload** | **vrf** *name*]
no ip nat source static network *local-network global-network mask* [**extendable** | **no-alias** | **no-payload** | **vrf** *name*]

Syntax Description

list *access - list-number*	Number of a standard IP access list. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
list *access - list-name*	Name of a standard IP access list. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
interface *type*	Specifies the interface type for the global address.
interface *number*	Specifies the interface number for the global address.
pool *name*	Name of the pool from which global IP addresses are allocated dynamically.
overload	(Optional) Enables the router to use one global address for many local addresses. When overloading is configured, the TCP or User Datagram Protocol (UDP) port number of each inside host distinguishes between the multiple conversations using the same local IP address.
vrf *name*	(Optional) Associates the NAT translation rule with a particular VPN routing and forwarding (VRF) instance.
static *local-ip*	Sets up a single static translation. The *local-ip* argument establishes the local IP address assigned to a host on the inside network. The address could be randomly chosen, allocated from the RFC 1918, or obsolete.
local-port	Sets the local TCP/UDP port in a range from 1 to 65535.

static *global-ip*	Sets up a single static translation. The *local-ip* argument establishes the globally unique IP address of an inside host as it appears to the outside network.
global-port	Sets the global TCP/UDP port in the range from 1 to 65535.
extendable	(Optional) Extends the translation.
no-alias	(Optional) Prohibits as alias from being created for the global address.
no-payload	(Optional) Prohibits the translation of an embedded address or port in the payload.
esp *local-ip*	Establishes IPSec-ESP (tunnel mode) support.
tcp	Establishes the Transmission Control Protocol.
udp	Establishes the User Datagram Protocol.
network *local-network*	Specified the local subnet translation.
global-network	Specifies the global subnet translation.
mask	Establishes the IP network mask to be used with subnet translations.

Command Modes

Global Configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Examples

The following example shows how to configure a virtual interface without inside or outside specification for the global address:

```
ip nat source list 1 pool NAT vrf bank overload
ip nat source list 1 pool NAT vrf park overload
ip nat source static 192.168.123.1 192.168.125.10 vrf services
```

Related Commands

Command	Description
ip nat enable	Configures an interface connecting VPNs and the Internet for NAT translation.
ip nat pool	Defines a pool of IP addresses for Network Address Translation.

ip nat stateful id

To designate the members of a translation group, use the **ip nat stateful id** command in global configuration mode. To disable the members of a translation group or reset default values, use the **no** form of this command.

no ip nat stateful id *id-number*

Syntax Description

id-number	Unique number given to each router in the stateful translation group.
redundancy *name*	Establishes Hot Standby Routing Protocol (HSRP) as the method of redundancy.
mapping-id *map-number*	Specifies whether or not the local Stateful (SNAT) router will distribute a particular set of locally created entries to a peer SNAT router.
protocol	(Optional) Enables the HSRP UDP default to be changed to TCP.
tcp	(Optional) Establishes the Transmission Control Protocol.
udp	(Optional) Establishes the User Datagram Protocol.
as -queuing	(Optional) Enables asymmetric routing during queuing for HSRP to be disabled.
disable	(Optional) Disables asymmetric routing during queuing in HSRP mode.
enable	(Optional) Enables asymmetric routing during queuing in HSRP mode.
primary i*p-address-primary*	Manually establishes redundancy for the primary router.
backup i*p-address-backup*	Manually establishes redundancy for the backup router.
peer *ip-address-peer*	Specifies the IP address of the peer router in the translation group.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.4(3)	The **protocol** and **as-queuing**keywords were added.
12.4(4)T	This command was intregrated into Cisco IOS Release 12.4(4)T.

Usage Guidelines

This command has two forms: HSRP stateful NAT and manual stateful NAT. The form that uses the keyword **redundancy** establishes the HSRP redundancy method. When HSRP mode is set, the primary and backup NAT routers are elected according to the HSRP standby state. To enable stateful NAT manually, configure the primary router and backup router.

In HSRP mode, the default TCP can be changed to UDP by using the optional **protocol udp** keywords with the **redundancy keyword**.

To disable the queuing during asymmetric routing in HSRP mode, use the optional **as-queuing disable** keywords with the **redundancy** keyword.

Examples

The following example shows how to configure SNAT with HSRP:

```
!
standby delay minimum 30 reload 60
standby 1 ip 10.1.1.1
standby 1 name SNATHSRP
standby 1 preempt delay minimum 60 reload 60 sync 60
!
ip nat Stateful id 1
redundancy SNATHSRP
mapping-id 10
as-queuing disable
protocol udp
ip nat pool SNATPOOL1 10.1.1.1 10.1.1.9 prefix-length 24
ip nat inside source route-map rm-101 pool SNATPOOL1 mapping-id 10 overload
ip classless
ip route 10.1.1.0 255.255.255.0 Null0
no ip http server
ip pim bidir-enable
```

The following example shows how to manually configure SNAT:

```
ip nat stateful id 1
primary 10.88.194.17
peer 10.88.194.18
mapping-id 10
ip nat stateful id 2
backup 10.88.194.18
peer 10.88.194.17
mapping-id 10
```

Related Commands

Command	Description
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Changes the amount of time after which NAT translations time out.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip nat switchover replication http

To enable replication of HTTP sessions during a switchover, use the **ip nat switchover replication http** command in global configuration mode. To disable replication of HTTP sessions during a switchover, use the **no** form of this command.

ip nat switchover replication http *port-number*
no ip nat switchover replication http

Syntax Description

port-number	HTTP port number. Valid values are from 1 to 65535.

Command Default

Replication of HTTP sessions during a switchover is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.0	This command was introduced.

Usage Guidelines

By default, NAT high availability (inter- and intra-box) does not replicate HTTP sessions to the standby router. Use the **ip nat switchover replication http** command to replicate HTTP sessions on the standby router during a switchover. Replication refers to the backing up of HTTP sessions on the standby router. HTTP sessions are usually short-lived connections and to reduce the high availability (HA) traffic between active and standby routers, backing up of HTTP sessions are avoided. The **ip nat switchover replication http** command enables you to control the replication of HTTP sessions based on your requirements.

Examples

The following example shows how to enable replication of HTTP sessions during a switchover:

```
Router(config)# ip nat switchover redundancy http 65
```

Related Commands

Command	Description
ip nat	Designates that traffic originating from or destined for an interface is subject to NAT.

ip nat translation

The **ip nat translation** command is replaced by the **ip nat translation**(timeout) and **ip nat translation max-entries** commands. See these commands for more information.

ip nat translation (timeout)

To change the Network Address Translation (NAT) timeout, use the **ip nat translation** command in global configuration mode. To disable the timeout, use the **no** form of this command.

ip nat translation {**arp-ping-timeout** | **dns-timeout** | **finrst-timeout** | **icmp-timeout** | **port-timeout** {**tcp** | **udp**} *port-number* | **pptp-timeout** | **routemap-entry-timeout** | **syn-timeout** | **tcp-timeout** | **timeout** | **udp-timeout**} {*seconds* | **never**}
no ip nat translation {**arp-ping-timeout** | **dns-timeout** | **finrst-timeout** | **icmp-timeout** | **port-timeout** {**tcp** | **udp**} *port-number* | **pptp-timeout** | **routemap-entry-timeout** | **syn-timeout** | **tcp-timeout** | **timeout** | **udp-timeout**}

Syntax Description

arp-ping-timeout	Specifies that the timeout value applies to the Address Resolution Protocol (ARP) ping.
dns-timeout	Specifies that the timeout value applies to connections to the Domain Name System (DNS). The default is 60 seconds.
finrst-timeout	Specifies that the timeout value applies to Finish and Reset TCP packets, which terminate a connection. The default is 60 seconds.
icmp-timeout	Specifies the timeout value for Internet Control Message Protocol (ICMP) flows. The default is 60 seconds.
port-timeout	Specifies that the timeout value applies to the TCP/UDP port.
tcp	Specifies TCP.
udp	Specifies UDP.
port-number	Port number for TCP or UDP. The range is from 1 to 65535.
pptp-timeout	Specifies that the timeout value applies to NAT Point-to-Point Tunneling Protocol (PPTP) flows. The default is 86,400 seconds (24 hours).
routemap-entry-timeout	Specifies that the timeout applies for a half entry created by a route map.
syn-timeout	Specifies that the timeout value applies to TCP flows immediately after a synchronous transmission (SYN) message that consists of digital signals that are sent with precise clocking. The default is 60 seconds.
tcp-timeout	Specifies that the timeout value applies to the TCP port. Default is 86,400 seconds (24 hours).
timeout	Specifies that the timeout value applies to dynamic translations, except for overload translations. The default is 86,400 seconds (24 hours).

udp-timeout	Specifies that the timeout value applies to the UDP port. The default is 300 seconds (5 minutes).
seconds	Number of seconds after which the specified port translation times out.
never	Specifies that port translation will not time out.

Command Default

NAT translation timeouts are enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
12.4(6)T	This command was modified. The **arp-ping-timeout** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **routemap-entry-timeout**, **tcp**, **udp**, and *port-number* keywords and arguments were added.

Usage Guidelines

When port translation is configured, each entry contains more information about the traffic that is using the translation, which gives you finer control over translation entry timeouts. Non-DNS UDP translations time out after 5 minutes, and DNS times out in 1 minute. TCP translations time out in 24 hours, unless a TCP Reset (RST) or a Finish (FIN) bit is seen on the stream, in which case they will time out in 1 minute.

Examples

The following example shows how to configure the router to cause UDP port translation entries to time out after 10 minutes (600 seconds):

```
Router# configure terminal
Router(config)# ip nat translation udp-timeout 600
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT; enables NAT logging; or enables static IP address support.
ip nat inside destination	Enables NAT of a globally unique host address to multiple inside host addresses.
ip nat inside source	Enables NAT of the inside source address.

Command	Description
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Specifies a port other than the default port for NAT.
ip nat translation max-entries	Limits the size of a NAT table to a specified maximum.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip nat translation max-entries

To limit the size of a Network Address Translation (NAT) table to a specified maximum, use the **ip nat translation max-entries** command in global configuration mode. To remove a specified limit, use the **no** form of this command.

ip nat translation max-entries {**all-host** | **all-vrf** | **host** *ip-address* | **list** {*list-namelist-number*} | **redundancy** *redundancy-id number-of-entries* | **vrf** *name*} *number*
no ip nat translation max-entries {**all-host** | **all-vrf** | **host** *ip-address* | **list** {*list-namelist-number*} | **redundancy** *redundancy-id number-of-entries* | **vrf** *name*} *number*

Syntax Description

all-host	Constrains each host by the specified number of NAT entries.
all-vrf	Constrains each VPN routing and forwarding (VRF) instance by the specified NAT limit.
host	Constrains an IP address by the specified NAT limit.
ip-address	IP address subject to the NAT limit.
list	Constrains an access control list (ACL) by the specified NAT limit.
list-name	ACL name subject to the NAT limit.
list-number	ACL number subject to the NAT limit.
redundancy	Specifies the NAT entries for redundancy groups (RGs).
redundancy-id	Redundancy ID. The range is from 1 to 2.
number-of-entries	Number of NAT entries. The range is from 1 to 2147483647.
vrf	Constrains an individual VRF instance by the specified NAT limit.
name	Name of the VRF instance subject to the NAT limit.
number	Maximum number of allowed NAT entries. The range is from 1 to 2147483647.



Note Note: On an ASR 1000 platform, if you are configuring Box-to-Box redundancy using the redundancy keyword, the limit set on the NAT table is ignored. Therefore, to enforce the limit, use the **ip nat translation max-entries** command without the redundancy keyword. For example: **ip nat translation max-entries** *number*command.

Command Default

No maximum size is specified for the NAT table.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRE	This command was modified. The **vrf** *name* keyword-argument pair was removed from Cisco 7600 series routers.
Cisco IOS XE Release 3.5S	This command was modified. The **redundancy** keyword and *redundancy-id* and *number-of-entries* arguments were added.
15.2(3)T	This command was modified. The order of precedence of the keywords was changed. For more information, see the "Usage Guidelines" section.

Usage Guidelines

Before you configure a NAT rate limit, you must first classify the current NAT usage and determine the sources of requests for NAT translations. If a specific host, an ACL, or a VRF instance is generating an unexpectedly high number of NAT requests, the host may be the source of a virus or worm attack.

Once you have identified the source of excessive NAT requests, you can set a NAT rate limit that constrains a specific host, an ACL, or a VRF instance, or you can set a general limit for the maximum number of NAT requests allowed regardless of their source.



Note When using the **no** form of the **ip nat translation max-entries** command, you must specify the type of NAT rate limit that you want to remove and its value. For more information about how to display the current NAT rate limit settings, see the **show ip nat statistics** command.

Prior to Cisco IOS Release 15.2(3)T, the order of precedence of keywords in the **ip nat translation max-entries** command is **vrf**, **all-vrf**, **host**, **all-host**, and **list**. For example, if you have configured the **ip nat translation max-entries list 50 2** and **ip nat translation max-entries all-host 10** commands in your NAT configuration, the **ip nat translation max-entries all-host 10** command overrides the **ip nat translation max-entries list 50 2** command, making the **ip nat translation max-entries list** command redundant. In Cisco IOS Release 15.2(3)T and later releases, the order of precedence of keywords is **vrf**, **all-vrf**, **host**, **list**, and **all-host**.

Examples

The following example shows how to limit the maximum number of allowed NAT entries to 300:

```
ip nat translation max-entries 300
```

Setting NAT Limits for VRF Instances

The following example shows how to limit each VRF instance to 200 NAT entries:

```
ip nat translation max-entries all-vrf 200
```

The following example shows how to limit the VRF instance named vrf1 to 150 NAT entries:

```
ip nat translation max-entries vrf vrf1 150
```

The following example shows how to limit the VRF instance named vrf2 to 225 NAT entries, but limit all other VRF instances to 100 NAT entries each:

```
ip nat translation max-entries all-vrf 100
ip nat translation max-entries vrf vrf2 225
```

Setting NAT Limits for ACLs

The following example shows how to limit the ACL named vrf3 to 100 NAT entries:

```
ip nat translation max-entries list vrf3 100
```

Setting NAT Limits for an IP Address

The following example shows how to limit the host at IP address 10.0.0.1 to 300 NAT entries:

```
ip nat translation max-entries host 10.0.0.1 300
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Enables a port other than the default port.
ip nat translation (timeout)	Changes the NAT timeout value.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip nat translation max-entries cpu

To configure the CPU utilization threshold for limiting the number of NAT translations, use the **ip nat translation max-entries cpu** command in global configuration mode.

To remove the CPU utilization threshold, use the **no** form of this command.

ip nat translation max-entries cpu *desired-percentage*
no ip nat translation max-entries cpu *desired-percentage*

Note The feature enabled by the **ip nat translation max-entries cpu** command is supported in Autonomous mode and is compatible with both classic NAT and CGN operational modes, but not in SD-WAN environments.

Syntax Description

cpu *desired-percentage*	Specifies the maximum CPU utilization threshold as a percentage of total CPU resources that can be used for processing NAT translations.

Command Default

By default, there is no CPU utilization threshold set for NAT translations.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 17.15.1a	This command was introduced.

Usage Guidelines

Set this threshold based on the average CPU load and performance requirements of your network. Monitor CPU utilization following threshold configuration; persistent high usage with no new translations may indicate a problem that requires Cisco support.

If the **clear ip nat translation** command is issued and the CPU utilization remains high (87 to 90 percent), without the gatekeeper command being configured, it is crucial to investigate and address the underlying issue to prevent service degradation.

This feature, enabled via the above command, requires cooperation with the NAT gatekeeper for proper management of NAT resources and synchronization.

Examples

The following example sets the CPU utilization threshold for NAT translations to 70%:

```
Device# configure terminal
Device(config)# ip nat translation max-entries cpu 70
```

ip netmask-format

To specify the format in which netmasks are displayed in **show** command output, use the **ip netmask-format**command inline configuration mode. To restore the default display format, use the **no** form of this command.

ip netmask-format {**bit-count** | **decimal** | **hexadecimal**}
no ip netmask-format {**bit-count** | **decimal** | **hexadecimal**}

Syntax Description

bit-count	Addresses are followed by a slash and the total number of bits in the netmask. For example, 131.108.11.0/24 indicates that the netmask is 24 bits.
decimal	Network masks are displayed in dotted-decimal notation (for example, 255.255.255.0).
hexadecimal	Network masks are displayed in hexadecimal format, as indicated by the leading 0X (for example, 0XFFFFFF00).

Command Default

Netmasks are displayed in dotted-decimal format.

Command Modes

Line configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

IP uses a 32-bit mask that indicates which address bits belong to the network and subnetwork fields, and which bits belong to the host field. This is called a *netmask*. By default, **show** commands display an IP address and then its netmask in dotted decimal notation. For example, a subnet would be displayed as 10.108.11.0 255.255.255.0.

However, you can specify that the display of the network mask appear in hexadecimal format or bit count format instead. The hexadecimal format is commonly used on UNIX systems. The previous example would be displayed as 10.108.11.0 0XFFFFFF00.

The bitcount format for displaying network masks is to append a slash (/) and the total number of bits in the netmask to the address itself. The previous example would be displayed as 10.108.11.0/24.

Examples

The following example configures network masks for the specified line to be displayed in bitcount notation in the output of **show** commands:

```
line vty 0 4
 ip netmask-format bitcount
```

ip nhrp authentication

To configure the authentication string for an interface using the Next Hop Resolution Protocol (NHRP), use the **ip nhrp authentication**command ininterface configuration mode. To remove the authentication string, use the **no** form of this command.

ip nhrp authentication *string*
no ip nhrp authentication [*string*]

Syntax Description

string	Authentication string configured for the source and destination stations that controls whether NHRP stations allow intercommunication. The string can be up to eight characters long.

Command Default

No authentication string is configured; the Cisco IOS software adds no authentication option to NHRP packets it generates.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

All routers configured with NHRP within one logical nonbroadcast multiaccess (NBMA) network must share the same authentication string.

Examples

In the following example, the authentication string named specialxx must be configured in all devices using NHRP on the interface before NHRP communication occurs:

```
ip nhrp authentication specialxx
```

ip nhrp group



Note The command **ip nhrp group** has been deprecated and is not in use. Use the command **nhrp group** instead of **ip nhrp group**.

To configure a Next Hop Resolution Protocol (NHRP) group on a spoke, use the **ip nhrp group**command in interface configuration mode. To remove an NHRP group, use the **no** form of this command.

ip nhrp group *group-name*
no ip nhrp group *group-name*

Syntax Description

group-name	Specifies an NHRP group name.

Command Default

No NHRP groups are created.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(22)T	This command was introduced.
15.4(1)T / 3.11S	This command was replaced with *nhrp group* and hidden.
16.6.5, 16.8.1	This hidden command was removed, manual migration to new syntax required before or after upgrade.

Usage Guidelines

After you create an NHRP group on a spoke, you use the **ip nhrp map group**command to map the group to a QoS policy map.

Examples

The following example shows how to create two NHRP groups named small and large.

```
Router> enable
Router# configure terminal
Router(config)# interface Tunnel 0
Router(config-if)# ip nhrp group small
Router(config-if)# ip nhrp group large
```

Related Commands

Command	Description
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
ip nhrp map group	Adds NHRP groups to QoS policy mappings on a hub.
show dmvpn	Displays DMVPN-specific session information.

Command	Description
show ip nhrp	Displays NHRP mapping information.
show ip nhrp group-map	Displays the details of NHRP group mappings on a hub and the list of tunnels using each of the NHRP groups defined in the mappings.
show policy-map mgre	Displays statistics about a specific QoS policy as it is applied to a tunnel endpoint.

ip nhrp holdtime

To change the number of seconds that Next Hop Resolution Protocol (NHRP) nonbroadcast multiaccess (NBMA) addresses are advertised as valid in authoritative NHRP responses, use the **ip nhrp holdtime**command ininterface configuration mode. To restore the default value, use the **no** form of this command.

ip nhrp holdtime *seconds*
no ip nhrp holdtime [*seconds*]

Syntax Description

seconds	Time in seconds that NBMA addresses are advertised as valid in positive authoritative NHRP responses. **Note** The recommended NHRP hold time value ranges from 300 to 600 seconds. Although a higher value can be used when required, we recommend that you do not use a value less than 300 seconds; and if used, it should be used with extreme caution.

Command Default

7200 seconds (2 hours)

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **ip nhrp holdtime** command affects authoritative responses only. The advertised holding time is the length of time the Cisco IOS software tells other routers to keep information that it is providing in authoritative NHRP responses. The cached IP-to-NBMA address mapping entries are discarded after the holding time expires.

The NHRP cache can contain static and dynamic entries. The static entries never expire. Dynamic entries expire regardless of whether they are authoritative or nonauthoritative.

Examples

In the following example, NHRP NBMA addresses are advertised as valid in positive authoritative NHRP responses for 1 hour:

```
ip nhrp holdtime 3600
```

ip nhrp interest

To control which IP packets can trigger sending a Next Hop Resolution Protocol (NHRP) request packet, use the **ip nhrp interest**command ininterface configuration mode. To restore the default value, use the **no** form of this command.

ip nhrp interest *access-list-number*
no ip nhrp interest [*access-list-number*]

Syntax Description

access-list-number	Standard or extended IP access list number in the range from 1 to 199.

Command Default

All non-NHRP packets can trigger NHRP requests.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command with the **access-list** command to control which IP packets trigger NHRP requests.

The **ip nhrp interest** command controls which packets cause NHRP address resolution to take place; the **ip nhrp use** command controls how readily the system attempts such address resolution.

Examples

In the following example, any TCP traffic can cause NHRP requests to be sent, but no other IP packets will cause NHRP requests:

```
ip nhrp interest 101
access-list 101 permit tcp any any
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
ip nhrp use	Configures the software so that NHRP is deferred until the system has attempted to send data traffic to a particular destination multiple times.

ip nhrp map

To statically configure the IP-to-nonbroadcast multiaccess (NBMA) address mapping of IP destinations connected to an NBMA network, use the **ip nhrp map** interface configuration command. To remove the static entry from Next Hop Resolution Protocol (NHRP) cache, use the **no** form of this command.

ip nhrp map *ip-address nbma-address* [**preference** *pref*]
no ip nhrp map *ip-address nbma-address* [**preference** *pref*]

Syntax Description

ip-address	IP address of the destinations reachable through the NBMA network. This address is mapped to the NBMA address.
nbma-address	NBMA address that is directly reachable through the NBMA network. The address format varies depending on the medium you are using. For example, ATM has a Network Service Access Point (NSAP) address, Ethernet has a MAC address, and Switched Multimegabit Data Service (SMDS) has an E.164 address. This address is mapped to the IP address.
preference *pref*	(Optional) Assigns a preference for the IP-to-NBMA address mapping. The preference must be in the range 1 to 255.

Command Default

No static IP-to-NBMA cache entries exist.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.2(1)T	This command was modified. NBMA address was modified to support IPv6 address.
Cisco IOS XE Release 16.8.1	This command was modified. Option to assign a preference for IP-to-NBMA address mapping was added.

Usage Guidelines

You will probably need to configure at least one static mapping in order to reach the next-hop server. Repeat this command to statically configure multiple IP-to-NBMA address mappings.

Examples

In the following example, this station in a multipoint tunnel network is statically configured to be served by two next-hop servers 10.0.0.1 and 10.0.1.3. The NBMA address for 10.0.0.1 is statically configured to be 192.0.0.1 and the NBMA address for 10.0.1.3 is 192.2.7.8.

```
interface tunnel 0
```

```
ip nhrp nhs 10.0.0.1
ip nhrp nhs 10.0.1.3
ip nhrp map 10.0.0.1 192.0.0.1 preference 3
ip nhrp map 10.0.1.3 192.2.7.8 preference 9
```

Related Commands

Command	Description
clear ip nhrp	Clears all dynamic entries from the NHRP cache.

ip nhrp map group

Note The command **ip nhrp map group** has been deprecated and is not in use. Use the command **nhrp map group** instead of **ip nhrp map group**.

To associate a Next Hop Resolution Protocol (NHRP) group to a QoS policy map, use the **ip nhrp map group**command in interface configuration mode. To remove an association, use the **no** form of this command.

ip nhrp map group *group-name* **service-policy output** *qos-policy-map-name*
no ip nhrp map group *group-name* **service-policy output** *qos-policy-map-name*

Syntax Description

group-name	Specifies an NHRP group name.
qos-policy-map-name	Specifies a QoS policy map name.

Command Default

No mappings are created.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(22)T	This command was introduced.
15.4(1)T / 3.11S	This command was replaced with *nhrp map group* and hidden.
16.6.5, 16.8.1	This hidden command was removed, manual migration to new syntax required before or after upgrade.

Usage Guidelines

The command allows a QoS policy in the output direction only.

Examples

The following example shows how to map two NHRP groups named small and large to two QoS policy maps named qos-small and qos-large respectively.

```
Router> enable
Router# configure terminal
Router(config)# interface Tunnel 0
Router(config-if)# ip nhrp map group small service-policy output qos-small
Router(config-if)# ip nhrp map group large service-policy output qos-large
```

Related Commands

Command	Description
ip nhrp group	Configures a NHRP group on a spoke.
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.

Command	Description
show dmvpn	Displays DMVPN-specific session information.
show ip nhrp	Displays NHRP mapping information.
show ip nhrp group-map	Displays the details of NHRP group mappings on a hub and the list of tunnels using each of the NHRP groups defined in the mappings.
show policy-map mgre	Displays statistics about a specific QoS policy as it is applied to a tunnel endpoint.

ip nhrp map multicast

To configure nonbroadcast multiaccess (NBMA) addresses used as destinations for broadcast or multicast packets to be sent over a tunnel network, use the **ip nhrp map multicast**command in interface configuration mode. To remove the destinations, use the **no** form of this command.

ip nhrp map multicast *nbma-address*
no ip nhrp map multicast *nbma-address*

Syntax Description

nbma-address	NBMA address that is directly reachable through the NBMA network. The address format varies depending on the medium you are using.

Command Default

No NBMA addresses are configured as destinations for broadcast or multicast packets.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.2(1)T	This command was modified. NBMA address was modified to support IPv6 address.

Usage Guidelines

This command applies only to tunnel interfaces.

The command is useful for supporting broadcasts over a tunnel network when the underlying network does not support IP multicast. If the underlying network does support IP multicast, you should use the **tunnel destination** command to configure a multicast destination for transmission of tunnel broadcasts or multicasts.

When multiple NBMA addresses are configured, the system replicates the broadcast packet for each address.

Examples

In the following example, if a packet is sent to 10.255.255.255, it is replicated to destinations 10.0.0.1 and 10.0.0.2. Addresses 10.0.0.1 and 10.0.0.2 are the IP addresses of two other routers that are part of the tunnel network, but those addresses are their addresses in the underlying network, not the tunnel network. They would have tunnel addresses that are in network 10.0.0.0.

```
interface tunnel 0
 ip address 10.0.0.3 255.0.0.0
 ip nhrp map multicast 10.0.0.1
 ip nhrp map multicast 10.0.0.2
```

ip nhrp map multicast dynamic

To allow Next Hop Resolution Protocol (NHRP) to automatically add routers to the multicast NHRP mappings, use the **ip nhrp map multicast dynamic**command in interface configuration mode. To disable this functionality or to clear dynamic entries, use the **no** form of this command.

ip nhrp map multicast dynamic
no ip nhrp map multicast dynamic

Syntax Description

This command has no arguments or keywords.

Command Default

This command is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)M3	This command was modified to enable the clearing of all dynamic entries in the multicast table by using the **no** form of this command.

Usage Guidelines

Use this command when spoke routers need to initiate multipoint generic routing encapsulation (GRE) and IPSecurity (IPSec) tunnels and register their unicast NHRP mappings. This command is needed to enable dynamic routing protocols to work over the Multipoint GRE and IPSec tunnels because IGP routing protocols use multicast packets. This command prevents the Hub router from needing a separate configuration line for a multicast mapping for each spoke router.

You can clear all dynamic entries in the multicast table by using the **no** form of this command.

Examples

The following example shows how to enable the **ip nhrp map multicast dynamic**command on the hub router:

```
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwith 1000
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1436
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp holdtime 600
 no ip split-horizon eigrp 1
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
```

```
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address 10.17.0.1 255.255.255.0
```

ip nhrp max-send

To change the maximum frequency at which Next Hop Resolution Protocol (NHRP) packets can be sent, use the **ip nhrp max-send**interface configuration command. To restore this frequency to the default value, use the **no** form of this command.

ip nhrp max-send *pkt-count* **every** *seconds*
no ip nhrp max-send

Syntax Description

pkt-count	Number of packets that can be sent in the range from 1 to 65535. Default is 100 packets.
every *seconds*	Time (in seconds) in the range from 10 to 65535. Default is 10 seconds.

Command Default

pkt-count : 100 packets*seconds:*10 seconds

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The software maintains a per-interface quota of NHRP packets that can be sent. NHRP traffic, whether locally generated or forwarded, cannot be sent at a rate that exceeds this quota. The quota is replenished at the rate specified by the *seconds*argument.

- This command needs to take into consideratin the number of spoke routers being handled by this hub and how often they send NHRP registration requests. To support this load you would need:

Number of spokes / registration timeout * *Max-send-interval*

- • Example

500 spokes with 100 second Registration timeout

Max send value = 500/100*10 = 50

- The Maximum number of spoke-spoke tunnels that are expected to be up at any one time across the whole DMVPN network.

spoke-spoke tunnels/NHRP holdtime * Max-send-interval

This would cover spoke-spoke tunnel creation and the refreshing of spoke-spoke tunnels that are used for longer periods of time.

- • Example

2000 spoke-spoke tunnels with 250 second hold timeout

Max send value = 2000/250*10 = 80

Then add these together and multiply this by 1.5 - 2.0 to give a buffer.

- • Example

Max send = (50 + 80) * 2 = 260

- The max-send-interval can be used to keep the long term average number of NHRP messages allowed to be sent constant, but allow greater peaks.
    - Example

400 messages in 10 seconds

In this case it could peak at approximately 200 messages in the first second of the 10 second interval, but still keep to a 40 messages per second average over the 10 second interval.

4000 messages in 100 seconds

In this case it could peak at approximately 2000 messages in the first second of the 100 second interval, but it would still be held to 40 messages per second average over the 100 second interval. In the second case it could handle a higher peak rate, but risk a longer period of time when no messages can be sent if it used up its quota for the interval.

By default, the maximum rate at which the software sends NHRP packets is five packets per 10 seconds. The software maintains a per-interface quota of NHRP packets (whether generated locally or forwarded) that can be sent.

Examples

In the following example, only one NHRP packet can be sent from serial interface 0 each minute:

```
interface serial 0
 ip nhrp max-send 1 every 60
```

Related Commands

Command	Description
ip nhrp interest	Controls which IP packets can trigger sending an NHRP request.
ip nhrp use	Configures the software so that NHRP is deferred until the system has attempted to send data traffic to a particular destination multiple times.

ip nhrp multicast

To configure multicast batch size and batch interval, use the **ip nhrp multicast** command in interface configuration mode. To remove the multicast batch size and batch interval configuration, use the **no** form of this command.

ip nhrp multicast [**batch-size** *num*][**batch-interval** *milliseconds*]

no ip nhrp multicast [**batch-size** *num*][**batch-interval** *milliseconds*]

Syntax Description

batch-size *num*	Specifies the batch size of multicast replication.
batch-interval *milliseconds*	Specifies the interval for batch multicast replication.

Command Default

The default multicast batch-size is 250. The default multicast batch-interval is 10 milliseconds.

Command Modes

Interface configuration

Command History

Release	Modification
IOS XE Release 16.8.1	Command introduced.

Usage Guidelines

By replacing **ip** in the command name with **ipv6**, you can set the multicast batch size and interval for IPv6 traffic.

Example

The following example shows the multicast batch-size configured to 12 and the batch-interval configured to 10 milliseconds for a tunnel interface.

```
interface tunnel0
 ip nhrp multicast batch-size 12 batch-interval 10
```

ip nhrp network-id

To enable the Next Hop Resolution Protocol (NHRP) on an interface, use the **ip nhrp network-id**command ininterface configuration mode. To disable NHRP on the interface, use the **no** form of this command.

ip nhrp network-id *number*
no ip nhrp network-id [*number*]

Syntax Description

number	Globally unique, 32-bit network identifier from a nonbroadcast multiaccess (NBMA) network. The range is from 1 to 4294967295.

Command Default

NHRP is disabled on the interface.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

In general, all NHRP stations within one logical NBMA network must be configured with the same network identifier.

Examples

The following example enables NHRP on the interface:

```
ip nhrp network-id 1
```

ip nhrp nhs

To specify the address of one or more Next Hop Resolution Protocol (NHRP) servers, use the **ip nhrp nhs**command in interface configuration mode. To remove the address, use the **no** form of this command.

Cisco IOS Release 12.2(33)SRA, 12.2SX, and Later Releases
ip nhrp nhs *nhs-address* [*net-address* [*netmask*]]
no ip nhrp nhs *nhs-address* [*net-address* [*netmask*]]

Cisco IOS Release 15.1(2)T and Later Releases
ip nhrp nhs {*nhs-address* [**nbma** {*nbma-addressFQDN-string*}] [**multicast**] [**priority** *value*] [**cluster** *value*] | **cluster** *value* **max-connections** *value* | **dynamic nbma** {*nbma-addressFQDN-string*} [**multicast**] [**priority** *value*] [**cluster** *value*] | **fallback** *seconds*}
no ip nhrp nhs {*nhs-address* [**nbma** {*nbma-addressFQDN-string*}] [**multicast**] [**priority** *value*] [**cluster** *value*] | **cluster** *value* **max-connections** *value* | **dynamic nbma** {*nbma-addressFQDN-string*} [**multicast**] [**priority** *value*] [**cluster** *value*] | **fallback** *seconds*}

Syntax Description

nhs-address	Address of the next-hop server being specified.
net-address	(Optional) IP address of a network served by the next-hop server.
netmask	(Optional) IP network mask to be associated with the IP address. The IP address is logically ANDed with the mask.
nbma	(Optional) Specifies the nonbroadcast multiple access (NBMA) address or FQDN.
nbma-address	NBMA address.
FQDN-string	Next hop server (NHS) fully qualified domain name (FQDN) string.
multicast	(Optional) Specifies to use NBMA mapping for broadcasts and multicasts.
priority *value*	(Optional) Assigns a priority to hubs to control the order in which spokes select hubs to establish tunnels. The range is from 0 to 255; 0 is the highest and 255 is the lowest priority.
cluster *value*	(Optional) Specifies NHS groups. The range is from 0 to 10; 0 is the highest and 10 is the lowest. The default value is 0.
max-connections *value*	Specifies the number of NHS elements from each NHS group that needs to be active. The range is from 0 to 255.
dynamic	Configures the spoke to learn the NHS protocol address dynamically.
fallback *seconds*	Specifies the duration, in seconds, for which the spoke must wait before falling back to an NHS of higher priority upon recovery.

Command Default

No next-hop servers are explicitly configured, so normal network layer routing decisions are used to forward NHRP traffic.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(2)T	This command was modified. The *net-address* and *mask* arguments were removed and the **nbma**, *nbma-address*, *FQDN-string*, **multicast**, **priority** *value*, **cluster** *value*, **max-connections** *value*, **dynamic**, and **fallback** *seconds* keywords and arguments were added.
15.2(1)T	This command was modified. The NBMA address was modified to support IPv6 address.

Usage Guidelines

Use the **ip nhrp nhs** command to specify the address of a next hop server and the networks it serves. Normally, NHRP consults the network layer forwarding table to determine how to forward NHRP packets. When next hop servers are configured, these next hop addresses override the forwarding path that would otherwise be used for NHRP traffic.

When the **ip nhrp nhs dynamic** command is configured on a DMVPN tunnel and the **shut** command is issued to the tunnel interface, the crypto socket does not receive shut message, thereby not bringing up a DMVPN session with the hub.

For any next hop server that is configured, you can specify multiple networks by repeating this command with the same *nhs-address*argument, but with different IP network addresses.

Examples

The following example shows how to register a hub to a spoke using NBMA and FQDN:

```
Router# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ip nhrp nhs 192.0.2.1 nbma examplehub.example1.com
```

The following example shows how to configure the desired **max-connections** value:

```
Router# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ip nhrp nhs cluster 5 max-connections 100
```

The following example shows how to configure the NHS fallback time:

```
Router# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ip nhrp nhs fallback 25
```

The following example shows how to configure NHS priority and group values:

```
Router# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ip nhrp nhs 192.0.2.1 priority 1 cluster 2
```

Related Commands

Command	Description
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
show ip nhrp	Displays NHRP mapping information.

ip nhrp record

To reenable the use of forward record and reverse record options in Next Hop Resolution Protocol (NHRP) request and reply packets, use the **ip nhrp record**interface configuration command. To suppress the use of such options, use the **no** form of this command.

ip nhrp record
no ip nhrp record

Syntax Description

This command has no arguments or keywords.

Command Default

Forward record and reverse record options are used in NHRP request and reply packets.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Forward record and reverse record options provide loop detection and are enabled by default. Using the **no** form of this command disables this method of loop detection. For another method of loop detection, see the **ip nhrp responder**command.

Examples

The following example suppresses forward record and reverse record options:

```
no ip nhrp record
```

Related Commands

Command	Description
ip nhrp responder	Designates the primary IP address of which interface the Next Hop Server will use in NHRP reply packets when the NHRP requester uses the Responder Address option.

ip nhrp redirect

To enable Next Hop Resolution Protocol (NHRP) redirect, use the **ip nhrp redirect**command in interface configuration mode. To remove the NHRP redirect, use the **no** form of this command.

ip nhrp redirect [**timeout** *seconds*]
no ip nhrp redirect [**timeout** *seconds*]

Syntax Description

timeout *seconds*	Indicates the interval, in seconds, that the NHRP redirects are sent for the same nonbroadcast multiaccess (NBMA) source and destination combination. The range is from 2 to 30 seconds.

Command Default

NHRP redirect is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The NHRP redirect message is an indication that the current path to the destination is not optimal. The receiver of the message should find a better path to the destination.

This command generates an NHRP redirect traffic indication message if the incoming and outgoing interface is part of the same DMVPN network. The NHRP shortcut switching feature depends on receiving the NHRP redirect message. NHRP shortcut switching does not trigger an NHRP resolution request on its own. It triggers an NHRP resolution request only after receiving an NHRP redirect message.

Most of the traffic would follow a spoke-hub-spoke path. NHRP redirect is generally required to be configured on all the DMVPN nodes in the event the traffic follows a spoke-spoke-hub-spoke path, which is unlikely the case.

Do not configure this command if the DMVPN network is configured for full-mesh. In a full-mesh configuration the spokes are populated with a full routing table with next-hop being the other spokes.

Examples

The following example shows how to enable NHRP redirects on the interface:

```
Router> enable

Router# configure terminal
Router(config)# interface Tunnel0
Router(config)# interface Tunnel0
Router(config-if)# ip address 192.2.0.11 255.255.255.0
Router(config-if)# ip nhrp authentication test
Router(config-if)# ip nhrp map multicast 192.2.0.2
Router(config-if)# ip nhrp map 192.2.0.2 192.2.0.13
Router(config-if)# ip nhrp network-id 100000
Router(config-if)# ip nhrp nhs 192.2.0.11
Router(config-if)# ip nhrp shortcut
Router(config-if)# ip nhrp redirect
Router(config-if)# tunnel source Serial1/0
```

```
Router(config-if)# tunnel mode gre multipoint
Router(config-if)# tunnel key 100000
Router(config-if)# tunnel protection ipsec profile vpnprof
```

Related Commands

Command	Description
ip nhrp shortcut	Enables NHRP shortcut switching.

ip nhrp registration

To enable the client to not set the unique flag in the Next Hop Resolution Protocol (NHRP) request and reply packets, use the **ip nhrp registration** command in interface configuration mode. To reenable this functionality, use the **no** form of this command.

ip nhrp registration [**timeout** *seconds* | **no-unique** | **req-def-map** [**include-label**]]
no ip nhrp registration [**timeout** *seconds* | **no-unique** | **req-def-map** [**include-label**]]

Syntax Description

timeout *seconds*	(Optional) Time between periodic registration messages. • *seconds* --Number of seconds. The range is from 1 through the value of the NHRP hold timer. • If the **timeout** keyword is not specified, NHRP registration messages are sent every number of seconds equal to 1/3 the value of the NHRP hold timer.
no-unique	(Optional) Enables the client to not set the unique flag in the NHRP request and reply packets.
req-def-map	(Optional) Enables the client to request default maps in registration.
include-label	(Optional) Enables the client to request default maps with labels in registration.

Command Default

This command is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.3	This command was introduced.
12.3(7.2)	The **timeout** keyword and *seconds*argument were added. In addition, effective with Cisco IOS Release 12.3(7.2), this command replaced the **ip nhrp registration no-unique** command.
12.3(7)T	The **timeout** keyword and *seconds*argument were integrated into Cisco IOS Release 12.3(7)T. In addition, the replacement of the **ip nhrp registration no-unique** command with this command was integrated into Cisco IOS Release 12.3(7)T.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 16.10.1	The **req-def-map** keyword was added.
Cisco IOS XE Release 17.11.1a	The **include-label** keyword was added.

Usage Guidelines

If the unique flag is set in the NHRP registration request packet, a next-hop server (NHS) must reject any registration attempts for the same private address using a different nonbroadcast multiaccess (NBMA) address. If a client receives a new IP address, for example via DHCP, and tries to register before the cache entry on the NHS times out, the NHS must reject it.

By configuring the **ip nhrp registration** command and **no-unique** keyword, the unique flag is not set, and the NHS can override the old registration information.

This command and keyword combination is useful in an environment where client IP addresses can change frequently such as a dial environment.

By configuring the **ip nhrp registration** command and the **req-def-map** keyword, the NHRP client requests for default map from the server via registration message.

Examples

The following example configures the client to not set the unique flag in the NHRP registration packet:

```
interface FastEthernet 0/0
 ip nhrp registration no-unique
```

The following example shows that the registration timeout is set to 120 seconds, and the delay is set to 5 seconds:

```
interface FastEthernet 0/0
 ip nhrp registration 120
```

The following example configures the client to enable requesting default maps in registration packet:

```
interface FastEthernet 0/0
 ip nhrp registration req-def-map
```

The following example configures the client to enable requesting default maps with labels in registration packet:

```
interface FastEthernet 0/0
 ip nhrp registration req-def-map include-label
```

Related Commands

Command	Description
ip nhrp holdtime	Changes the number of seconds that NHRP NBMA addresses are advertised as valid in authoritative NHRP responses

ip nhrp registration no-unique

The **ip nhrp registration no-unique** command is replaced by the **ip nhrp registration command.**See the **ip nhrp registration**command for more information.

ip nhrp responder

To designate the primary IP address the Next Hop Server that an interface will use in Next Hop Resolution Protocol (NHRP) reply packets when the NHRP requestor uses the Responder Address option, use the **ip nhrp responder**command ininterface configuration mode. To remove the designation, use the **no** form of this command.

ip nhrp responder *interface-type interface-number*
no ip nhrp responder [*interface-type*] [*interface-number*]

Syntax Description

interface-type	Interface type whose primary IP address is used when a next-hop server complies with a Responder Address option (for example, **serial or tunnel**).
interface-number	Interface number whose primary IP address is used when a next-hop server complies with a Responder Address option.

Command Default

The next-hop server uses the IP address of the interface where the NHRP request was received.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If an NHRP requestor wants to know which next-hop server generates an NHRP reply packet, it can request that information through the Responder Address option. The next-hop server that generates the NHRP reply packet then complies by inserting its own IP address in the Responder Address option of the NHRP reply. The next-hop server uses the primary IP address of the specified interface.

If an NHRP reply packet being forwarded by a next-hop server contains the IP address of that next-hop server, the next-hop server generates an Error Indication of type “NHRP Loop Detected” and discards the reply packet.

Examples

In the following example, any NHRP requests for the Responder Address will cause this router acting as a next-hop server to supply the primary IP address of serial interface 0 in the NHRP reply packet:

```
ip nhrp responder serial 0
```

ip nhrp resolution refresh base

The default NHRP resolution requests follow the routed path to the destination spoke (exit point out the DMVPN cloud). For the first resolution request, this routed path is via the hub(s) all the way to the destination spoke. Owing to the on-demand route created as a result of the resolution process, for a resolution request sent for refreshing on-demand spoke-spoke routes and tunnels the routed path is the direct path between the spokes. This revalidates the direct spoke-spoke path like a keepalive and also reduces the load on the hub.

You can use this command to make the requests follow the base routed path via the hub(s), and do not take the on-demand path/route that was learnt for the prefix/next hop.

ip nhrp resolution refresh base *number*
no ip nhrp resolution refresh base

Syntax Description

refresh	Displays resolution refresh-related configuration options.
base	Configures the base routed path for routing resolution requests for refresh. This excludes the on-demand/shortcut routed path for routing resolution requests for refreshes.
number	(Optional) Specifies which refresh goes through the base path.

Command Default

The default settings are used.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE 17.4 Release	The **refresh** and **base** keywords were introduced to the **ip nhrp resolution refresh base** command.

Usage Guidelines

Use **ip nhrp resolution refresh base** *number* on the tunnel interface on the spoke when it is intended that the resolution requests follow the base routed path via the hub(s) and don't take the on-demand path/route that was learnt for the prefix/next hop. When configured, it should be configured symmetrically at both ends, else, it leads to asymmetric behavior.

Examples

The following example displays what the *number* denotes:

- When the value is n=1, every refresh goes through the base path.
- When the value is n=2, every second refresh goes through the base path, while other values still follow the default behaviour.

```
ip nhrp resolution refresh base 1
```

Related Commands

Command	Description
ip nhrp send-routed	This command is enabled by default and causes NHRP control packets to be sent over the routed path.

Command	Description
no ip nhrp send-routed	This command causes NHRP control packets to be sent over the routed path to the destination/next hop. This is enabled by default.

ip nhrp send-routed

To forward the resolution requests via the routed path, use **ip nhrp send-routed** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ip nhrp send-routed
no ip nhrp send-routed

Command Default

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
16.9	This command was introduced.

Usage Guidelines

With **ip nhrp send-routed** configured, the control packets take the routed path instead of nhs priority path. Without send-routed, the nhs priority configuration takes effect. The path taken by the control packets can be verfied using **show ip nhrp traffic** command.

For all non-registration packets, the first NHRP resolution request takes the route installed by the IGP initially and then is forwarded along the routed path, for subsequent requests. The routed path can be the NHRP route or NHOs.

If the routed path fails for some reasons, tunnel falls back to the NHS path.

By replacing **ip** in the command name with **ipv6**, you can forward the resolution requests via the routed path for IPv6 traffic.

Examples

The following is an example of tunnel interface when the tunnel interface is disabled:

```
interface Tunnel1
ip address 192.168.10.10 255.255.255.0
no ip redirects
ip nhrp authentication C!sco123
ip nhrp network-id 1
ip nhrp nhs 192.168.10.1 nbma 172.16.10.1 multicast
no ip nhrp send-routed
tunnel source GigabitEthernet2
tunnel mode gre multipoint
end
```

ip nhrp server-only

To configure the interface to operate in Next Hop Resolution Protocol (NHRP) server-only mode, use the **ip nhrp server-only**command ininterface configuration mode. To disable this feature, use the **no** form of this command.

ip nhrp server-only [**non-caching**]
no ip nhrp server-only

Syntax Description

non-caching	(Optional) The router will not cache NHRP information received on this interface.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.0	The **non-caching** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When the interface is operating in NHRP server-only mode, the interface does not originate NHRP requests or set up an NHRP shortcut Switched Virtual Circuit (SVC).

Examples

The following example configures the interface to operate in server-only mode:

```
ip nhrp server-only
```

ip nhrp shortcut

To enable Next Hop Resolution Protocol (NHRP) shortcut switching, use the **ip nhrp shortcut**command in interface configuration mode. To remove shortcut switching from NHRP, use the **no** form of this command.

ip nhrp shortcut
no ip nhrp shortcut

Syntax Description

This command has no arguments or keywords.

Command Default

The NHRP shortcut switching is enabled in Cisco IOS XE Everest 16.6.2 and Cisco IOS 15.7(2)M releases and later. Prior to these releases, this command was disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
Cisco IOS XE Everest Release 16.6.2 and Cisco IOS Release 15.7(2)M	By default, NHRP shortcut switching was enabled.

Usage Guidelines

Do not configure this command if the DMVPN network is configured for full-mesh. In a full-mesh configuration the spokes are populated with a full routing table with next-hop being the other spokes.

Examples

The following example shows how to configure an NHRP shortcut on an interface:

```
Router> enable

Router# configure terminal
Router(config)# interface Tunnel0
Router(config-if)# ip address 192.2.0.11 255.255.255.0
Router(config-if)# ip nhrp authentication test
Router(config-if)# ip nhrp map multicast 192.2.0.2
Router(config-if)# ip nhrp map 192.2.0.2 192.2.0.13
Router(config-if)# ip nhrp network-id 100000
Router(config-if)# ip nhrp nhs 192.2.0.11
Router(config-if)# ip nhrp shortcut
Router(config-if)# ip nhrp redirect
Router(config-if)# tunnel source Serial1/0
Router(config-if)# tunnel mode gre multipoint
Router(config-if)# tunnel key 100000
Router(config-if)# tunnel protection ipsec profile vpnprof
```

Related Commands

Command	Description
ip nhrp redirect	Enables NHRP redirect.

ip nhrp trigger-svc

To configure when the Next Hop Resolution Protocol (NHRP) will set up and tear down a switched virtual circuit (SVC) based on aggregate traffic rates, use the **ip nhrp trigger-svc**command ininterface configuration mode. To restore the default thresholds, use the **no** form of this command.

ip nhrp trigger-svc *trigger-threshold teardown-threshold*
no ip nhrp trigger-svc

Syntax Description

trigger-threshold	Average traffic rate calculated during the **load interval**, at or above which NHRP will set up an SVC for a destination. The default value is 1 kbps.
teardown-threshold	Average traffic rate calculated during the load interval, at or below which NHRP will tear down the SVC to the destination. The default value is 0 kbps.

Command Default

trigger-threshold : 1 kbps

teardown-threshold : 0 kbps

Command Modes

Interface configuration

Command History

Release	Modification
12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The two thresholds are measured during a sampling interval of 30 seconds, by default. To change that interval, use the **load-interval** *seconds* argument of the **ip cef traffic-statistics** command.

Examples

In the following example, the triggering and teardown thresholds are set to 100 kbps and 5 kbps, respectively:

```
ip nhrp trigger-svc 100 5
```

Related Commands

Command	Description
ip cef	Enables CEF on the route processor card.
ip cef accounting	Enables network accounting of CEF information.
ip cef traffic-statistics	Changes the time interval that controls when NHRP will set up or tear down an SVC.
ip nhrp interest	Controls which IP packets can trigger sending an NHRP request.

ip nhrp use

To configure the software so that Next Hop Resolution Protocol (NHRP) is deferred until the system has attempted to send data traffic to a particular destination multiple times, use the **ip nhrp use**commandininterface configuration mode. To restore the default value, use the **no** form of this command.

ip nhrp use *usage-count*
no ip nhrp use *usage-count*

Syntax Description

usage-count	Packet count in the range from 1 to 65535. Default is 1.

Command Default

usage-count : 1. The first time a data packet is sent to a destination for which the system determines NHRP can be used, an NHRP request is sent.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When the software attempts to send a data packet to a destination for which it has determined that NHRP address resolution can be used, an NHRP request for that destination is normally sent immediately. Configuring the *usage-count*argument causes the system to wait until that many data packets have been sent to a particular destination before it attempts NHRP. The *usage-count* argument for a particular destination is measured over 1-minute intervals (the NHRP cache expiration interval).

The usage count applies *per destination*. So if the *usage-count* argument is configured to be 3, and four data packets are sent toward 10.0.0.1 and one packet toward 10.0.0.2, then an NHRP request is generated for 10.0.0.1 only.

If the system continues to need to forward data packets to a particular destination, but no NHRP response has been received, retransmission of NHRP requests is performed. This retransmission occurs only if data traffic continues to be sent to a destination.

The **ip nhrp interest** command controls *which* packets cause NHRP address resolution to take place; the **ip nhrp use** command controls *how readily* the system attempts such address resolution.

Examples

In the following example, if in the first minute five packets are sent to the first destination and five packets are sent to a second destination, then a single NHRP request is generated for the second destination.

If in the second minute the same traffic is generated and no NHRP responses have been received, then the system resends its request for the second destination.

```
ip nhrp use 5
```

Related Commands

Command	Description
ip nhrp interest	Controls which IP packets can trigger sending an NHRP request.
ip nhrp max-send	Changes the maximum frequency at which NHRP packets can be sent.

ip options

To drop or ignore IP options packets that are sent to the router, use the **ip options**command in global configuration mode. To disable this functionality and allow all IP options packets to be sent to the router, use the **no** form of this command.

ip options {**drop** | **ignore**}
no ip options {**drop** | **ignore**}

Syntax Description

drop	Router drops all IP options packets that it receives.
ignore	Router ignores all options and treats the packets as though they did not have any IP options. (The options are not removed from the packet--just ignored.) **Note** This option is not available on the Cisco 10000 series router.

Command Default

This command is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.3(19)	This command was integrated into Cisco IOS Release 12.3(19).
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2 for the PRE3.

Usage Guidelines

The **ip options** command allows you to filter IP options packets, mitigating the effects of IP options on the router, and on downstream routers and hosts.

Drop and ignore modes are mutually exclusive; that is, if the drop mode is configured and you configure the ignore mode, the ignore mode overrides the drop mode.

Cisco 10720 Internet Router

The **ip options ignore** command is not supported. Only drop mode (the **ip options drop** command) is supported.

Cisco 10000 Series Router

This command is only available on the PRE3. The PRE2 does not support this command.

The **ip options ignore** command is not supported. The router supports only the **ip options drop** command.

Examples

The following example shows how to configure the router (and downstream routers) to drop all options packets that enter the network:

```
ip options drop
% Warning:RSVP and other protocols that use IP Options packets may not function in drop or
 ignore modes.
end
```

ip proxy-arp

To enable proxy Address Resolution Protocol (ARP) on an interface, use the **ip proxy-arp** command in interface configuration mode. To disable proxy ARP on the interface, use the **no**form of this command.

ip proxy-arp
no ip proxy-arp

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **ip arp proxy disable** command overrides any proxy ARP interface configuration.

Examples

The following example enables proxy ARP on Ethernet interface 0:

```
interface ethernet 0
 ip proxy-arp
```

Related Commands

Command	Description
ip arp proxy disable	Globally disables proxy ARP.

ip route

To establish static routes, use the **ip route** command in global configuration mode. Toremove static routes, use the **no**form of this command.

ip route [**vrf** *vrf-name*] *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [**dhcp**] [*distance*] [**name** *next-hop-name*] [**permanent** | **track** *number*] [**tag** *tag*]
no ip route [**vrf** *vrf-name*] *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [**dhcp**] [*distance*] [**name** *next-hop-name*] [**permanent** | **track** *number*] [**tag** *tag*]

Syntax Description

vrf *vrf-name*	(Optional) Configures the name of the VRF by which static routes should be specified.
prefix	IP route prefix for the destination.
mask	Prefix mask for the destination.
ip-address	IP address of the next hop that can be used to reach that network.
interface-type interface-number	Network interface type and interface number.
dhcp	(Optional) Enables a Dynamic Host Configuration Protocol (DHCP) server to assign a static route to a default gateway (option 3). **Note** Specify the **dhcp** keyword for each routing protocol.
distance	(Optional) Administrative distance. The default administrative distance for a static route is 1.
name *next-hop-name*	(Optional) Applies a name to the next hop route.
permanent	(Optional) Specifies that the route will not be removed, even if the interface shuts down.
track *number*	(Optional) Associates a track object with this route. Valid values for the *number* argument range from 1 to 500.
tag *tag*	(Optional) Tag value that can be used as a “match” value for controlling redistribution via route maps.

Command Default

No static routes are established.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.3(2)XE	The **track** keyword and *number* argument were added.

Release	Modification
12.3(8)T	The **track** keyword and *number* argument were integrated into Cisco IOS Release 12.3(8)T. The **dhcp** keyword was added.
12.3(9)	The changes made in Cisco IOS Release 12.3(8)T were added to Cisco IOS Release 12.3(9).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The establishment of a static route is appropriate when the Cisco IOS software cannot dynamically build a route to the destination.

When you specify a DHCP server to assign a static route, the interface type and number and administrative distance may be configured also.

If you specify an administrative distance, you are flagging a static route that can be overridden by dynamic information. For example, routes derived with Enhanced Interior Gateway Routing Protocol (EIGRP) have a default administrative distance of 100. To have a static route that would be overridden by an EIGRP dynamic route, specify an administrative distance greater than 100. Static routes have a default administrative distance of 1.

Static routes that point to an interface on a connected router will be advertised by way of Routing Information Protocol (RIP) and EIGRP regardless of whether **redistribute static** commands are specified for those routing protocols. This situation occurs because static routes that point to an interface are considered in the routing table to be connected and hence lose their static nature. Also, the target of the static route should be included in the **network**(DHCP) command. If this condition is not met, no dynamic routing protocol will advertise the route unless a **redistribute static**command is specified for these protocols. With the following configuration:

```
rtr1 (serial 172.16.188.1/30)--------------> rtr2(Fast Ethernet 172.31.1.1/30) ------>
router [rip | eigrp]
 network 172.16.188.0
 network 172.31.0.0
```

- RIP and EIGRP redistribute the route if the route is pointing to the Fast Ethernet interface:

```
ip route 172.16.188.252 255.255.255.252 FastEthernet 0/0
```

RIP and EIGRP do not redistribute the route with the following **ip route**command because of the split horizon algorithm:

```
ip route 172.16.188.252 255.255.255.252 serial 2/1
```

- EIGRP redistributes the route with both of the following commands:

```
ip route 172.16.188.252 255.255.255.252 FastEthernet 0/0
ip route 172.16.188.252 255.255.255.252 serial 2/1
```

With the Open Shortest Path First (OSPF) protocol, static routes that point to an interface are not advertised unless a **redistribute static**command is specified.

Adding a static route to an Ethernet or other broadcast interface (for example, ip route 0.0.0.0 0.0.0.0 Ethernet 1/2) will cause the route to be inserted into the routing table only when the interface is up. This configuration is not generally recommended. When the next hop of a static route points to an interface, the router considers

each of the hosts within the range of the route to be directly connected through that interface, and therefore it will send Address Resolution Protocol (ARP) requests to any destination addresses that route through the static route.

A logical outgoing interface, for example, a tunnel, needs to be configured for a static route. If this outgoing interface is deleted from the configuration, the static route is removed from the configuration and hence does not show up in the routing table. To have the static route inserted into the routing table again, configure the outgoing interface once again and add the static route to this interface.

The practical implication of configuring the **ip route 0.0.0.0 0.0.0.0 ethernet 1/2** command is that the router will consider all of the destinations that the router does not know how to reach through some other route as directly connected to Ethernet interface 1/2. So the router will send an ARP request for each host for which it receives packets on this network segment. This configuration can cause high processor utilization and a large ARP cache (along with memory allocation failures). Configuring a default route or other static route that directs the router to forward packets for a large range of destinations to a connected broadcast network segment can cause your router to reload.

Specifying a numerical next hop that is on a directly connected interface will prevent the router from using proxy ARP. However, if the interface with the next hop goes down and the numerical next hop can be reached through a recursive route, you may specify both the next hop and interface (for example, ip route 0.0.0.0 0.0.0.0 ethernet 1/2 10.1.2.3) with a static route to prevent routes from passing through an unintended interface.



Note Configuring a default route that points to an interface, such as **ip route 0.0.0.0 0.0.0.0 ethernet 1/2**,displays a warning message. This command causes the router to consider all the destinations that the router cannot reach through an alternate route, as directly connected to Ethernet interface 1/2. Hence, the router sends an ARP request for each host for which it receives packets on this network segment. This configuration can cause high processor utilization and a large ARP cache (along with memory allocation failures). Configuring a default route or other static route that directs the router to forward packets for a large range of destinations to a connected broadcast network segment can cause the router to reload.

The **name** *next-hop-name* keyword and argument combination allows you to associate static routes with names in your running configuration. If you have several static routes, you can specify names that describe the purpose of each static route in order to more easily identify each one.

The **track** *number* keyword and argument combination specifies that the static route will be installed only if the state of the configured track object is up.

Recursive Static Routing

In a recursive static route, only the next hop is specified. The output interface is derived from the next hop.

For the following recursive static route example, all destinations with the IP address prefix address prefix 192.168.1.1/32 are reachable via the host with address 10.0.0.2:

```
ip route 192.168.1.1 255.255.255.255 10.0.0.2
```

A recursive static route is valid (that is, it is a candidate for insertion in the IPv4 routing table) only when the specified next hop resolves, either directly or indirectly, to a valid IPv4 output interface, provided the route does not self-recurse, and the recursion depth does not exceed the maximum IPv4 forwarding recursion depth.

The following example defines a valid recursive IPv4 static route:

```
interface serial 2/0
 ip address 10.0.0.1 255.255.255.252
```

```
 exit
ip route 192.168.1.1 255.255.255.255 10.0.0.2
```

The following example defines an invalid recursive IPv4 static route. This static route will not be inserted into the IPv4 routing table because it is self-recursive. The next hop of the static route, 192.168.1.0/30, resolves via the first static route 192.168.1.0/24, which is itself a recursive route (that is, it only specifies a next hop). The next hop of the first route, 192.168.1.0/24, resolves via the directly connected route via the serial interface 2/0. Therefore, the first static route would be used to resolve its own next hop.

```
interface serial 2/0
 ip address 10.0.0.1 255.255.255.252
 exit
ip route 192.168.1.0 255.255.255.0 10.0.0.2
ip route 192.168.1.0 255.255.255.252 192.168.1.100
```

It is not normally useful to manually configure a self-recursive static route, although it is not prohibited. However, a recursive static route that has been inserted in the IPv4 routing table may become self-recursive as a result of some transient change in the network learned through a dynamic routing protocol. If this situation occurs, the fact that the static route has become self-recursive will be detected and the static route will be removed from the IPv4 routing table, although not from the configuration. A subsequent network change may cause the static route to no longer be self-recursive, in which case it will be re-inserted in the IPv4 routing table.



Note IPv4 recursive static routes are checked at one-minute intervals. Therefore, a recursive static route may take up to a minute to be inserted into the routing table once its next hop becomes valid. Likewise, it may take a minute or so for the route to disappear from the table if its next hop becomes invalid.

Examples

The following example shows how to choose an administrative distance of 110. In this case, packets for network 10.0.0.0 will be routed to a router at 172.31.3.4 if dynamic information with an administrative distance less than 110 is not available.

```
ip route 10.0.0.0 255.0.0.0 172.31.3.4 110
```



Note Specifying the next hop without specifying an interface when configuring a static route can cause traffic to pass through an unintended interface if the default interface goes down.

The following example shows how to route packets for network 172.31.0.0 to a router at 172.31.6.6:

```
ip route 172.31.0.0 255.255.0.0 172.31.6.6
```

The following example shows how to route packets for network 192.168.1.0 directly to the next hop at 10.1.2.3. If the interface goes down, this route is removed from the routing table and will not be restored unless the interface comes back up.

```
ip route 192.168.1.0 255.255.255.0 Ethernet 0 10.1.2.3
```

The following example shows how to install the static route only if the state of track object 123 is up:

```
ip route 0.0.0.0 0.0.0.0 Ethernet 0/1 10.1.1.242 track 123
```

The following example shows that using the **dhcp** keyword in a configuration of Ethernet interfaces 1 and 2 enables the interfaces to obtain the next-hop router IP addresses dynamically from a DHCP server:

```
ip route 10.165.200.225 255.255.255.255 ethernet1 dhcp
ip route 10.165.200.226 255.255.255.255 ethernet2 dhcp 20
```

The following example shows that using the **name** *next-hop-name* keyword and argument combination for each static route in the configuration helps you remember the purpose for each static route.

```
ip route 172.0.0.0 255.0.0.0 10.0.0.1 name Seattle2Detroit
```

The name for the static route will be displayed when the **show running-configuration** command is entered:

```
Router# show running-config
 | include ip route
ip route 172.0.0.0 255.0.0.0 10.0.0.1 name Seattle2Detroit
```

Related Commands

Command	Description
network (DHCP)	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

ip route vrf

To establish static routes for a Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **ip route vrf**command in global configuration mode. To disable static routes, use the **no** form of this command.

ip route vrf *vrf-name prefix mask* [*next-hop-address*] [*interface interface-number*] [**global**] [*distance*] [**permanent**] [**tag** *tag*]
no ip route vrf *vrf-name prefix mask* [*next-hop-address*] [*interface interface-number*] [**global**] [*distance*] [**permanent**] [**tag** *tag*]

Syntax Description

vrf-name	Name of the VRF for the static route.
prefix	IP route prefix for the destination, in dotted decimal format.
mask	Prefix mask for the destination, in dotted decimal format.
next-hop-address	(Optional) IP address of the next hop (the forwarding router that can be used to reach that network).
interface	(Optional) Name of network interface to use.
interface-number	(Optional) Number identifying the network interface to use.
global	(Optional) Specifies that the given next hop address is in the non-VRF routing table.
distance	(Optional) An administrative distance for this route.
permanent	(Optional) Specifies that this route will not be removed, even if the interface shuts down.
tag *tag*	(Optional) Specifies the label (tag) value that can be used for controlling redistribution of routes through route maps.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
XE 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

Use a static route when the Cisco IOS software cannot dynamically build a route to the destination.

If you specify an administrative distance when you set up a route, you are flagging a static route that can be overridden by dynamic information. For example, Interior Gateway Routing Protocol (IGRP)-derived routes have a default administrative distance of 100. To set a static route to be overridden by an IGRP dynamic route, specify an administrative distance greater than 100. Static routes each have a default administrative distance of 1.

Static routes that point to an interface are advertised through the Routing Information Protocol (RIP), IGRP, and other dynamic routing protocols, regardless of whether the routes are redistributed into those routing protocols. That is, static routes configured by specifying an interface lose their static nature when installed into the routing table.

However, if you define a static route to an interface not defined in a network command, no dynamic routing protocols advertise the route unless a **redistribute static** command is specified for these protocols.

Supported Static Route Configurations

When you configure static routes in a Multiprotocol Label Switching (MPLS) or MPLS VPN environment, note that some variations of the **ip route** and **ip route vrf** commands are not supported. These variations of the commands are not supported in Cisco IOS releases that support the Tag Forwarding Information Base (TFIB), specifically Cisco IOS releases 12.*x* T, 12.*x* M, and 12.0S. The TFIB cannot resolve prefixes when the recursive route over which the prefixes travel disappears and then reappears. However, the command variations are supported in Cisco IOS releases that support the MPLS Forwarding Infrastructure (MFI), specifically Cisco IOS release 12.2(25)S and later releases. Use the following guidelines when configuring static routes.

Supported Static Routes in an MPLS Environment

The following **ip route** command is supported when you configure static routes in an MPLS environment:

ip route *destination-prefix mask interface next-hop-address*

The following **ip route** commands are supported when you configure static routes in an MPLS environment and configure load sharing with static nonrecursive routes and a specific outbound interface:

ip route *destination-prefix mask* **interface1 next-hop1 ip route** *destination-prefix mask* **interface2 next-hop2**

Unsupported Static Routes in an MPLS Environment That Uses the TFIB

The following **ip route** command is not supported when you configure static routes in an MPLS environment:

ip route *destination-prefix mask next-hop-address*

The following **ip route** command is not supported when you configure static routes in an MPLS environment and enable load sharing where the next hop can be reached through two paths:

ip route *destination-prefix mask next-hop-address*

The following **ip route** command is not supported when you configure static routes in an MPLS environment and enable load sharing where the destination can be reached through two next hops:

ip route *destination-prefix mask* **next-hop1 ip route** *destination-prefix mask* **next-hop2**

Use the *interface* and *next-hop* arguments when specifying static routes.

Supported Static Routes in an MPLS VPN Environment

The following **ip route vrf**commands are supported when you configure static routes in an MPLS VPN environment, and the next hop and interface are in the same VRF:

- • **ip route vrf** *vrf-name destination-prefix mask next-hop-address*
  • **ip route vrf** *vrf-name destination-prefix mask interface next-hop-address*
  • **ip route vrf** *vrf-name destination-prefix mask interface1 next-hop1* **ip route vrf** *vrf-name destination-prefix ma sk interface2 next-hop2*

The following **ip route vrf**commands are supported when you configure static routes in an MPLS VPN environment, and the next hop is in the global table in the MPLS cloud in the global routing table. For example, these commands are supported when the next hop is pointing to the Internet gateway.

- • **ip route vrf** *vrf-name destination-prefix mask next-hop-address* **global**
  • **ip route vrf** *vrf-name destination-prefix mask interface next-hop-address* (This command is supported when the next hop and interface are in the core.)

The following **ip route**commands are supported when you configure static routes in an MPLS VPN environment and enable load sharing with static nonrecursive routes and a specific outbound interface:

ip route *destination-prefix mask* **interface1 next-hop1 ip route** *destination-prefix mask* **interface2 next-hop2**

Unsupported Static Routes in an MPLS VPN Environment That Uses the TFIB

The following **ip route** command is not supported when you configure static routes in an MPLS VPN environment, the next hop is in the global table in the MPLS cloud within the core, and you enable load sharing where the next hop can be reached through two paths:

ip route vrf *destination-prefix mask next-hop-address* **global**

The following **ip route** commands are not supported when you configure static routes in an MPLS VPN environment, the next hop is in the global table in the MPLS cloud within the core, and you enable load sharing where the destination can be reached through two next hops:

ip route vrf *destination-prefix mask* **next-hop1 global ip route vrf** *destination-prefix mask* **next-hop2 global**

The following **ip route vrf** commands are not supported when you configure static routes in an MPLS VPN environment, and the next hop and interface are in the same VRF:

ip route vrf *vrf-name destination-prefix mask* **next-hop1 ip route vrf** *vrf-name destination-prefix mask* **next-hop2**

Supported Static Routes in an MPLS VPN Environment Where the Next Hop Resides in the Global Table on the CE Router

The following **ip route vrf**command is supported when you configure static routes in an MPLS VPN environment, and the next hop is in the global table on the customer equipment (CE) side. For example, the following command is supported when the destination prefix is the CE router's loopback address, as in external BGP (EBGP) multihop cases.

ip route vrf *vrf-name destination-prefix mask interface next-hop-address*

The following **ip route** commands are supported when you configure static routes in an MPLS VPN environment, the next hop is in the global table on the CE side, and you enable load sharing with static nonrecursive routes and a specific outbound interfaces:

ip route *destination-prefix mask* **interface1 nexthop1 ip route** *destination-prefix mask* **interface2 nexthop2**

Examples

The following command shows how to reroute packets addressed to network 10.23.0.0 in VRF vpn3 to router 10.31.6.6:

```
Router(config)# ip route vrf vpn3 10.23.0.0 255.255.0.0 10.31.6.6
```

Related Commands

Command	Description
show ip route vrf	Displays the IP routing table associated with a VRF.
redistribute static	Redistributes routes from another routing domain into the specified domain.

ip routing

To enable IP routing, use the **ip routing** command in global configuration mode. To disable IP routing, use the **no**form of this command.

ip routing
no ip routing

Syntax Description

This command has no arguments or keywords.

Command Default

IP routing is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To bridge IP, the **no ip routing** command must be configured to disable IP routing. However, you need not specify **no ip routing** in conjunction with concurrent routing and bridging to bridge IP.

The ip routing command is disabled on the Cisco VG200 voice over IP gateway.

Disabling IP routing is not allowed if you are running Cisco IOS Release 12.2SX on a Catalyst 6000 platform. The workaround is to not assign an IP address to the SVI.

Examples

The following example enables IP routing:

```
Router# configure terminal
Router(config
)
# ip routing
```

ip source binding

To add a static IP source binding entry, use the **ip source binding** command. Use the **no** form of this command to delete a static IP source binding entry

ip source binding *mac-address* **vlan** *vlan-id ip-address* **interface** *type mod/port*

Syntax Description

mac-address	Binding MAC address.
vlan *vlan-id*	Specifies the Layer 2 VLAN identification; valid values are from 1 to 4094.
ip-address	Binding IP address.
interface *type*	Interface type; possible valid values are **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **port-channel** *num*, and **vlan** *vlan-id*.
mod / port	Module and port number.

Command Default

No IP source bindings are configured.

Command Modes

Global configuration.

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

You can use this command to add a static IP source binding entry only.

The **no** format deletes the corresponding IP source binding entry. It requires the exact match of all required parameter in order for the deletion to be successful. Note that each static IP binding entry is keyed by a MAC address and a VLAN number. If the command contains the existing MAC address and VLAN number, the existing binding entry is updated with the new parameters instead of creating a separate binding entry.

Examples

This example shows how to add a static IP source binding entry:

```
Router(config)#
ip source binding 000C.0203.0405 vlan 100 172.16.30.2 interface gigabitethernet5/3
```

This example shows how to delete a static IP source binding entry:

```
Router(config)#
no ip source binding 000C.0203.0405 vlan 100 172.16.30.2 interface gigabitethernet5/3
```

Related Commands

Command	Description
ip verify source vlan dhcp snooping	Enables or disables the per 12-port IP source guard.
show ip source binding	Displays the IP source bindings configured on the system.

Command	Description
show ip verify source	Displays the IP source guard configuration and filters on a particular interface.

ip source-route

To allow the Cisco IOS software to handle IP datagrams with source routing header options, use the **ip source-route** command in global configuration mode. To have the software discard any IP datagram containing a source-route option, use the **no** form of this command.

ip source-route
no ip source-route

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example enables the handling of IP datagrams with source routing header options:

```
ip source-route
```

Related Commands

Command	Description
ping (privileged)	Diagnoses basic network connectivity (in privileged EXEC mode) on Apollo, AppleTalk, CLNS, DECnet, IP, Novell IPX, VINES, or XNS networks.
ping (user)	Diagnoses basic network connectivity (in user EXEC mode) on Apollo, AppleTalk, CLNS, DECnet, IP, Novell IPX, VINES, or XNS networks.

ip sticky-arp (global configuration)

To enable sticky ARP, use the **ip sticky-arp** command in global configuration mode. To disable sticky ARP, use the **no** form of this command.

ip sticky-arp
no ip sticky-arp

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXF	This command was changed to support all Layer 3 interfaces.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

In releases prior to Release 12.2(18)SXF, sticky ARP was supported on PVLAN interfaces only.

You can enter the **ip sticky-arp (interface configuration)**command to disable sticky ARP on a specific interface.

ARP entries that are learned on Layer 3 interfaces are sticky ARP entries. We recommend that you display and verify ARP entries on the Layer 3 interface using the **show arp** command.

For security reasons, sticky ARP entries on the Layer 3 interface do not age out. Connecting new equipment with the same IP address generates a message and the ARP entry is not created.

Because the ARP entries on the Layer 3 interface do not age out, you must manually remove ARP entries on the Layer 3 interface if a MAC address changes.

Unlike static entries, sticky-ARP entries are not stored and restored when you enter the **reboot** and **restart** commands.

Examples

This example shows how to enable sticky ARP:

```
Router(config) ip sticky-arp
```

This example shows how to disable sticky ARP:

```
Router(config) no ip sticky-arp
```

Related Commands

Command	Description
arp	Enables ARP entries for static routing over the SMDS network.
ip sticky-arp (interface configuration)	Enables sticky ARP on an interface.
show arp	Displays the ARP table.

ip sticky-arp (interface configuration)

To enable sticky ARP on an interface, use the **ip sticky-arp** command in interface configuration mode. To disable sticky ARP on an interface, use the **no** form of this command.

ip sticky-arp [**ignore**]
no ip sticky-arp [**ignore**]

Syntax Description

ignore	(Optional) Overwrites the **ip sticky-arp**(global configuration) command.

Command Default

This command has no default settings.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXF	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You can enter this command on any Layer 3 interface.

You can enter the **ip sticky-arp ignore** command to overwrite the PVLAN sticky-ARP global configuration on a specific interface.

Examples

This example shows how to enable sticky ARP on an interface:

```
Router(config-if) ip sticky-arp
```

This example shows how to remove the previously configured command on an interface:

```
Router(config-if) no ip sticky-arp
```

This example shows how to disable sticky ARP on an interface:

```
Router(config-if) ip sticky-arp
 ignore
```

Related Commands

Command	Description
arp	Enables ARP entries for static routing over the SMDS network.
ip sticky-arp (global configuration)	Enables sticky ARP.
show arp	Displays the ARP table.

ip subnet-zero

To enable the use of subnet 0 for interface addresses and routing updates, use the **ip subnet-zero** command in global configuration mode. To restore the default, use the no form of this command.

ip subnet-zero
no ip subnet-zero

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **ip subnet-zero** command provides the ability to configure and route to subnet 0 subnets.

Subnetting with a subnet address of 0 is discouraged because of the confusion inherent in having a network and a subnet with indistinguishable addresses.

Examples

The following example enables subnet zero:

```
ip subnet-zero
```

ip unnumbered

To enable IP processing on an interface without assigning an explicit IP address to the interface, use the **ip unnumbered** command in interface configuration mode or subinterface configuration mode. To disable the IP processing on the interface, use the **no** form of this command.

ip unnumbered *type number* [**poll**]
no ip unnumbered [*type number*]

Syntax Description

type	Type of interface. For more information, use the question mark (**?**) online help function.
number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (**?**) online help function.
poll	(Optional) Enables IP connected host polling.

Command Default

Unnumbered interfaces are not supported.

Command Modes

Interface configuration (config-if)

Subinterface configuration (config-subif)

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command was modified to configure IP unnumbered support on Ethernet VLAN subinterfaces and subinterface ranges.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE. This command was made available on the Supervisor Engine 720.
12.2(18)SXF	This command was modified to support Ethernet physical interfaces and switched virtual interfaces (SVIs).
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers..
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY. The **poll** keyword was added.

Usage Guidelines

When an unnumbered interface generates a packet (for example, for a routing update), it uses the address of the specified interface as the source address of the IP packet. It also uses the address of the specified interface in determining which routing processes are sending updates over the unnumbered interface.

The following restrictions are applicable for this command:

- This command is not supported on Cisco 7600 Series Routers that are configured with a Supervisor Engine 32.
- Serial interfaces using High-Level Data Link Control (HDLC), PPP, Link Access Procedure Balanced (LAPB), Frame Relay encapsulations, and Serial Line Internet Protocol (SLIP), and tunnel interfaces can be unnumbered.
- This interface configuration command cannot be used with X.25 or Switched Multimegabit Data Service (SMDS) interfaces.
- You cannot use the **ping** EXEC command to determine whether the interface is up because the interface has no address. Simple Network Management Protocol (SNMP) can be used to remotely monitor interface status.
- It is not possible to netboot a Cisco IOS image over a serial interface that is assigned an IP address with the **ip unnumbered** command.
- You cannot support IP security options on an unnumbered interface.

The interface that you specify using the *type* and *number* arguments must be enabled (listed as "up" in the **show interfaces** command display).

If you are configuring Intermediate System-to-Intermediate System (IS-IS) across a serial line, you must configure the serial interfaces as unnumbered. This configuration allows you to comply with RFC 1195, which states that IP addresses are not required on each interface.



Note Using an unnumbered serial line between different major networks (or *majornets*) requires special care. If at each end of the link there are different majornets assigned to the interfaces that you specified as unnumbered, any routing protocol that is running across the serial line must not advertise subnet information.

Examples

The following example shows how to assign the address of Ethernet 0 to the first serial interface:

```
Device(config)# interface ethernet 0
Device(config-if)# ip address 10.108.6.6 255.255.255.0
!
Device(config-if)# interface serial 0
Device(config-if)# ip unnumbered ethernet 0
```

The following example shows how to configure Ethernet VLAN subinterface 3/0.2 as an IP unnumbered subinterface:

```
Device(config)# interface ethernet 3/0.2
Device(config-subif)# encapsulation dot1q 200
Device(config-subif)# ip unnumbered ethernet 3/1
```

The following example shows how to configure Fast Ethernet subinterfaces in the range from 5/1.1 to 5/1.4 as IP unnumbered subinterfaces:

```
Device(config)# interface range fastethernet5/1.1 - fastethernet5/1.4
Device(config-if-range)# ip unnumbered ethernet 3/1
```

The following example shows how to enable polling on a Gigabit Ethernet interface:

```
Device(config)# interface loopback0
Device(config-if)# ip address 10.108.6.6 255.255.255.0
```

```
!
Device(config-if)# ip unnumbered gigabitethernet 3/1
Device(config-if)# ip unnumbered loopback0 poll
```

IP Unnumbered Ethernet Polling Support

ip verify source vlan dhcp-snooping

To enable Layer 2 IP source guard, use the **ip verify source vlan dhcp-snooping** command in the service instance mode. Use the **no** form of this command to disable Layer 2 IP source guard.

ip verify source vlan dhcp-snooping [**port-security**]
no ip verify source vlan dhcp-snooping [**port-security**]

Syntax Description

port-security	Enables IP/MAC mode and applies both IP and MAC filtering.

Command Default

Layer 2 IP source guard is disabled.

Command Modes

Service instance (config-if-srv)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRD	The **port-security**keyword was added.

Usage Guidelines

The **ip verify source vlan dhcp-snooping** command enables VLANs only on the configured service instance (EVC) and looks for DHCP snooping matches only for the configured bridge domain VLAN.

Examples

This example shows how to enable Layer 2 IP source guard on an interface:

```
Router# enable
Router# configure terminal
Router(config)# interface GigabitEthernet7/1
Router(config-if)# no ip address
Router(config-if)# service instance 71 ethernet
Router(config-if-srv)# encapsulation dot1q 71
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# ip verify source vlan dhcp-snooping
Router(config-if-srv)#  bridge-domain 10
```

Related Commands

Command	Description
service instance ethernet	Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.

ipv4-prefix

To configure an IPv4 prefix for a Network Address Translation 64 (NAT64) mapping of address and ports translation (MAP-T) basic mapping rule, use the **ipv4-prefix** command in NAT64 MAP-T BMR configuration mode. To remove the IPv4 prefix, use the **no** form of this command.

ipv4-prefix *ipv4-prefix/prefix-length*
no ipv4-prefix *ipv4-prefix/prefix-length*

Syntax Description

ipv4-prefix/prefix-length	IPv4 prefix in dotted decimal and the length of the IPv4 prefix. The prefix-length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

Command Modes

NAT64 MAP-T BMR configuration (config-nat64-mapt-bmr)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.
Cisco IOS Release 15.5(2)T	This command was integrated into Cisco IOS Release 15.5(2)T.

Usage Guidelines

MAP-T or Mapping of address and port (MAP) double stateless translation-based solution (MAP-T) provides IPv4 hosts connectivity to and across an IPv6 domain. MAP-T builds on existing stateless IPv4/IPv6 address translation techniques that are specified in RFC 6052, RFC 6144, and RFC 6145.

Examples

The following example shows how to configure an IPv4 prefix for a NAT64 MAP-T basic mapping rule:

```
Device(config)# nat64 map-t domain 89
Device(config-nat64-mapt)# basic-mapping-rule
Device(config-nat4-mapt-bmr)# ipv4-prefix 198.51.100.1/32
```

Related Commands

Command	Description
basic-mapping-rule	Configures a basic mapping rule for NAT64 MAP-T.
nat64 map-t	Configures NAT64 MAP-T settings.

ipv6 address autoconfig

To enable automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and enable IPv6 processing on the interface, use the **ipv6 address autoconfig** command in interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address autoconfig [**default**]
no ipv6 address autoconfig

Syntax Description

default	(Optional) If a default device is selected on this interface, the **default** keyword causes a default route to be installed using that default device. The **default** keyword can be specified only on one interface.

Command Default

No IPv6 address is defined for the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 address autoconfig** command causes the device to perform IPv6 stateless address auto-configuration to discover prefixes on the link and then to add the EUI-64 based addresses to the interface. Addresses are configured depending on the prefixes received in Router Advertisement (RA) messages.

Using the **no ipv6 address autoconfig** command without arguments removes all IPv6 addresses from an interface.

Examples

The following example assigns the IPv6 address automatically:

```
Device(config)# interface ethernet 0
Device(config-if)# ipv6 address autoconfig
```

Related Commands

Command	Description
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 unnumbered	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 address dhcp

To acquire an IPv6 address on an interface from the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server, use the **ipv6 address dhcp** command in the interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address dhcp [**rapid-commit**]
no ipv6 address dhcp

Syntax Description

rapid-commit	(Optional) Allows the two-message exchange method for address assignment.

Command Default

No IPv6 addresses are acquired from the DHCPv6 server.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 address dhcp** interface configuration command allows any interface to dynamically learn its IPv6 address by using DHCP.

The **rapid-commit** keyword enables the use of the two-message exchange for address allocation and other configuration. If it is enabled, the client includes the rapid-commit option in a solicit message.

Examples

The following example shows how to acquire an IPv6 address and enable the rapid-commit option:

```
Router(config)# interface fastethernet 0/0
Router(config-if)# ipv6 address dhcp
rapid-commit
```

You can verify your settings by using the **show ipv6 dhcp interface** command in privileged EXEC mode.

Related Commands

Command	Description
show ipv6 dhcp interface	Displays DHCPv6 interface information.

ipv6 address dhcp client request

To configure an IPv6 client to request a vendor-specific option from a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server, use the **ipv6 address dhcp client request** command in interface configuration mode. To remove the request, use the **no** form of this command.

ipv6 address dhcp client request vendor
no ipv6 address dhcp client request vendor

Syntax Description

vendor	Requests the vendor-specific options.

Command Default

IPv6 clients are not configured to request an option from DHCP.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)T	This command was introduced.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

Use the **ipv6 address dhcp client request vendor** command to request a vendor-specific option. When this command is enabled, the IPv6 client can request a vendor-specific option only when an IPv6 address is acquired from DHCP. If you enter the command after the interface has acquired an IPv6 address, the IPv6 client cannot request a vendor-specific option until the next time the client acquires an IPv6 address from DHCP.

Examples

The following example shows how to configure an interface to request vendor-specific options:

```
Router(config)# interface fastethernet 0/0
Router(config-if)# ipv6 address dhcp client request vendor
```

Related Commands

Command	Description
ipv6 address dhcp	Acquires an IPv6 address on an interface from the DHCPv6 server.

ipv6 dhcp binding track ppp

To configure Dynamic Host Configuration Protocol (DHCP) for IPv6 to release any bindings associated with a PPP connection when that connection closes, use the **ipv6 dhcp binding track ppp** command in global configuration mode. To return to the default behavior, use the **no** form of this command.

ipv6 dhcp binding track ppp
no ipv6 dhcp binding track ppp

Syntax Description

This command has no arguments or keywords.

Command Default

When a PPP connection closes, the DHCP bindings associated with that connection are not released.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.5	This command was introduced.

Usage Guidelines

The **ipv6 dhcp binding track ppp** command configures DHCP for IPv6 to automatically release any bindings associated with a PPP connection when that connection is closed. The bindings are released automatically to accommodate subsequent new registrations by providing sufficient resource.

Note In IPv6 broadband deployment using DHCPv6, you must enable release of prefix bindings associated with a PPP virtual interface using this command. This ensures that DHCPv6 bindings are tracked together with PPP sessions, and in the event of DHCP REBIND failure, the client initiates DHCPv6 negotiation again.

A binding table entry on the DHCP for IPv6 server is automatically:

- Created whenever a prefix is delegated to a client from the configuration pool.
- Updated when the client renews, rebinds, or confirms the prefix delegation.
- Deleted when the client releases all the prefixes in the binding voluntarily, all prefixes' valid lifetimes have expired, or an administrator clears the binding.

Examples

The following example shows how to release the prefix bindings associated with the PPP:

```
Router(config)# ipv6 dhcp binding track ppp
```

ipv6 dhcp client information refresh minimum

To configure the minimum acceptable Dynamic Host Configuration Protocol (DHCP) for IPv6 client information refresh time on a specified interface, use the **ipv6 dhcp client information refresh minimum**command in interface configuration mode. To remove the configured refresh time, use the **no** form of this command.

ipv6 dhcp client information refresh minimum *seconds*
no ipv6 dhcp client information refresh minimum *seconds*

Syntax Description

seconds	The refresh time, in seconds. The minimum value that can be used is 600 seconds.

Command Default

The default is 86,400 seconds (24 hours).

Command Modes

Interface configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

The **ipv6 dhcp client information refresh minimum**command specifies the minimum acceptable information refresh time. If the server sends an information refresh time option of less than the configured minimum refresh time, the configured minimum refresh time will be used instead.

This command may be configured in several situations:

- In unstable environments where unexpected changes are likely to occur.
- For planned changes, including renumbering. An administrator can gradually decrease the time as the planned event nears.
- Limit the amount of time before new services or servers are available to the client, such as the addition of a new Simple Network Time Protocol (SNTP) server or a change of address of a Domain Name System (DNS) server.

Examples

The following example configures an upper limit of 2 hours:

```
ipv6 dhcp client information refresh minimum 7200
```

ipv6 dhcp client pd

To enable the Dynamic Host Configuration Protocol (DHCP) for IPv6 client process and enable request for prefix delegation through a specified interface, use the **ipv6 dhcp client pd** command in interface configuration mode. To disable requests for prefix delegation, use the **no** form of this command.

ipv6 dhcp client pd {*prefix-name* | **hint** *ipv6-prefix*} [**rapid-commit**]
no ipv6 dhcp client pd

Syntax Description

prefix-name	IPv6 general prefix name.
hint	An IPv6 prefix sent as a hint.
ipv6-prefix	IPv6 general prefix.
rapid-commit	(Optional) Allow two-message exchange method for prefix delegation.

Command Default

Prefix delegation is disabled on an interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

Enabling the **ipv6 dhcp client pd**command starts the DHCP for IPv6 client process if this process is not yet running.

The **ipv6 dhcp client pd**command enables request for prefix delegation through the interface on which this command is configured. When prefix delegation is enabled and a prefix is successfully acquired, the prefix is stored in the IPv6 general prefix pool with an internal name defined by the *ipv6-prefix*argument. Other commands and applications (such as the **ipv6 address** command) can then refer to the prefixes in the general prefix pool.

The **hint** keyword with the *ipv6-prefix* argument enables the configuration of an IPv6 prefix that will be included in DHCP for IPv6 solicit and request messages sent by the DHCP for IPv6 client on the interface as a hint to prefix-delegating routers. Multiple prefixes can be configured by issuing the **ipv6 dhcp client pd hint***ipv6-prefix* command multiple times. The new prefixes will not overwrite old ones.

The **rapid-commit** keyword enables the use of the two-message exchange for prefix delegation and other configuration. If it is enabled, the client will include the rapid commit option in a solicit message.

The DHCP for IPv6 client, server, and relay functions are mutually exclusive on an interface. When one of these functions is already enabled and a user tries to configure a different function on the same interface, one of the following messages is displayed: "Interface is in DHCP client mode," "Interface is in DHCP server mode," or "Interface is in DHCP relay mode."

Examples

The following example enables prefix delegation:

```
Router(config-if)# ipv6 dhcp client pd dhcp-prefix
```

The following example configures a hint for prefix-delegating routers:

```
Router(config-if)# ipv6 dhcp client pd hint 2001:0DB8:1/48
```

Related Commands

Command	Description
clear ipv6 dhcp client	Restarts the DHCP for IPv6 client on an interface.
show ipv6 dhcp interface	Displays DHCP for IPv6 interface information.

ipv6 dhcp database

To configure a Dynamic Host Configuration Protocol (DHCP) for IPv6 binding database agent, use the **ipv6 dhcp database** command in global configuration mode. To delete the database agent, use the **no** form of this command.

ipv6 dhcp database *agent* [**write-delay** *seconds*] [**timeout** *seconds*]
no ipv6 dhcp database *agent*

Syntax Description

agent	A flash, local bootflash, compact flash, NVRAM, FTP, TFTP, or Remote Copy Protocol (RCP) uniform resource locator.
write-delay *seconds*	(Optional) How often (in seconds) DHCP for IPv6 sends database updates. The default is 300 seconds. The minimum write delay is 60 seconds.
timeout *seconds*	(Optional) How long, in seconds, the router waits for a database transfer.

Command Default

Write-delay default is 300 seconds. Timeout default is 300 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

The **ipv6 dhcp database** command specifies DHCP for IPv6 binding database agent parameters. The user may configure multiple database agents.

A binding table entry is automatically created whenever a prefix is delegated to a client from the configuration pool, updated when the client renews, rebinds, or confirms the prefix delegation, and deleted when the client releases all the prefixes in the binding voluntarily, all prefixes' valid lifetimes have expired, or administrators enable the clear ipv6 dhcp binding command. These bindings are maintained in RAM and can be saved to permanent storage using the *agent* argument so that the information about configuration such as prefixes assigned to clients is not lost after a system reload or power down. The bindings are stored as text records for easy maintenance.

Each permanent storage to which the binding database is saved is called the database agent. A database agent can be a remote host such as an FTP server or a local file system such as NVRAM.

The **write-delay** keyword specifies how often, in seconds, that DHCP sends database updates. By default, DHCP for IPv6 server waits 300 seconds before sending any database changes.

The **timeout** keyword specifies how long, in seconds, the router waits for a database transfer. Infinity is defined as 0 seconds, and transfers that exceed the timeout period are terminated. By default, the DHCP for IPv6 server waits 300 seconds before terminating a database transfer. When the system is going to reload, there is no transfer timeout so that the binding table can be stored completely.

Examples

The following example specifies DHCP for IPv6 binding database agent parameters and stores binding entries in TFTP:

```
ipv6 dhcp database tftp://10.0.0.1/dhcp-binding
```

The following example specifies DHCP for IPv6 binding database agent parameters and stores binding entries in bootflash:

```
ipv6 dhcp database bootflash
```

Related Commands

Command	Description
clear ipv6 dhcp binding	Deletes automatic client bindings from the DHCP for IPv6 server binding table
show ipv6 dhcp database	Displays DHCP for IPv6 binding database agent information.

ipv6 dhcp debug redundancy

To display debugging output for IPv6 DHCP high availability (HA) processing, use the **ipv6 dhcp debug redundancy**command in privileged EXEC mode. To disable debugging output, use the no form of this command.

ipv6 dhcp debug redundancy
no ipv6 dhcp debug redundancy

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

Use the **ipv6 dhcp debug redundancy** command to display stateful switchover (SSO) state transitions and errors.

Examples

The following example enables IPv6 DHCP redundancy debugging:

```
Router# ipv6 dhcp debug redundancy
```

ipv6 dhcp framed password

To assign a framed prefix when using a RADIUS server, use the **ipv6 dhcp framed password**command in interface configuration mode. To remove the framed prefix, use the **no** form of this command.

ipv6 dhcp framed password *password*
no ipv6 dhcp framed password

Syntax Description

password	Password to be used with the RADIUS server.

Command Default

No framed prefix is assigned.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 2.5	This command was introduced.

Usage Guidelines

The ipv6 dhcp framed password command enables a user to request a framed prefix of a RADIUS server. When a PPPoE client requests a prefix from a network using the framed-prefix system, the RADIUS server should assign an address. However, the RADIUS server is configured to receive a password. Because the client does not send a password, the RADIUS server does not send a framed prefix.



Note Ordinarily, the **ipv6 dhcp framed password** command will not need to be used because a client will have been authenticated as part of PPP session establishment.

Examples

The following example shows how to configure a password to be used with the RADIUS server:

```
Router(config-if)# ipv6 dhcp framed password password1
```

ipv6 dhcp guard attach-policy

To attach a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) guard policy, use the **ipv6 dhcp guard attach-policy** command in interface configuration or VLAN configuration mode. To unattach the DHCPv6 guard policy, use the **no** form of this command.

Syntax Available In Interface Configuration Mode
ipv6 dhcp guard [**attach-policy** [*policy-name*]] [**vlan** {**add** | **all** | **except** | **none** | **remove**} *vlan-id* [. . . *vlan-id*]]
no ipv6 dhcp guard [**attach-policy** [*policy-name*]] [**vlan** {**add** | **all** | **except** | **none** | **remove**} *vlan-id* [. . . *vlan-id*]]

Syntax Available In VLAN Configuration Mode
ipv6 dhcp guard attach-policy [*policy-name*]
no ipv6 dhcp guard attach-policy [*policy-name*]

Syntax Description

policy-name	(Optional) DHCPv6 guard policy name.
vlan	(Optional) Specifies that the DHCPv6 policy is to be attached to a VLAN.
add	(Optional) Attaches a DHCPv6 guard policy to the specified VLAN(s).
all	(Optional) Attaches a DHCPv6 guard policy to all VLANs.
except	(Optional) Attaches a DHCPv6 guard policy to all VLANs except the specified VLAN(s).
none	(Optional) Attaches a DHCPv6 guard policy to none of the specified VLAN(s).
remove	(Optional) Removes a DHCPv6 guard policy from the specified VLAN(s).
vlan-id	(Optional) Identity of the VLAN(s) to which the DHCP guard policy applies.

Command Default

No DHCPv6 guard policy is attached.

Command Modes

Interface configuration (config-if)

VLAN configuration (config-vlan)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

This command allows you to attach a DHCPv6 policy to an interface or to one or more VLANs. DHCPv6 guard policies can be used to block reply and advertisement messages that come from unauthorized DHCP servers and relay agents that forward DHCP packets from servers to clients. Client messages or messages sent by relay agents from clients to servers are not blocked.

Examples

The following example shows how to attach a DHCPv6 guard policy to an interface:

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet 0/2/0
Router# switchport
Router(config-if)# ipv6 dhcp guard attach-policy pol1 vlan add 1
```

Related Commands

Command	Description
ipv6 dhcp guard policy	Defines the DHCPv6 guard policy name.
show ipv6 dhcp guard policy	Displays DHCPv6 guard policy information.

ipv6 dhcp guard policy

To define a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) guard policy name, use the **ipv6 dhcp guard policy** command in global configuration mode. To remove the DHCPv6 guard policy name, use the **no** form of this command.

ipv6 dhcp guard policy [*policy-name*]
no ipv6 dhcp guard policy [*policy-name*]

Syntax Description

policy-name	(Optional) DHCPv6 guard policy name.

Command Default

No DHCPv6 guard policy name is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

This command allows you to enter DHCPv6 guard configuration mode. DHCPv6 guard policies can be used to block reply and advertisement messages that come from unauthorized DHCP servers and relay agents that forward DHCP packets from servers to clients. Client messages or messages sent by relay agents from clients to servers are not blocked.

Examples

The following example shows how to define a DHCPv6 guard policy name:

```
Router> enable
Router# configure terminal
Router(config)# ipv6 dhcp guard policy policy1
```

Related Commands

Command	Description
show ipv6 dhcp guard policy	Displays DHCPv6 guard policy information.

ipv6 dhcp iana-route-add

To add routes for individually assigned IPv6 addresses on a relay or server, use the **ipv6 dhcp iana-route-add** command in global configuration mode. To disable route addition for individually assigned IPv6 addresses on a relay or server, use the **no** form of the command.

ipv6 dhcp iana-route-add
no ipv6 dhcp iana-route-add

Syntax Description

This command has no arguments or keywords.

Command Default

Route addition for individually assigned IPv6 addresses on a relay or server is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(1)S	This command was introduced.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.

Usage Guidelines

The **ipv6 dhcp iana-route-add** command is disabled by default and has to be enabled if route addition is required. Route addition for Internet Assigned Numbers Authority (IANA) is possible if the client is connected to the relay or server through unnumbered interfaces, and if route addition is enabled with the help of this command.

Examples

The following example shows how to enable route addition for individually assigned IPv6 addresses:

```
Router> enable
Router# configure terminal
Router(config)# ipv6 dhcp iana-route-add
```

ipv6 dhcp iapd-route-add

To enable route addition by Dynamic Host Configuration Protocol for IPv6 (DHCPv6) relay and server for the delegated prefix, use the **ipv6 dhcp iapd-route-add** command in global configuration mode. To disable route addition, use the **no** form of the command.

ipv6 dhcp iapd-route-add
no ipv6 dhcp iapd-route-add

Syntax Description

This command has no arguments or keywords.

Command Default

DHCPv6 relay and DHCPv6 server add routes for delegated prefixes by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(1)S	This command was introduced.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.

Usage Guidelines

The DHCPv6 relay and the DHCPv6 server add routes for delegated prefixes by default. The presence of this command on a router does not mean that routes will be added on that router. When you configure the command, routes for delegated prefixes will only be added on the first Layer 3 relay and server.

Examples

The following example shows how to enable the DHCPv6 relay and server to add routes for a delegated prefix:

```
Router> enable
Router# configure terminal
Router(config)# ipv6 dhcp iapd-route-add
```

ipv6 dhcp-ldra

To enable Lightweight DHCPv6 Relay Agent (LDRA) functionality on an access node, use the **ipv6 dhcp-ldra** command in global configuration mode. To disable the LDRA functionality, use the **no** form of this command.

ipv6 dhcp-ldra {enable | disable}
no ipv6 dhcp-ldra {enable | disable}

Syntax Description

enable	Enables LDRA functionality on an access node.
disable	Disables LDRA functionality on an access node.

Command Default

By default, LDRA functionality is not enabled on an access node.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(2)SG	This command was introduced.
Cisco IOS XE Release 3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.

Usage Guidelines

You must configure the LDRA functionality globally using the **ipv6 dhcp-ldra** command before configuring it on a VLAN or an access node (such as a Digital Subscriber Link Access Multiplexer [DSLAM] or an Ethernet switch) interface.

Example

The following example shows how to enable the LDRA functionality:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 dhcp-ldra enable
Device(config)# exit
```

Note In the above example, Device denotes an access node.

Related Commands

Command	Description
ipv6 dhcp ldra attach-policy	Enables LDRA functionality on a VLAN.
ipv6 dhcp-ldra attach-policy	Enables LDRA functionality on an interface.

ipv6 dhcp-ldra attach-policy

To enable Lightweight DHCPv6 Relay Agent (LDRA) functionality on a port or interface, use the **ipv6 dhcp-ldra attach-policy** command in interface configuration mode. To disable LDRA functionality on an interface or port, use the **no** form of this command.

ipv6 dhcp-ldra attach-policy {client-facing-trusted | client-facing-untrusted | client-facing-disable | server-facing}
no ipv6 dhcp-ldra attach-policy {client-facing-trusted | client-facing-untrusted | client-facing-disable | server-facing}

Syntax Description

client-facing-trusted	Specifies client-facing interfaces or ports as trusted.
client-facing-untrusted	Specifies client-facing interfaces or ports as untrusted.
client-facing-disable	Disables LDRA functionality on an interface or port.
server-facing	Specifies an interface or port as server facing.

Command Default

By default, LDRA functionality is not enabled on an interface or port.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(2)SG	This command was introduced.
Cisco IOS XE Release 3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.

Usage Guidelines

You need to configure the LDRA functionality globally using the **ipv6 dhcp-ldra** command before configuring it on an interface or port.

The **ipv6 dhcp-ldra attach-policy** command enables LDRA functionality on a specific interface or port. Instead of configuring LDRA individually on all the client-facing interfaces or ports individually, use the **ipv6 dhcp ldra attach-policy** command to configure LDRA on an entire VLAN.

Example

The following example shows how to enable LDRA functionality on an interface and specify it as server facing:

```
Device>enable
Device#configure terminal
Device(config)# ipv6 dhcp-ldra enable
Device(config)# interface ethernet 0/0
Device(config-if)# switchport
Device(config-if)# ipv6 dhcp-ldra attach-policy server-facing
Device(config-if)# exit
```

Related Commands

Command	Description
ipv6 dhcp-ldra	Enables LDRA functionality on an access node.
ipv6 dhcp ldra attach-policy	Enables LDRA functionality on a VLAN.

ipv6 dhcp ldra attach-policy (VLAN)

To enable Lightweight DHCPv6 Relay Agent (LDRA) functionality on a VLAN, use the **ipv6 dhcp ldra attach-policy** command in VLAN configuration mode. To disable LDRA functionality on a VLAN, use the **no** form of this command.

ipv6 dhcp ldra attach-policy {client-facing-trusted | client-facing-untrusted}
no ipv6 dhcp ldra attach-policy {client-facing-trusted | client-facing-untrusted}

Syntax Description

client-facing-trusted	Specifies client-facing interfaces or ports as trusted.
client-facing-untrusted	Specifies client-facing interfaces or ports as untrusted.

Command Default

By default, the LDRA functionality is not enabled on a VLAN.

Command Modes

VLAN configuration (config-vlan-config)

Command History

Release	Modification
15.1(2)SG	This command was introduced.
Cisco IOS XE Release 3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.

Usage Guidelines

You need to configure the LDRA functionality globally using the **ipv6 dhcp-ldra** command before configuring it on a VLAN.

In a typical deployment, a majority of the interfaces or ports on a device are client facing. Instead of configuring LDRA individually on all the client facing interfaces and ports, use the **ipv6 dhcp ldra attach-policy** command to configure LDRA on the entire VLAN. As a result, all the ports or interfaces associated with the VLAN will be configured as client facing.

Example

The following example shows how to enable LDRA functionality on a VLAN:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 dhcp-ldra enable
Device(config)# vlan configuration 5
Device(config-vlan-config)# ipv6 dhcp ldra attach-policy client-facing-trusted
Device(config-vlan-config)# exit
```

Related Commands

Command	Description
ipv6 dhcp-ldra	Enables LDRA functionality on an access node.
ipv6 dhcp-ldra attach-policy	Enables LDRA functionality on an interface.

ipv6 dhcp ping packets

To specify the number of packets a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server sends to a pool address as part of a ping operation, use the **ipv6 dhcp ping packets** command in global configuration mode. To prevent the server from pinging pool addresses, use the **no** form of this command.

ipv6 dhcp ping packets *number*
ipv6 dhcp ping packets

Syntax Description

number	The number of ping packets sent before the address is assigned to a requesting client. The valid range is from 0 to 10.

Command Default

No ping packets are sent before the address is assigned to a requesting client.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The DHCPv6 server pings a pool address before assigning the address to a requesting client. If the ping is unanswered, the server assumes, with a high probability, that the address is not in use and assigns the address to the requesting client.

Setting the *number* argument to 0 turns off the DHCPv6 server ping operation

Examples

The following example specifies four ping attempts by the DHCPv6 server before further ping attempts stop:

```
Router(config)# ipv6 dhcp ping packets 4
```

Related Commands

Command	Description
clear ipv6 dhcp conflict	Clears an address conflict from the DHCPv6 server database.
show ipv6 dhcp conflict	Displays address conflicts found by a DHCPv6 server, or reported through a DECLINE message from a client.

ipv6 dhcp pool

To configure a Dynamic Host Configuration Protocol (DHCP) for IPv6 server configuration information pool and enter DHCP for IPv6 pool configuration mode, use the **ipv6 dhcp pool** command in global configuration mode. To delete a DHCP for IPv6 pool, use the **no** form of this command.

ipv6 dhcp pool *poolname*
no ipv6 dhcp pool *poolname*

Syntax Description

poolname	User-defined name for the local prefix pool. The pool name can be a symbolic string (such as "Engineering") or an integer (such as 0).

Command Default

DHCP for IPv6 pools are not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Use the **ipv6 dhcp pool**command to create a DHCP for IPv6 server configuration information pool. When the **ipv6 dhcp pool** command is enabled, the configuration mode changes to DHCP for IPv6 pool configuration mode. In this mode, the administrator can configure pool parameters, such as prefixes to be delegated and Domain Name System (DNS) servers, using the following commands:

- **address prefix** *IPv6-prefix* [**lifetime** {*valid-lifetime preferred-lifetime* | **infinite**}]sets an address prefix for address assignment. This address must be in hexadecimal, using 16-bit values between colons.
- **link-address** *IPv6-prefix* sets a link-address IPv6 prefix. When an address on the incoming interface or a link-address in the packet matches the specified IPv6-prefix, the server uses the configuration information pool. This address must be in hexadecimal, using 16-bit values between colons.
- **vendor-specific** *vendor-id* enables DHCPv6 vendor-specific configuration mode. Specify a vendor identification number. This number is the vendor IANA Private Enterprise Number. The range is 1 to 4294967295. The following configuration command is available:
  - **suboption** *number* sets vendor-specific suboption number. The range is 1 to 65535. You can enter an IPv6 address, ASCII text, or a hex string as defined by the suboption parameters.

Note The **hex** value used under the **suboption** keyword allows users to enter only hex digits (0-f). Entering an invalid **hex** value does not delete the previous configuration.

Once the DHCP for IPv6 configuration information pool has been created, use the **ipv6 dhcp server** command to associate the pool with a server on an interface. If you do not configure an information pool, you need to use the **ipv6 dhcp server interface** configuration command to enable the DHCPv6 server function on an interface.

When you associate a DHCPv6 pool with an interface, only that pool services requests on the associated interface. The pool also services other interfaces. If you do not associate a DHCPv6 pool with an interface, it can service requests on any interface.

Not using any IPv6 address prefix means that the pool returns only configured options.

The **link-address** command allows matching a link-address without necessarily allocating an address. You can match the pool from multiple relays by using multiple link-address configuration commands inside a pool.

Since a longest match is performed on either the address pool information or the link information, you can configure one pool to allocate addresses and another pool on a subprefix that returns only configured options.

Examples

The following example specifies a DHCP for IPv6 configuration information pool named cisco1 and places the router in DHCP for IPv6 pool configuration mode:

```
Router(config)# ipv6 dhcp pool cisco1
Router(config-dhcpv6)#
```

The following example shows how to configure an IPv6 address prefix for the IPv6 configuration pool cisco1:

```
Router(config-dhcpv6)# address prefix 2001:1000::0/64
Router(config-dhcpv6)# end
```

The following example shows how to configure a pool named engineering with three link-address prefixes and an IPv6 address prefix:

```
Router# configure terminal
Router(config)# ipv6 dhcp pool engineering
Router(config-dhcpv6)# link-address 2001:1001::0/64
Router(config-dhcpv6)# link-address 2001:1002::0/64
Router(config-dhcpv6)# link-address 2001:2000::0/48
Router(config-dhcpv6)# address prefix 2001:1003::0/64
Router(config-dhcpv6)# end
```

The following example shows how to configure a pool named 350 with vendor-specific options:

```
Router# configure terminal
Router(config)# ipv6 dhcp pool 350
Router(config-dhcpv6)# vendor-specific 9
Router(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Router(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
Router(config-dhcpv6-vs)# end
```

Related Commands

Command	Description
ipv6 dhcp server	Enables DHCP for IPv6 service on an interface.
show ipv6 dhcp pool	Displays DHCP for IPv6 configuration pool information.

ipv6 dhcp relay destination

To specify a destination address to which client messages are forwarded and to enable Dynamic Host Configuration Protocol (DHCP) for IPv6 relay service on the interface, use the **ipv6 dhcp relay destination** command in interface configuration mode. To remove a relay destination on the interface or to delete an output interface for a destination, use the **no** form of this command.

ipv6 dhcp relay destination *ipv6-address* [*interface-type interface-number* | **vrf** *vrf-name* | **global**]
no ipv6 dhcp relay destination *ipv6-address* [*interface-type interface-number* | **vrf** *vrf-name* | **global**]

Cisco CMTS Routers

ipv6 dhcp relay destination *ipv6-address* [*interface-type interface-number*] [**link-address** *link-address*] [**source-address***source-address*]
no ipv6 dhcp relay destination *ipv6-address* [*interface-type interface-number*] [**link-address** *link-address*] [**source-address** *source-address*]

Syntax Description

ipv6-address	Relay destination address. There are two types of relay destination address: • Link-scoped unicast or multicast IPv6 address. A user must specify an output interface for this kind of address. • Global or site-scoped unicast or multicast IPv6 address. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
interface-type interface-number	(Optional) Interface type and number that specifies the output interface for a destination. If this argument is configured, client messages are forwarded to the destination address through the link to which the output interface is connected.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) associated with the relay destination IPv6 address.
global	(Optional) Specifies the relay destination when the relay destination is in the global address space and when the relay source is in a VRF.
link-address *link-address*	(Optional) Specifies the DHCPv6 link address. The link-address must be an IPv6 globally scoped address configured on the network interface where the DHCPv6 relay is operational.
source-address *source-address*	(Optional) Specifies the Cisco CMTS network interface source address. The source-address can be any IPv6 global-scoped address on the router.

Command Default

The relay function is disabled, and there is no relay destination on an interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(2)S	This command was modified. The **vrf** *vrf-name* keyword and argument were added. The **global** keyword was added.
Cisco IOS XE Release 3.3S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
12.2(33)SCE5	This command was integrated into Cisco IOS Release 12.2(33)SCE5. The **link-address** and **source-address** keywords were added.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Usage Guidelines

The **ipv6 dhcp relay destination** command specifies a destination address to which client messages are forwarded, and it enables DHCP for IPv6 relay service on the interface. When relay service is enabled on an interface, a DHCP for IPv6 message received on that interface will be forwarded to all configured relay destinations. The incoming DHCP for IPv6 message may have come from a client on that interface, or it may have been relayed by another relay agent.

The relay destination can be a unicast address of a server or another relay agent, or it may be a multicast address. There are two types of relay destination addresses:

- A link-scoped unicast or multicast IPv6 address, for which a user must specify an output interface
- A global or site-scoped unicast or multicast IPv6 address. A user can optionally specify an output interface for this kind of address.

If no output interface is configured for a destination, the output interface is determined by routing tables. In this case, it is recommended that a unicast or multicast routing protocol be running on the router.

Multiple destinations can be configured on one interface, and multiple output interfaces can be configured for one destination. When the relay agent relays messages to a multicast address, it sets the hop limit field in the IPv6 packet header to 32.

Unspecified, loopback, and node-local multicast addresses are not acceptable as the relay destination. If any one of them is configured, the message "Invalid destination address" is displayed.

Note that it is not necessary to enable the relay function on an interface for it to accept and forward an incoming relay reply message from servers. By default, the relay function is disabled, and there is no relay destination on an interface. The **no** form of the command removes a relay destination on an interface or deletes an output interface for a destination. If all relay destinations are removed, the relay service is disabled on the interface.

The DHCP for IPv6 client, server, and relay functions are mutually exclusive on an interface. When one of these functions is already enabled and a user tries to configure a different function on the same interface, one of the following messages is displayed: "Interface is in DHCP client mode," "Interface is in DHCP server mode," or "Interface is in DHCP relay mode."

In Cisco CMTS, if you change one or more parameters of this command, you have to disable the command using the no form, and execute the command again with changed parameters.

The default behavior (when **no source-address**, **link-address**, and **no output interface** commands are provisioned in the **ipv6 dhcp relay destination** command) of the new functionality is to copy the Cisco IOS SAS-computed source address to the link-address of the DHCPv6 relay-forward message.

Examples

The following example sets the relay destination address on Ethernet interface 4/3:

```
ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 ethernet 4/3
```

The following example shows how to set the relay destination address on the Ethernet interface 4/3 on a Cisco CMTS router:

```
ipv6 dhcp relay destination 2001:db8:1234:5678:9abc:def1:2345:6789 ethernet 4/3
```

Related Commands

Command	Description
show ipv6 dhcp interface	Displays DHCP for IPv6 interface information.

ipv6 dhcp-relay source-interface

To configure an interface to use as the source when relaying messages, use the **ipv6 dhcp-relay source-interface**command in global configuration mode. To remove the interface from use as the source, use the no form of this command.

ipv6 dhcp-relay source-interface *interface-type interface-number*
no ipv6 dhcp-relay source-interface *interface-type interface-number*

Syntax Description

interface-type *interface-number*	(Optional) Interface type and number that specifies output interface for a destination. If this argument is configured, client messages are forwarded to the destination address through the link to which the output interface is connected.

Command Default

The address of the server-facing interface is used as the IPv6 relay source.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

If the configured interface is shut down, or if all of its IPv6 addresses are removed, the relay will revert to its standard behavior.

The interface configuration (using the **ipv6 dhcp relay source-interface** command in interface configuration mode) takes precedence over the global configuration if both have been configured.

Examples

The following example configures the Loopback 0 interface to be used as the relay source:

```
Router(config)# ipv6 dhcp-relay source-interface loopback 0
```

Related Commands

Command	Description
ipv6 dhcp relay source-interface	Enables DHCP for IPv6 service on an interface.

ipv6 dhcp-relay bulk-lease

To configure bulk lease query parameters, use the **ipv6 dhcp-relay bulk-lease**command in global configuration mode. To remove the bulk-lease query configuration, use the **no** form of this command.

ipv6 dhcp-relay bulk-lease {**data-timeout** *seconds* | **retry** *number*} [**disable**]
no ipv6 dhcp-relay bulk-lease [**disable**]

Syntax Description

data-timeout	(Optional) Bulk lease query data transfer timeout.
seconds	(Optional) The range is from 60 seconds to 600 seconds. The default is 300 seconds.
retry	(Optional) Sets the bulk lease query retries.
number	(Optional) The range is from 0 to 5. The default is 5.
disable	(Optional) Disables the DHCPv6 bulk lease query feature.

Command Default

Bulk lease query is enabled automatically when the DHCP for IPv6 (DHCPv6) relay agent feature is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)S	This command was introduced.

Usage Guidelines

Use the **ipv6 dhcp-relay bulk-lease**command in global configuration mode to configure bulk lease query parameters, such as data transfer timeout and bulk-lease TCP connection retries.

The DHCPv6 bulk lease query feature is enabled automatically when the DHCPv6 relay agent is enabled. The DHCPv6 bulk lease query feature itself cannot be enabled using this command. To disable this feature, use the **ipv6 dhcp-relay bulk-lease**command with the **disable** keyword.

Examples

The following example shows how to set the bulk lease query data transfer timeout to 60 seconds:

```
Router(config)# ipv6 dhcp-relay bulk-lease data-timeout 60
```

Related Commands

Command	Description

ipv6 dhcp-relay option vpn

To enable the DHCP for IPv6 relay VRF-aware feature, use the ipv6 dhcp-relay option vpn command in global configuration mode. To disable the feature, use the **no** form of this command.

ipv6 dhcp-relay option vpn
no ipv6 dhcp-relay option vpn

Syntax Description

This command has no arguments or keywords.

Command Default

The DHCP for IPv6 relay VRF-aware feature is not enabled on the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(2)S	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Usage Guidelines

The **ipv6 dhcp-relay option vpn** command allows the DHCPv6 relay VRF-aware feature to be enabled globally on the router. If the **ipv6 dhcp relay option vpn** command is enabled on a specified interface, it overrides the global **ipv6 dhcp-relay option vpn** command.

Examples

The following example enables the DHCPv6 relay VRF-aware feature globally on the router:

```
Router(config)# ipv6 dhcp-relay option vpn
```

Related Commands

Command	Description
ipv6 dhcp relay option vpn	Enables the DHCPv6 relay VRF-aware feature on an interface.

ipv6 dhcp-relay show bindings

To enable the DHCPv6 relay agent to list prefix delegation (PD) bindings, use the **ipv6 dhcp-relay show bindings**command in global configuration mode. To disable PD binding tracking, use the no form of this command.

ipv6 dhcp-relay show bindings
no ipv6 dhcp-relay show bindings

Syntax Description

This command has no arguments or keywords.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

The **ipv6 dhcp-relay show bindings** command lists the PD bindings that the relay agent is tracking. The command lists the bindings in the relay's radix tree, lists DHCPv6 relay routes, and prints each entry's prefix and length, client identity association identification (IAID), and lifetime. <<Any more information here?>>

Examples

The following example enables the DHCPv6 relay agent to list PD bindings: <<OK?>>:

```
Router# ipv6 dhcp-relay show bindings
```

ipv6 dhcp-relay source-interface

To configure an interface to use as the source when relaying messages, use the **ipv6 dhcp-relay source-interface**command in global configuration mode. To remove the interface from use as the source, use the no form of this command.

ipv6 dhcp-relay source-interface *interface-type interface-number*
no ipv6 dhcp-relay source-interface *interface-type interface-number*

Syntax Description

interface-type *interface-number*	(Optional) Interface type and number that specifies output interface for a destination. If this argument is configured, client messages are forwarded to the destination address through the link to which the output interface is connected.

Command Default

The address of the server-facing interface is used as the IPv6 relay source.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

If the configured interface is shut down, or if all of its IPv6 addresses are removed, the relay will revert to its standard behavior.

The interface configuration (using the **ipv6 dhcp relay source-interface** command in interface configuration mode) takes precedence over the global configuration if both have been configured.

Examples

The following example configures the Loopback 0 interface to be used as the relay source:

```
Router(config)# ipv6 dhcp-relay source-interface loopback 0
```

Related Commands

Command	Description
ipv6 dhcp relay source-interface	Enables DHCP for IPv6 service on an interface.

ipv6 dhcp server

To enable Dynamic Host Configuration Protocol (DHCP) for IPv6 service on an interface, use the **ipv6 dhcp server** in interface configuration mode. To disable DHCP for IPv6 service on an interface, use the **no** form of this command.

ipv6 dhcp server [*poolname* | **automatic**] [**rapid-commit**] [**preference** *value*] [**allow-hint**]
no ipv6 dhcp server

Syntax Description

poolname	(Optional) User-defined name for the local prefix pool. The pool name can be a symbolic string (such as "Engineering") or an integer (such as 0).
automatic	(Optional) Enables the server to automatically determine which pool to use when allocating addresses for a client.
rapid-commit	(Optional) Allows the two-message exchange method for prefix delegation.
preference *value*	(Optional) Specifies the preference value carried in the preference option in the advertise message sent by the server. The range is from 0 to 255. The preference value defaults to 0.
allow-hint	(Optional) Specifies whether the server should consider delegating client suggested prefixes. By default, the server ignores client-hinted prefixes.

Command Default

DHCP for IPv6 service on an interface is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.4(24)T	The **automatic** keyword was added.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 dhcp server** command enables DHCP for IPv6 service on a specified interface using the pool for prefix delegation and other configuration through that interface.

The **automatic** keyword enables the system to automatically determine which pool to use when allocating addresses for a client. When an IPv6 DHCP packet is received by the server, the server determines if it was received from a DHCP relay or if it was directly received from the client. If the packet was received from a

relay, the server verifies the link-address field inside the packet associated with the first relay that is closest to the client. The server matches this link address against all address prefix and link-address configurations in IPv6 DHCP pools to find the longest prefix match. The server selects the pool associated with the longest match.

If the packet was directly received from the client, the server performs this same matching, but it uses all the IPv6 addresses configured on the incoming interface when performing the match. Once again, the server selects the longest prefix match.

The **rapid-commit** keyword enables the use of the two-message exchange for prefix delegation and other configuration. If a client has included a rapid commit option in the solicit message and the **rapid-commit** keyword is enabled for the server, the server responds to the solicit message with a reply message.

If the **preference** keyword is configured with a value other than 0, the server adds a preference option to carry the preference value for the advertise messages. This action affects the selection of a server by the client. Any advertise message that does not include a preference option is considered to have a preference value of 0. If the client receives an advertise message that includes a preference option with a preference value of 255, the client immediately sends a request message to the server from which the advertise message was received.

If the **allow-hint** keyword is specified, the server will delegate a valid client-suggested prefix in the solicit and request messages. The prefix is valid if it is in the associated local prefix pool and it is not assigned to a device. If the **allow-hint** keyword is not specified, a hint is ignored and a prefix is delegated from the free list in the pool.

The DHCP for IPv6 client, server, and relay functions are mutually exclusive on an interface. When one of these functions is already enabled and a user tries to configure a different function on the same interface, one of the following messages is displayed:

```
Interface is in DHCP client mode
Interface is in DHCP server mode
Interface is in DHCP relay mode
```

Examples

The following example enables DHCP for IPv6 for the local prefix pool named server1:

```
Router(config-if)# ipv6 dhcp server server1
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCP for IPv6 pool and enters DHCP for IPv6 pool configuration mode.
show ipv6 dhcp interface	Displays DHCP for IPv6 interface information.

ipv6 dhcp server vrf enable

To enable the DHCP for IPv6 server VRF-aware feature, use the **ipv6 dhcp server vrf enable**command in global configuration mode. To disable the feature, use the **no** form of this command.

ipv6 dhcp server vrf enable
no ipv6 dhcp server vrf enable

Syntax Description

This command has no arguments or keywords.

Command Default

The DHCPv6 server VRF-aware feature is not enabled on the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(2)S	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Usage Guidelines

The **ipv6 dhcp server option vpn** command allows the DHCPv6 server VRF-aware feature to be enabled globally on the router.

Examples

The following example enables the DHCPv6 server VRF-aware feature globally on the router:

```
Router(config)# ipv6 dhcp server option vpn
```

ipv6 inspect tcp finwait-time

To define how long a TCP session will be managed after the firewall detects a FIN-exchange, use the **ipv6 inspect tcp finwait-timeip inspect tcp finwait-time**command in global configuration mode. To reset the timeout to the default of 5 seconds, use the **no** form of this command.

ipv6 inspect tcp finwait-time *seconds*
no ipv6 inspect tcp finwait-time

Syntax Description

seconds	Specifies how long a TCP session will be managed after the firewall detects a FIN-exchange. The default is 5 seconds. Valid values are from 1 to 2147483.

Command Default

Command Modes

Global configuration (config)

Command History

Release	Modification

Usage Guidelines

Examples

Related Commands

Command	Description

ipv6 nd managed-config-flag

To set the "managed address configuration flag" in IPv6 router advertisements, use the **ipv6 nd managed-config-flag**command in interface configuration mode. To clear the flag from IPv6 router advertisements, use the **no** form of this command.

ipv6 nd managed-config-flag
no ipv6 nd managed-config-flag

Syntax Description

This command has no arguments or keywords.

Command Default

The "managed address configuration flag" flag is not set in IPv6 router advertisements.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Setting the "managed address configuration flag" flag in IPv6 router advertisements indicates to attached hosts whether they should use stateful autoconfiguration to obtain addresses. If the flag is set, the attached hosts should use stateful autoconfiguration to obtain addresses. If the flag is not set, the attached hosts should not use stateful autoconfiguration to obtain addresses.

Hosts may use stateful and stateless address autoconfiguration simultaneously.

Examples

The following example configures the "managed address configuration flag" flag in IPv6 router advertisements on Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd managed-config-flag
```

Related Commands

Command	Description
ipv6 nd prefix-advertisement	Configures which IPv6 prefixes are included in IPv6 router advertisements

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd other-config-flag

To set the "other stateful configuration" flag in IPv6 router advertisements, use the **ipv6 nd other-config-flag**command in interface configuration mode. To clear the flag from IPv6 router advertisements, use the **no** form of this command.

ipv6 nd other-config-flag
no ipv6 nd other-config-flag

Syntax Description

This command has no arguments or keywords.

Command Default

The "other stateful configuration" flag is not set in IPv6 router advertisements.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

The setting of the "other stateful configuration" flag in IPv6 router advertisements indicates to attached hosts how they can obtain autoconfiguration information other than addresses. If the flag is set, the attached hosts should use stateful autoconfiguration to obtain the other (nonaddress) information.



Note If the "managed address configuration" flag is set using the **ipv6 nd managed-config-flag** command, then an attached host can use stateful autoconfiguration to obtain the other (nonaddress) information regardless of the setting of the "other stateful configuration" flag.

Examples

The following example configures the "other stateful configuration" flag in IPv6 router advertisements on Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd other-config-flag
```

Related Commands

Command	Description
ipv6 nd managed-config-flag	Sets the "managed address configuration" flag in IPv6 router advertisements.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6-prefix

To configure an IPv6 address for a Network Address Translation 64 (NAT64) mapping of address and ports translation (MAP-T) basic mapping rule, use the **ipv6-prefix** command in NAT64 MAP-T BMR configuration mode. To remove the IPv6 address, use the **no** form of this command.

ipv6-prefix *ipv6-prefix/prefix-length*
no ipv6-prefix

Syntax Description

ipv6-prefix/prefix-length	The IPv6 address assigned to the interface and the length of the IPv6 prefix. The prefix-length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

Command Modes

NAT64 MAP-T BMR configuration (config-nat64-mapt-bmr)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.
Cisco IOS Release 15.5(2)T	This command was integrated into Cisco IOS Release 15.5(2)T.

Usage Guidelines

MAP-T or Mapping of address and port (MAP) double stateless translation-based solution (MAP-T) provides IPv4 hosts connectivity to and across an IPv6 domain. MAP-T builds on existing stateless IPv4/IPv6 address translation techniques that are specified in RFC 6052, RFC 6144, and RFC 6145.

Examples

The following example shows how to configure an IPv6 address for a NAT64 MAP-T basic mapping rule:

```
Device(config)# nat64 map-t domain 89
Device(config-nat64-mapt)# basic-mapping-rule
Device(config-nat4-mapt-bmr)# ipv6-prefix 2001:0DB8:0:1::/64
```

Related Commands

Command	Description
basic-mapping-rule	Configures a basic mapping rule for NAT64 MAP-T.
nat64 map-t	Configures NAT64 MAP-T settings.

iterate-ip-addrs

To display the interface descriptor blocks (IDBs) that are visited by the IP iterators, use the **iterate-ip-addrs** command in privileged EXEC mode.

iterate-ip-addrs *target-ip-address mask* [**secondary**] [**time-only**]

Syntax Description

target-ip-address	Target IP address.
mask	Target IP address mask.
secondary	(Optional) Displays the secondary addresses.
time-only	(Optional) Displays only the time measurements of all macros.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRB	This command was integrated in a release earlier than Cisco IOS Release 12.2(33)SRB.

Examples

The following is sample output of the **iterate-ip-addrs secondary** command:

```
Router# iterate-ip-addrs 10.0.0.1 255.0.0.0 secondary
target = 10.0.0.1, mask = 255.0.0.0, sec = TRUE
  interface            primary address     tableid
  -------------------- ------------------  ----------
FOR_SWIDBS_WITH_IPADDR(idb, tbl, target, sec, cref) visits
        ExecTime=0 microsec
FOR_SWIDBS_ON_IPSUBNET(idb, tbl, target & mask, mask, sec, cref) visits
  Gi6/2                     10.4.9.87/24  0x00000000
        ExecTime=1 microsec
FOR_SWIDBS_WITH_IPNETADDR(idb, tbl, target, mask, sec, cref) visits
        ExecTime=1 microsec
FOR_SWIDBS_WHOSE_SUBNET_HAS_IPADDR(idb, tbl, target, sec, cref) visits
        ExecTime=1 microsec
FOR_NUMBERED_SWIDBS(idb, tbl, cref) visits
  Gi6/2                      10.4.9.87/24  0x00000000
  EO0/0                     192.0.2.51/8   0x00000FFF
  Gi1/1                      10.1.1.1/24   0x00000000
  Vl1                    192.0.2.1/24  0x00000000
        ExecTime=2 microsec
  interface            address             tableid
  -------------------- ------------------  ----------
FOR_ENTRIES_ON_IPSUBNET(addr, tbl, target & mask, mask, cref) visits
  Gi6/2                      10.4.9.87/24  0x00000000
        ExecTime=2 microsec
FOR_NUMBERED_ENTRIES(addr, tbl, cref) visits
  Gi6/2                      10.4.9.87/24  0x00000000
  EO0/0                     192.0.2.51/8   0x00000FFF
  Gi1/1                      10.1.1.1/24   0x00000000
  Vl1                    192.0.2.1/24  0x00000000
```

```
        ExecTime=2 microsec
FOR_ALL_IPADDR_ENTRIES(addr, tbl, cref) visits
  Gi6/2                      10.4.9.87/24  0x00000000
  EO0/0                     192.0.2.51/8   0x00000FFF
  Gi1/1                      10.1.1.1/24   0x00000000
  Vl1                    192.0.2.1/24  0x00000000
        ExecTime=2 microsec
FOR_ALL_IPADDR_ENTRIES_WITH_IPADDR(addr, tbl, target, cref) visits
        ExecTime=1 microsec
FOR_TYPED_IPADDR_ENTRIES(addr, tbl, cref) visits ALIAS
        ExecTime=1 microsec
FOR_TYPED_IPADDR_ENTRIES(addr, tbl, cref) visits INTERFACE
  Gi6/2                      10.4.9.87/24  0x00000000
  EO0/0                     192.0.2.51/8   0x00000FFF
  Gi1/1                      10.1.1.1/24   0x00000000
  Vl1                    192.0.2.1/24  0x00000000
        ExecTime=1 microsec
FOR_TYPED_IPADDR_ENTRIES(addr, tbl, cref) visits ALL
  Gi6/2                      10.4.9.87/24  0x00000000
  EO0/0                     192.0.2.51/8   0x00000FFF
  Gi1/1                      10.1.1.1/24   0x00000000
  Vl1                    192.0.2.1/24  0x00000000
        ExecTime=2 microsec
Summary
Macro No. 0     ExecTime=0 microsec
Macro No. 1     ExecTime=1 microsec
Macro No. 2     ExecTime=1 microsec
Macro No. 3     ExecTime=1 microsec
Macro No. 4     ExecTime=2 microsec
Macro No. 5     ExecTime=2 microsec
Macro No. 6     ExecTime=2 microsec
Macro No. 7     ExecTime=2 microsec
Macro No. 8     ExecTime=1 microsec
Macro No. 9     ExecTime=1 microsec
Macro No. 10    ExecTime=1 microsec
Macro No. 11    ExecTime=2 microsec
Router# iterate-ip-addrs 10.0.0.1 255.0.0.0 secondary time-only

target = 10.0.0.1, mask = 255.0.0.0, sec = TRUE
  interface            primary address     tableid
  -------------------- ------------------  ----------
FOR_SWIDBS_WITH_IPADDR(idb, tbl, target, sec, cref) visits
        ExecTime=1 microsec
FOR_SWIDBS_ON_IPSUBNET(idb, tbl, target & mask, mask, sec, cref) visits
        ExecTime=2 microsec
FOR_SWIDBS_WITH_IPNETADDR(idb, tbl, target, mask, sec, cref) visits
        ExecTime=1 microsec
FOR_SWIDBS_WHOSE_SUBNET_HAS_IPADDR(idb, tbl, target, sec, cref) visits
        ExecTime=1 microsec
FOR_NUMBERED_SWIDBS(idb, tbl, cref) visits
        ExecTime=2 microsec
interface            address             tableid
  -------------------- ------------------  ----------
FOR_ENTRIES_ON_IPSUBNET(addr, tbl, target & mask, mask, cref) visits
        ExecTime=1 microsec
FOR_NUMBERED_ENTRIES(addr, tbl, cref) visits
        ExecTime=2 microsec
FOR_ALL_IPADDR_ENTRIES(addr, tbl, cref) visits
        ExecTime=2 microsec
FOR_ALL_IPADDR_ENTRIES_WITH_IPADDR(addr, tbl, target, cref) visits
        ExecTime=0 microsec
FOR_TYPED_IPADDR_ENTRIES(addr, tbl, cref) visits ALIAS
        ExecTime=1 microsec
FOR_TYPED_IPADDR_ENTRIES(addr, tbl, cref) visits INTERFACE
```

```
        ExecTime=1 microsec
FOR_TYPED_IPADDR_ENTRIES(addr, tbl, cref) visits ALL
        ExecTime=2 microsec
Summary
Macro No. 0     ExecTime=1 microsec
Macro No. 1     ExecTime=2 microsec
Macro No. 2     ExecTime=1 microsec
Macro No. 3     ExecTime=1 microsec
Macro No. 4     ExecTime=2 microsec
Macro No. 5     ExecTime=1 microsec
Macro No. 6     ExecTime=2 microsec
Macro No. 7     ExecTime=2 microsec
Macro No. 8     ExecTime=0 microsec
Macro No. 9     ExecTime=1 microsec
Macro No. 10    ExecTime=1 microsec
Macro No. 11    ExecTime=2 microsec
```



lease through renew dhcp

- lease, on page 544
- local-ip (IPC transport-SCTP local), on page 546
- local-port, on page 548
- logging (cfg-dns-view), on page 549
- logging (DNS), on page 550
- logging server-arp, on page 551
- mac packet-classify, on page 553
- mac packet-classify use vlan, on page 555
- match learnt-interface, on page 556
- match location, on page 558
- match message-type, on page 560
- match reply prefix-list, on page 561
- match server access-list, on page 562
- match service-instance, on page 563
- match service-type, on page 564
- mode (nat64), on page 565
- name, on page 566
- nat64 enable, on page 567
- nat64 logging, on page 568
- nat64 logging translations flow-export, on page 569
- nat64 map-t, on page 571
- nat64 prefix stateful, on page 572
- nat64 prefix stateless, on page 574
- nat64 route, on page 576
- nat64 service ftp, on page 577
- nat64 settings, on page 578
- nat64 settings eif , on page 579
- nat64 settings flow-entries disable, on page 580
- nat64 settings mtu minimum, on page 582
- nat64 switchover replicate http, on page 583
- nat64 translation, on page 584
- nat64 v4, on page 585
- nat64 v4v6, on page 586

- nat64 v6v4, on page 588
- nat66 inside, on page 590
- nat66 outside, on page 591
- nat66 prefix, on page 592
- netbios-name-server, on page 593
- netbios-node-type, on page 594
- network (DHCP), on page 595
- next-server, on page 597
- nhrp cache limit, on page 598
- nhrp group, on page 600
- nhrp map group, on page 602
- nis address, on page 604
- nis domain-name, on page 605
- nisp domain-name, on page 606
- nisp address, on page 607
- odap client, on page 608
- odap server, on page 609
- option, on page 610
- option hex, on page 612
- option ext, on page 614
- origin, on page 616
- override default-router, on page 618
- override utilization high, on page 620
- override utilization low, on page 621
- port-parameters, on page 622
- preempt, on page 623
- preference (DHCPv6 Guard), on page 624
- prefix-delegation, on page 625
- prefix-delegation aaa, on page 627
- prefix-delegation pool, on page 630
- priority (firewall), on page 632
- protocol, on page 633
- rate-limit (mDNS), on page 634
- rbe nasip, on page 636
- redistribute mdns-sd, on page 638
- redundancy, on page 640
- redundancy asymmetric-routing enable, on page 645
- redundancy group, on page 646
- redundancy group (interface), on page 647
- relay agent information, on page 649
- relay destination, on page 650
- relay source, on page 651
- relay target, on page 652
- relay-information hex, on page 654
- release dhcp, on page 656
- remote command, on page 658

- remote login, on page 660
- remote-ip (IPC transport-SCTP remote), on page 662
- remote-port, on page 664
- remote-span, on page 665
- renew deny unknown, on page 666
- renew dhcp, on page 668

lease

To configure the duration of the lease for an IP address that is assigned from a Cisco IOS Dynamic Host Configuration Protocol (DHCP) server to a DHCP client, use the **lease** command in DHCP pool configuration mode. To restore the default value, use the no form of this command.

lease {*days* [*hours* [*minutes*]] | **infinite**}
no lease

Syntax Description

days	Specifies the duration of the lease in numbers of days.
hours	(Optional) Specifies the number of hours in the lease. A *days* value must be supplied before you can configure an *hours* value.
minutes	(Optional) Specifies the number of minutes in the lease. A *days* value and an *hours* value must be supplied before you can configure a *minutes* value.
infinite	Specifies that the duration of the lease is unlimited.

Command Default

1 day

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows a 1-day lease:

```
lease 1
```

The following example shows a 1-hour lease:

```
lease 0 1
```

The following example shows a 1-minute lease:

```
lease 0 0 1
```

The following example shows an infinite (unlimited) lease:

```
lease infinite
```

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

local-ip (IPC transport-SCTP local)

To define at least one local IP address that is used to communicate with the local peer, use the **local-ip**command in IPC transport-SCTP local configuration mode. To remove one or all IP addresses from your configuration, use the **no** form of this command.

local-ip *device-real-ip-address* [*device-real-ip-address2*]
no local-ip *device-real-ip-address* [*device-real-ip-address2*]

Syntax Description

device-real-ip-address	IP address of the local device. The local IP addresses must match the remote IP addresses on the peer router. There can be either one or two IP addresses, which must be in global Virtual Private Network (VPN) routing and forwarding (VRF). A virtual IP (VIP) address cannot be used.
device-real-ip-address2	(Optional) IP address of the local device.

Command Default

No IP addresses are defined; thus, peers cannot communicate with the local peer.

Command Modes

IPC transport-SCTP local configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use the **local-ip** command to help associate Stream Control Transmission Protocol (SCTP) as the transport protocol between the local and remote peer.

This command is part of a suite of commands used to configure the Stateful Switchover (SSO) protocol. SSO is necessary for IP Security (IPSec) and Internet Key Exchange (IKE) to learn about the redundancy state of the network and to synchronize their internal application state with their redundant peers.

Examples

The following example shows how to enable SSO:

```
!
redundancy inter-device
 scheme standby HA-in
!
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 10.0.0.1
   remote-port 5000
    remote-ip 10.0.0.2
```

Related Commands

Command	Description
local-port	Defines the local SCTP port number that is used to communicate with the redundant peer.
remote-ip	Defines at least one remote IP address that is used to communicate with the redundant peer.

local-port

To define the local Stream Control Transmission Protocol (SCTP) port that is used to communicate with the redundant peer, use the **local-port**command in SCTP protocol configuration mode.

local-port *local-port-number*

Syntax Description

local-port-number	Local port number, which should be the same as the remote port number on the peer router (which is specified via the **remote-port** command).

Command Default

A local SCTP port is not defined.

Command Modes

SCTP protocol configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

The **local-port** command enters IPC transport-SCTP local configuration mode, which allows you to specify at least one local IP address (via the **local-ip** command) that is used to communicate with the redundant peer.

Examples

The following example shows how to enable Stateful Switchover (SSO):

```
!
redundancy inter-device
 scheme standby HA-in
!
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 10.0.0.1
   remote-port 5000
    remote-ip 10.0.0.2
```

Related Commands

Command	Description
local-ip	Defines at least one local IP address that is used to communicate with the local peer.
remote-port	Defines the remote SCTP that is used to communicate with the redundant peer.

logging (cfg-dns-view)

To enable logging of a system message logging (syslog) message each time the Domain Name System (DNS) view is used, use the **logging** command in DNS view configuration mode. To disable logging of a syslog message each time the DNS view is used, use the **no** form of this command.

logging
no logging

Syntax Description

This command has no arguments or keywords.

Command Default

No syslog message is logged when the DNS view is used.

Command Modes

DNS view configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command enables the logging of syslog messages for the DNS view.

To display the logging setting for a DNS view, use the **show ip dns view** command.

Examples

The following example shows how to enable logging of a syslog message each time the DNS view named user3 that is associated with the VRF vpn32 is used:

```
Router(config)# ip dns view vrf vpn32 user3

Router(cfg-dns-view)# logging
```

Related Commands

Command	Description
ip dns view	Enters DNS view configuration mode for the specified DNS view so that the logging setting, forwarding parameters, and resolving parameters can be configured for the view.
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

logging (DNS)

To enable logging of a system message logging (syslog) message each time the Domain Name System (DNS) view is used, use the **logging** command in DNS view configuration mode. To disable logging of a syslog message each time the DNS view is used, use the **no** form of this command.

logging
no logging

Syntax Description

This command has no arguments or keywords.

Command Default

No syslog message is logged when the DNS view is used.

Command Modes

DNS view configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command enables the logging of syslog messages for the DNS view.

To display the logging setting for a DNS view, use the **show ip dns view** command.

Examples

The following example shows how to enable logging of a syslog message each time the DNS view named user3 that is associated with the VRF vpn32 is used:

```
Router(config)# ip dns view vrf vpn32 user3

Router(cfg-dns-view)# logging
```

Related Commands

Command	Description
ip dns view	Enters DNS view configuration mode for the specified DNS view so that the logging setting, forwarding parameters, and resolving parameters can be configured for the view.
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

logging server-arp

To enable the sending of Address Resolution Protocol (ARP) requests for syslog server address during system initialization bootup, use the **logging server-arp** command in global configuration mode. To disable the sending of ARP requests for syslog server addresses, use the **no** form of this command.

logging server-arp
no logging server-arp

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Global configuration.

Command History

Release	Modification
12.3	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(5)B	This command was integrated into Cisco IOS Release 12.3(5)B.

Usage Guidelines

The **logging server-arp** global configuration command allows the sending of ARP requests for syslog server addresses during system initialization bootup.

When this CLI command is configured and saved to the startup configuration file, the system will send an ARP request for remote syslog server address before sending out the first syslog message.

The command should only be used when the remote syslog server is in the same subnet as the system router sending the ARP request.

Note Use this command even if a static ARP has been configured with the remote syslog server address.

Examples

The following example shows how to enable an ARP request for syslog server addresses:

```
Router# configure terminal
Router(config)# logging server-arp
Router(config)# exit
```

The following example shows how to disable an ARP request for syslog server addresses:

```
Router# configure terminal
Router(config)# no
 logging server-arp
Router(config)# exit
```

Related Commands

Command	Description
arp (global)	Adds a permanent entry in the Address Resolution Protocol (ARP) cache, use the **arp** command in global configuration mode.

mac packet-classify

To classify Layer 3 packets as Layer 2 packets, use the **mac packet-classify** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

mac packet-classify [**bpdu**]
no mac packet-classify [**bpdu**]

Syntax Description

bpdu	(Optional) Specifies Layer 2 policy enforcement for BPDU packets.

Command Default

Layer 3 packets are not classified as Layer 2 packets.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(50)SY	Added support for MAC ACLs on BPDU packets.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

You can configure these interface types for multilayer MAC access control list (ACL) quality of service (QoS) filtering:

- VLAN interfaces without Layer 3 addresses
- Physical LAN ports that are configured to support Ethernet over Multiprotocol Label Switching (EoMPLS)
- Logical LAN subinterfaces that are configured to support EoMPLS

The ingress traffic that is permitted or denied by a MAC ACL on an interface configured for multilayer MAC ACL QoS filtering is processed by egress interfaces as MAC-layer traffic. You cannot apply egress IP ACLs to traffic that was permitted or denied by a MAC ACL on an interface configured for multilayer MAC ACL QoS filtering.

Microflow policing does not work on interfaces that have the **mac packet-classify** command enabled.

The **mac packet-classify** command causes the Layer 3 packets to be classified as Layer 2 packets and disables IP classification.

Traffic is classified based on 802.1Q class of service (CoS), trunk VLAN, EtherType, and MAC addresses.

Examples

This example shows how to classify incoming and outgoing Layer 3 packets as Layer 2 packets:

```
Router(config-if)# mac packet-classify
Router(config-if)#
```

This example shows how to disable the classification of incoming and outgoing Layer 3 packets as Layer 2 packets:

```
Router(config-if)# no mac packet-classify
Router(config-if)#
```

This example shows how to enforce Layer 2 policies on BPDU packets:

```
Router(config-if)# mac packet-classify bpdu
Router(config-if)#
```

This example shows how to disable Layer 2 policies on BPDU packets:

```
Router(config-if)# no mac packet-classify bpdu
Router(config-if)#
```

Related Commands

Command	Description
mac packet-classify use vlan	Enables VLAN-based QoS filtering in the MAC ACLs.

mac packet-classify use vlan

To enable VLAN-based quality of service (QoS) filtering in the MAC access control lists (ACLs), use the **mac packet-classify use vlan** command in global configuration mode. To return to the default settings, use the **no** form of this command.

mac packet-classify use vlan
no mac packet-classify use vlan

Syntax Description

This command has no arguments or keywords.

Command Default

VLAN-based QoS filtering in the MAC ACLs is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720 and the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported in PFC3BXL or PFC3B mode only.

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

You must use the **no mac packet-classify use vlan** command to disable the VLAN field in the Layer 2 key if you want to apply QoS to the Layer 2 Service Advertising Protocol (SAP)-encoded packets (for example, Intermediate System-to-Intermediate System [IS-IS] and Internet Packet Exchange [IPX]).

QoS does not allow policing of non-Advanced Research Protocol Agency (ARPA) Layer 2 packets (for example, IS-IS and IPX) if the VLAN field is enabled.

Examples

This example shows how to enable Layer 2 classification of IP packets:

```
Router(config)# mac packet-classify use vlan
Router(config)
```

This example shows how to disable Layer 2 classification of IP packets:

```
Router(config)# no mac packet-classify use vlan
Router(config)
```

Related Commands

Command	Description
mac packet-classify	Classifies Layer 3 packets as Layer 2 packets.

match learnt-interface

To filter services that are available on an interface and associate the filtered data to a specific service-list, use the **match learnt-interface** command in multicast Domain Name System (mDNS) service discovery service-list mode. To disable the association between the filtered services on an interface with a specific service-list, use the **no** form of this command.

match learnt-interface *interface number*
no match learnt-interface

Syntax Description

interface number	Interface type and number. For more information on the type of available interfaces, use the question mark (?) online help function. **Note** The services on the interface will be filtered and associated with a service-list. These services can then be permitted or prohibited across subnets by applying the service-list on an interface.

Command Default

Services associated with an interface are not filtered and associated with a service-list.

Command Modes

mdns service discovery service-list (config-mdns-sd-sl)

Command History

Release	Modification
15.2(3)E	This command was introduced.
Cisco IOS XE 3.7E	This command was integrated into the Cisco IOS XE 3.7E release.
15.5(2)S	This command was integrated into Cisco IOS Release 15.5(2)S.
Cisco IOS XE Release 3.15S	This command was integrated into the Cisco IOS XE Release 3.15S

Usage Guidelines

The **match learnt-interface** command must be used after a service-list is created and the permit or deny option is exercised.

Examples

The following example shows how to filter services available on an interface and associate the filtered data with a specific service-list:

```
Device> enable
Device# configure terminal
Device(config)# service-list mdns-sd sl7 permit 30
Device(config-mdns-sd-sl)# match learnt-interface ethernet 0/1
Device(config-mdns-sd-sl)# exit
```

Related Commands

Command	Description
service-list mdns-sd	Creates a service-list and applies a filter on the service-list or associates a query for the service-list.
match message-type	Configures parameters for a service-list, for a message-type.
match service-type	Configures parameters for a service-list, for a specified service-type.
show mdns statistics	Displays mDNS statistics for the specified service-list.

match location

To configure parameters for a service-list based on a civic location, use the **match location** command in multicast Domain Name System (mDNS) service discovery service-list mode. To disable configuration of parameters for a service-list based on a civic location, use the **no** form of this command.

match location civic *civic-location-name*
no match location civic

Syntax Description

civic *civic-location-name*	Specifies the civic location name.

Command Default

A service-list is not filtered for a civic location name.

Command Modes

Multicast DNS service discovery service-list (config-mdns-sd-sl)

Command History

Release	Modification
15.2(2)E	This command was introduced.
Cisco IOS XE 3.6E	This command was integrated into the Cisco IOS XE 3.6E release.
15.2(1)SY	This command was integrated into Cisco IOS Release 15.2(1)SY.
15.5(2)S	This command was integrated into Cisco IOS Release 15.5(2)S.
Cisco IOS XE Release 3.15S	This command was integrated into the Cisco IOS XE Release 3.15S

Usage Guidelines

The **match location** command must be used after a service-list is created, and the permit or deny option is exercised.

If the civic location is available and the civic location criteria are set, then the match operation can be performed. If the civic location is not available, then the match operation cannot retrieve the location.

Examples

The following example shows how to filter a service-list by a civic location:

```
Device> enable
Device# configure terminal
Device(config)# service-list mdns-sd sl1 permit 3
Device(config-mdns-sd-sl)# match location civic location3
Device(config-mdns-sd-sl)# exit
```

Related Commands

Command	Description
match message-type	Configures parameters for a service-list, for a message-type.
match service-type	Configures parameters for a service-list, for a specified service-type.

Command	Description
service-list mdns-sd	Creates a service-list and applies a filter on the service-list or associates a query for the service-list.
show running-config mdns-sd service-list	Displays current running mDNS service-list configuration details.

match message-type

To configure parameters for a service-list based on a message type, use the **match message-type** command in multicast Domain Name System (mDNS) service discovery service-list mode. To disable configuration of parameters for a service-list based on a message type, use the **no** form of this command.

match message-type {**announcement** | **any** | **query**}
no match message-type

Syntax Description

announcement	Filters a service-list according to periodic mDNS announcements sent out by a device.
any	Filters a service-list for queries and announcements.
query	Filters a service-list according to associated queries.

Command Default

A service-list is not filtered for a query or announcement.

Command Modes

mdns service discovery service-list (config-mdns-sd-sl)

Command History

Release	Modification
15.2(1)E	This command was introduced.

Usage Guidelines

The **match message-type** command must be used after a service-list is created, and the permit or deny option is exercised.

Examples

The following example shows how to filter a service-list for the announcement message type.:

```
Device> enable
Device# configure terminal
Device(config)# service-list mdns-sd sl1 permit 3
Device(config-mdns-sd-sl)# match message-type announcement
Device(config-mdns-sd-sl)# exit
```

Related Commands

Command	Description
service-list mdns-sd	Creates a service-list and applies a filter on the service-list or associates a query for the service-list.
match service-instance	Configures parameters for a service-list, for a specified service-instance.
match service-type	Configures parameters for a service-list, for a specified service-type.
show mdns statistics	Displays mDNS statistics for the specified service-list.

match reply prefix-list

To enable verification of the advertised prefixes in the Dynamic Host Configuration Protocol (DHCP) reply messages from the configured authorized prefix list, use the **match reply prefix-list** command in DHCPv6 guard configuration mode. To disable verification of the advertised prefixes in the DHCP reply messages from the configured authorized prefix list, use the **no** form of this command.

match reply prefix-list *ipv6 prefix-list name*
no match reply prefix-list *ipv6 prefix-list name*

Syntax Description

ipv6 prefix-list name	The name of the prefix list.

Command Default

The advertised prefixes in DHCP reply messages from the configured authorized prefix list are not verified.

Command Modes

DHCPv6 guard configuration (config-dhcp-guard)

Command History

Release	Modification
15.2(4)S	This command was introduced.

Usage Guidelines

This command enables verification of the advertised prefixes in DHCP reply messages from the configured authorized prefix list. If not configured, this check will be bypassed. A prefix list is configured using the **ipv6 prefix-list** command. An empty prefix list is treated as a permit.

Examples

The following example defines a DHCPv6 guard policy name as policy1, places the router in DHCPv6 guard configuration mode, and enables verification of the advertised prefixes in DHCP reply messages from the configured authorized prefix list:

```
Router(config)# ipv6 dhcp guard policy policy1
Router(config-dhcp-guard)# match reply prefix-list ipv6pre1
```

Related Commands

Command	Description
ipv6 dhcp guard policy	Defines the DHCPv6 guard policy name.
ipv6 prefix-list	Creates an entry in an IPv6 prefix list.

match server access-list

To enable verification of the advertised Dynamic Host Configuration Protocol (DHCP) server or relay address in inspected messages from the configured authorized server access list, use the **match server access-list** command in DHCPv6 guard configuration mode. To disable verification of the advertised DHCP server or relay address in inspected messages from the configured authorized server access list, use the **no** form of this command.

match server access-list *ipv6 access-list-name*
no match server access-list *ipv6 access-list-name*

Syntax Description

ipv6 access-list-name	The name of the access list.

Command Default

The advertised DHCP server or relay address in inspected messages from the configured authorized server access list are not verified.

Command Modes

DHCPv6 guard configuration (config-dhcp-guard)

Command History

Release	Modification
15.2(4)S	This command was introduced.

Usage Guidelines

Enables verification of the advertised DHCP server or relay address in inspected messages from the configured authorized server access list. If not configured, this check will be bypassed. An access list is configured using the **ipv6 access-list** command. An empty access list is treated as a permit. The access list is configured using the **ipv6 access-list** command.

Examples

The following example defines a DHCPv6 guard policy name as policy1, places the router in DHCPv6 guard configuration mode, and enables verification of the advertised DHCP server or relay address in inspected messages from the configured authorized server access list:

```
Router(config)# ipv6 dhcp guard policy policy1
Router(config-dhcp-guard)# match server access-list ipv6acl1
```

Related Commands

Command	Description
ipv6 dhcp guard policy	Defines the DHCPv6 guard policy name.
ipv6 access-list	Defines an IPv6 access list.

match service-instance

To configure parameters for a service-list based on a service-instance, use the **match service-instance** command in multicast Domain Name System (mDNS) service discovery service-list mode. To disable configuration of parameters for a service-list based on a service-instance, use the **no** form of this command.

match service-instance *instance-name*
no match service-instance

Syntax Description

instance-name	Service instance name. The service-list is filtered according to the specified service-list.

Command Default

A service-list is not filtered for a service-instance name.

Command Modes

mdns service discovery service-list (config-mdns-sd-sl)

Command History

Release	Modification
15.2(1)E	This command was introduced.

Usage Guidelines

The **match service-instance** command must be used after a service-list is created, and the permit or deny option is exercised.

Examples

The following example shows how to filter a service-list by a service instance:

```
Device> enable
Device# configure terminal
Device(config)# service-list mdns-sd sl1 permit 3
Device(config-mdns-sd-sl)# match service-instance service1
Device(config-mdns-sd-sl)# exit
```

Related Commands

Command	Description
service-list mdns-sd	Creates a service-list and applies a filter on the service-list or associates a query for the service-list.
match message-type	Configures parameters for a service-list, for a message-type.
match service-type	Configures parameters for a service-list, for a specified service-type.
show mdns statistics	Displays mDNS statistics for the specified service-list.

match service-type

To configure parameters for a service-list based on a service-type, use the **match service-type** command in multicast Domain Name System (mDNS) service discovery service-list mode. To disable configuration of parameters for a service-list based on a service-type, use the **no** form of this command.

match service-type *mDNS-service-type-string*
no match service-type

Syntax Description

mDNS-service-type-string	Service type string. The service-list is filtered for the specified service-type.

Command Default

A service-list is not filtered for a service-type.

Command Modes

mdns service discovery service-list (config-mdns-sd-sl)

Command History

Release	Modification
15.2(1)E	This command was introduced.

Usage Guidelines

The **match service-type** command must be used after a service-list is created, and the permit or deny option is exercised.

Examples

The following example shows how to filter a service-list for a TXT service-type:

```
Device> enable
Device# configure terminal
Device(config)# service-list mdns-sd sl1 permit 3
Device(config-mdns-sd-sl)# match service-type TXT
Device(config-mdns-sd-sl)# exit
```

Related Commands

Command	Description
service-list mdns-sd	Creates a service-list and applies a filter on the service-list or associates a query for the service-list.
match service-instance	Configures parameters for a service-list, for a service-instance.
match message-type	Configures parameters for a service-list, for a message-type.
show mdns statistics	Displays mDNS statistics for the specified service-list.

mode (nat64)

To configure the Network Address Translation 64 (NAT64) mapping of addresses and ports (MAP-T) mode, use the **mode** command in NAT64 MAP-T configuration mode. To exit from the NAT64 MAP-T mode, use the **no** form of this command.

mode {**divi** | **map-t**}
no mode

Syntax Description

divi	Configures the stateless dual translation mode.
map-t	Configures the MAP-T mode. This mode is the default.

Command Default

MAP-T is the default mode.

Command Modes

NAT64 MAP-T configuration (config-nat64-mapt)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.
Cisco IOS Release 15.5(2)T	This command was integrated into Cisco IOS Release 15.5(2)T.

Usage Guidelines

MAP-T or Mapping of address and port (MAP) double stateless translation-based solution (MAP-T) provides IPv4 hosts connectivity to and across an IPv6 domain. MAP-T builds on existing stateless IPv4/IPv6 address translation techniques that are specified in RFC 6052, RFC 6144, and RFC 6145.

In dual translation mode, IPv4 is translated into IPv6 and vice versa.

Examples

The following example shows how to configure the dual translation mode for stateless NAT64:

```
Device(config)# nat64 map-t domain 89
Device(config-nat64-mapt)# mode divi
```

Related Commands

Command	Description
nat64 map-t	Configures NAT64 MAP-T settings.

name

To configure the redundancy group with a name, use the **name**command in redundancy application group configuration mode. To remove the name of a redundancy group, use the **no** form of this command.

name *group-name*
no name *group-name*

Syntax Description

group-name	Name of the redundancy group.

Command Default

The redundancy group is not configured with a name.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Examples

The following example shows how to configure the redundancy group name as group1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# name group1
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
group(firewall)	Enters redundancy application group configuration mode.
shutdown	Shuts down a group manually.

nat64 enable

To enable Network Address Translation 64 (NAT64) on an interface, use the **nat64 enable** command in interface configuration mode. To disable the NAT64 configuration on an interface, use the **no** form of this command.

nat64 enable
no nat64 enable

Syntax Description

This command has no arguments or keywords.

Command Default

NAT64 is not enabled on an interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.
15.4(1)T	This command was integrated into Cisco IOS Release 15.4(1)T.

Examples

The following example shows how to enable NAT64 on a Gigabit Ethernet interface:

```
Device# configure terminal
Device(config)# interface gigabitethernet0/0/0
Device(config-if)# nat64 enable
Device(config-if)# end
```

Related Commands

Command	Description
show nat64 adjacency	Displays information about the NAT64-managed adjacencies.
show nat64 ha status	Displays information about the NAT64 HA status.
show nat64 statistics	Displays statistics about a NAT64 interface and the transmitted and dropped packet count.

nat64 logging

To enable Network Address Translation 64 (NAT64) high-speed logging (HSL), use the **nat64 logging** command in global configuration mode. To disable NAT64 logging, use the **no** form of this command.

nat64 logging translations flow-export v9 udp destination *hostname port*
no nat64 logging translations

Syntax Description

translations	Enables NAT64 translation logging.
flow-export	Enables NAT64 logging through flow export.
v9	Enables Version 9 NetFlow export format logging.
udp	Enables logging of UDP packets.
destination	Specifies the NAT64 external logging destination.
hostname	Hostname or the IPv4 address of the external collector for logging records.
port	Port number of the IPv4 host of the external collector for logging records. Valid values are from 1 to 65535.

Command Default

NAT64 logging is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.4(2)T	This command was integrated into Cisco IOS Release 15.4(2)T.

Usage Guidelines

The **nat64 logging** command allows you to specify remote logging for NAT64 objects.

The **nat64 logging** command is based on the NetFlow Version 9 export format.

In Cisco IOS XE Release 3.4S and later releases, NAT supports HSL. When HSL is configured, NAT provides a log of the packets that are flowing through the routing devices (similar to the Version 9 NetFlow-like records) to an external collector.

Examples

The following example shows how to enable NAT64 HSL logging:

```
Device(config)# nat64 logging translations flow-export v9 udp destination 10.1.1.1 2000
```

Related Commands

Command	Description
nat64 enable	Enables NAT64 on an interface.

nat64 logging translations flow-export

To enable the high-speed logging of NAT64 translations by using a flow exporter, use the **nat64 logging translations flow-export** command in global configuration mode. To disable the logging of NAT64 translations by using a flow exporter, use the **no** form of this command.

nat64 logging translations flow-exportv9 udp {**destination** *IPv4address-port* | **ipv6-destination** *ipv6address-port*}[**vrf** *vrf-name* | **source** *interface-name interface-number*]
no nat64 logging translations flow-export

Syntax Description

v9	Specifies the flow exporter Version 9 format.
udp	Specifies the UDP protocol.
destination	Specifies the destination IPv4 address for which translations will be logged.
ipv6-destination	Specifies the destination address for which translations will be logged.
hostname	Name or IPv4 address of the destination.
local-udp-port	Local UDP port number. Valid values are from 1 to 65335.
source *interface-type interface-number*	(Optional) Specifies the source interface for which translations will be logged.
vrf *vrf-name*	(Optional) Specifies the destination VRF for which translations will be logged.

Command Default

Logging is disabled for all NAT64 translations.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was modified. The **bind-only** keyword was added.
Cisco IOS XE Fuji Release 16.7.1	This command was modified. The following keywords were added: • **ipv6-destination** • **vrf**

Examples

The following example shows how to enable translation logging for a specific destination and source interface:

```
Device(config)# nat64 logging translations flow-export v9 udp destination 10.10.0.1 1020
source gigabithethernet 0/0/1
```

This example shows how to enable high-speed logging using an IPv6 address

```
Device(config)# nat64 logging translations flow-export v9 udp ipv6-destination 2001::06
5050 source GigabitEthernet 0/0/0
```

This example shows how to enable high-speed logging using an IPv6 address for a VRF

```
Device(config)# nat64 logging translations flow-export v9 udp ipv6-destination 2001::06
5050 vrf hslvrf source GigabitEthernet 0/0/0
```

nat64 map-t

To configure the Network Address Translation 64 (NAT64) mapping of addresses and ports translation (MAP-T) settings, use the **nat64 map-t** command in global configuration mode. To remove the NAT64 MAP-T settings, use the **no** form of this command.

nat64 map-t domain *number*
no nat64 map-t domain *number*

Syntax Description

domain *number*	Specifies the NAT64 MAP-T domain. Valid values for the *number* argument are from 1 to 128.

Command Default

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.
Cisco IOS Release 15.5(2)T	This command was integrated into Cisco IOS Release 15.5(2)T.

Usage Guidelines

MAP-T or Mapping of address and port (MAP) double stateless translation-based solution (MAP-T) provides IPv4 hosts connectivity to and across an IPv6 domain. MAP-T builds on existing stateless IPv4/IPv6 address translation techniques that are specified in RFC 6052, RFC 6144, and RFC 6145.

After you configure the **nat64 map-t** command, the command mode changes to NAT64 MAP-T configuration mode.

Examples

The following example shows how to configure NAT64 MAP-T settings:

```
Device(config)# nat64 map-t domain 89
Device(config-nat64-map-t)#
```

Related Commands

Command	Description
basic-mapping-rule	Configures a basic mapping rule for NAT64 MAP-T.
default-mapping-rule	Configures NAT64 MAP-T domain default mapping rule.

nat64 prefix stateful

To configure a prefix and a prefix length for stateful Network Address Translation 64 (NAT64), use the **nat64 prefix stateful** command in global configuration or interface configuration mode. To disable the configuration, use the **no** form of this command.

nat64 prefix stateful *ipv6-prefix/prefix-length*
no nat64 prefix stateful *ipv6-prefix / prefix-length*

Syntax Description

ipv6-prefix	IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/prefix-length	Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

NAT64 stateful prefixes are not configured.

Command Modes

Global configuration (config)

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release3.4 S	This command was introduced.
15.4(2)T	This command was integrated into Cisco IOS Release 15.4(2)T.

Usage Guidelines

Use the **nat64 prefix stateful** command in global configuration mode to assign a global NAT64 stateful prefix, or use it in interface configuration mode to assign a unique NAT64 stateful prefix for an interface. A maximum of one global stateful prefix and one stateful prefix per interface is supported. If a global stateful prefix or an interface stateful prefix is not configured, the Well Known Prefix (WKP) of 64:ff9b::/96 is used to translate the IPv4 address of the IPv4 host.

Examples

The following example shows how to configure a global NAT64 stateful prefix:

```
Device(config)# nat64 prefix stateful 2001:DB8:0:1::/96
```

The following example shows how to configure a NAT64 stateful prefix for a Gigabit Ethernet interface:

```
Device(config)# interface gigabitethernet0/0/0
Device(config-if)# nat64 prefix stateful 2001:DB8:0:1::/96
```

Related Commands

Command	Description
nat64 prefix stateless	Assigns a global or interface-specific NAT64 stateless prefix.
show nat64 prefix stateful	Displays information about NAT64 stateful prefixes.

nat64 prefix stateless

To assign a global or interface-specific Network Address Translation 64 (NAT64) stateless prefix, use the **nat64 prefix stateless** command in global configuration or interface configuration mode. To disable the configuration, use the **no** form of this command.

nat64 prefix stateless *ipv6-prefix*/*prefix-length*
no nat64 prefix stateless

Syntax Description

ipv6-prefix	IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/ *prefix-length*	Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

No NAT64 translation is performed.

Command Modes

Global configuration (config)

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.
15.4(1)T	This command was integrated into Cisco IOS Release 15.4(1)T.

Usage Guidelines

The **nat64 prefix stateless** command uses a prefix and prefix length for IPv4-translatable IPv6 addresses. Use the **nat64 prefix stateless** command in global configuration mode to assign a global NAT64 stateless prefix or in interface configuration mode to assign an unique NAT64 stateless prefix for each interface. In interface configuration mode, a stateless prefix should be configured on an IPv6-facing interface.

All packets coming to an IPv6 interface are matched against the configured prefix, and the matched packets are translated to IPv4. Similarly, the packets that the IPv6 interface sends use the stateless prefix to construct the source and destination IPv6 address.

Note A maximum of one global stateless prefix and one stateless prefix per interface is supported.

If NAT64 is enabled on an interface that does not have a stateless prefix configured, then the global stateless prefix is used. However, if a global prefix and an interface prefix are configured, then the interface prefix is used for stateless NAT64 translation. The use of a stateless prefix on an interface has priority over the configured global stateless prefix.

Examples

The following example shows how to configure a global NAT64 stateless prefix:

```
Device# configure terminal
Device(config)# nat64 prefix stateless 2001::DB8::1/96
Device(config)# end
```

The following example shows how to assign a NAT64 stateless prefix for a Gigabit Ethernet interface:

```
Device# configure terminal
Device(config)# interface gigabitethernet0/0/0
Device(config-if)# nat64 prefix stateless 2001:0DB8:0:1::/96
Device(config-if# end
```

Related Commands

Command	Description
nat64 route	Specifies the NAT64 stateless prefix to which an IPv4 prefix should be translated.
show nat64 prefix stateless	Displays information about the configured NAT64 stateless prefixes.

nat64 route

To specify the Network Address Translation 64 (NAT64) prefix to which an IPv4 prefix should be translated, use the **nat64 route** command in global configuration mode. To disable the configuration, use the **no** form of this command.

nat64 route *ipv4-prefix/mask interface-type interface-number*
no nat64 route *ipv4-prefix/mask*

Syntax Description

ipv4-prefix / mask	Length of the IPv4 prefix and the mask.
interface-type	Interface type. For more information, use the question mark (?) online help function.
interface-number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Default

No NAT64 routing is performed.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.
15.4(1)T	This command was integrated into Cisco IOS Release 15.4(1)T.

Usage Guidelines

A prefix that is configured on an interface is used as the stateless prefix on that interface. If no interface-specific prefix is configured, the configured global prefix is used for NAT64 translation.

Examples

The following example shows how to assign an IPv4 prefix and mask to an interface:

```
Device# configure terminal
Device(config)# nat64 route 192.168.0.0/24 gigabitethernet0/0/1
Device(config)# exit
```

Related Commands

Command	Description
nat64 prefix stateless	Assigns a global or interface-specific NAT64 stateless prefix.
show nat64 routes	Displays information about the configured NAT64 routes.

nat64 service ftp

To enable the Network Address Translation 64 (NAT64) FTP service, use the **nat64 service ftp** command in global configuration mode. To disable the NAT64 FTP service, use the **no** form of this command.

nat64 service ftp
no nat64 service ftp

Syntax Description

This command has no arguments or keywords.

Command Default

The NAT64 FTP service is enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

Service FTP is an application-level gateway (ALG) that helps NAT64 operate on Layer 7 data.

Examples

The following example shows how to disable the NAT64 FTP service:

```
Router(config)# no nat64 service ftp
```

Related Commands

Command	Description
nat64 enable	Enables NAT64 on an interface.

nat64 settings

To configure Network Address Translation 64 (NAT64) settings, use the **nat64 settings** command in global configuration mode. To disable NAT64 settings, use the **no** form of this command.

nat64 settings {**fragmentation header disable** | **v4 tos ignore**}
no nat64 settings {**fragmentation header disable** | **v4 tos ignore**}

Syntax Description

fragmentation header disable	Disables the NAT64 fragmentation header.
v4 tos ignore	Specifies not to copy the IPv4 type-of-service (ToS) header.

Command Default

NAT64 settings are disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

Usage Guidelines

By default, NAT64 adds a fragmentation header for all IPv4-to-IPv6 packets that do not have the Do Not Fragment (DF) bits set. Configure the **nat64 settings fragmentation header disable** command to disable the adding of a fragmentation header for packets that are not fragmented.

By default, NAT64 copies ToS bits from an IPv4 header to an IPv6 header. Configure the **nat64 settings v4 tos ignore** command to disable the copying of ToS bits from an IPv4 header to IPv6 header.

Examples

The following example shows how to disable the NAT64 fragmentation header:

```
Router(config)# nat64 settings fragmentation header disable
```

Related Commands

Command	Description
nat64 enable	Enables NAT64 on an interface.

nat64 settings eif

To enable the Network Address Translation 64 (NAT64) end-point independent filtering (EIF), use the **nat64 settings eif** command in global configuration mode. To disable the EIF settings, use the **no** form of this command.

nat64 settings eif enable

no nat64 settings eif enable

Syntax Description

enable	Enables EIF settings.

Command Default

NAT64 EIF settings are disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced.

Examples

The following example shows how to enable the NAT64 EIF:

```
Device(config)# nat64 settings eif enable
```

Related Commands

Command	Description
nat64 settings	Configures NAT64 settings

nat64 settings flow-entries disable

To disable flow cache entries in Network Address Translation 64 (NAT64) configurations, use the **nat64 settings flow-entries disable** command in global configuration mode. To enable flow cache entries in NAT64 configurations, use the **no** form of this command.

nat64 settings flow-entries disable
no nat64 settings flow-entries disable

Syntax Description

This command has no arguments or keywords.

Command Default

Flow cache entries are enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.10S	This command was introduced.

Usage Guidelines

Note Disabling flow cache entries will result in lesser performance as this functionality performs multiple database searches to find the most specific translation to use.

By default, Network Address Translation (NAT) creates a session (which is a 5-tuple entry) for every translation. A session is also called a flow cache entry.

NAT64 (stateful and stateless) translations support the disabling of flow cache entries. You can disable flow cache entries in dynamic and static NAT64 configurations. Instead of creating sessions, dynamic and static NAT64 translations can translate a packet off the binding (or bindings if both inside and outside bindings are available). A binding or a half entry is an association between a local IP address and a global IP address.

Disabling flow cache entries for dynamic and static translations saves memory usage and provides more scalability for your NAT64 translations.

Note Port Address Translation (PAT) or interface overload does not support disabling of flow cache entries.

Examples

The following example shows how to enable flow cache entries in a static NAT64 configuration:

```
Device# configure terminal
Device(config)# ipv6 unicast-routing
Device(config)# nat64 prefix stateful 2001:DB8:1::1/96
Device(config)# nat64 v6v4 static 2001:DB8:1::FFFE 209.165.201.1
Device(config)# no nat64 settings flow-entries disable
```

Related Commands

Command	Description
ipv6 unicast-routing	Enables the forwarding of IPv6 unicast datagrams.
nat64 prefix stateful	Configures a prefix and a prefix length for stateful NAT64.
nat64 prefix stateless	Assigns a global or interface-specific NAT64 stateless prefix.
nat64 v6v4	Translates an IPv6 source address to an IPv4 source address and an IPv4 destination address to an IPv6 destination address for NAT64.

nat64 settings mtu minimum

To set the minimum size for the Network Address Translation 64 (NAT64) maximum transmission units (MTU), use the **nat64 settings mtu minimum** command in interface configuration mode. To return to the default MTU size of 1280 bytes, use the **no** form of this command.

nat64 settings mtu minimum *size*
no nat64 settings mtu minimum

Syntax Description

size	Minimum MTU in bytes. The range is from 1281 to the MTU of the interface.

Command Default

The default value is 1280 bytes, which is the minimum MTU on an IPv6 link.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

Usage Guidelines

Each interface has a default maximum packet size or MTU size. The MTU size of an interface defaults to the largest size possible for that interface type. To adjust the MTU size of an interface, configure the **mtu** command. Packets are fragmented based on the configured MTU size.

If the Do Not Fragment (DF) bits are not set, during the NAT64 translation and fragmentation of IPv4 packets to IPv6, NAT64 assumes that the IPv6 link minimum MTU size is 1280 bytes. However, the link MTU size could be greater than the minimum IPv6 link MTU size. To better utilize the network, network administrators can use the **nat64 settings mtu minimum** command to set a higher minimum MTU size. For example, if interfaces in a network are all Ethernet interfaces and the MTU size is 1500 bytes, fragmenting packets at 1280 bytes is not an effective utilization of the bandwidth. In this case, the network administrator can change the MTU size to 1500 bytes. When the **nat64 settings mtu minimum** command is configured, NAT64 ignores the implicit minimum MTU of 1280 bytes and fragments IPv6 packets based on the configured MTU size.



Note The **nat64 settings mtu minimum** command works only on IPv6-facing interfaces.

Examples

The following example shows how to configure a minimum MTU size of 1450 bytes for Gigabit Ethernet interface 0/0/1:

```
Router(config)# interface gigabitethernet 0/0/1
Router(config-if)# nat64 settings mtu minimum 1450
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
mtu	Adjusts the maximum packet size or MTU size.

nat64 switchover replicate http

To replicate the Network Address Translation 64 (NAT64) HTTP switchover settings, use the **nat64 switchover replicate http** command in global configuration mode. To disable the HTTP switchover replication settings, use the **no** form of this command.

nat64 switchover replicate http {**enable** | **disable**} **port** *port-number*
no nat64 switchover replicate http

Syntax Description

disable	Disables HTTP session replication.
enable	Enables HTTP session replication.
port	Specifies the HTTP port.
port-number	Port number. Valid values are from 1 to 65535.

Command Default

NAT64 HTTP sessions are not replicated.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

Usage Guidelines

In stateful NAT64 intra-chassis redundancy, HTTP sessions are not backed up on the standby Forward Processor (FP). A typical HTTP application has short-lived, transient flows. Because of the transient nature of the HTTP flows, these flows are not replicated. With stateful NAT64 intra-chassis redundancy you have the ability to replicate HTTP sessions so that HTTP flows can be made to live longer. To replicate HTTP sessions on the standby FP during a switchover, you must configure the **nat64 switchover replicate http enable** command.

You can enable and disable the replication of HTTP sessions on ports. For example, you can configure the **nat64 switchover replicate http port 80** command and replicate the switchover of HTTP sessions on port 80. Configure the **nat64 switchover replicate http disable port 8080** command to disable the replication of HTTP sessions on port 8080. You can disable the replication of sessions on only one port at any given time; however, you can enable the replication of sessions on all ports.

Examples

The following example shows how to replicate switchover of NAT64 HTTP sessions:

```
Router(config)# nat64 switchover replicate http enable port 80
```

Related Commands

Command	Description
ip nat switchover replication http	Replicates HTTP sessions during a switchover.

nat64 translation

To enable Network Address Translation 64 (NAT64) translation, use the **nat64 translation** command in global configuration mode. To disable NAT64 translation, use the **no** form of this command.

nat64 translation {**max-entries** *limit* | **timeout** {**icmp** | **tcp** | **tcp-transient** | **udp**} *seconds*}
nat64 translation {**max-entries** | **timeout** {**icmp** | **tcp** | **tcp-transient** | **udp**}}

Syntax Description

max-entries	Configures the maximum number of stateful NAT64 translations allowed on a router.
limit	NAT64 translation entry limit. Valid values are from 1 to 2147483647.
timeout	Specifies the NAT64 translation entry timeout.
icmp	Specifies the timeout for NAT64 Internet Control Message Protocol (ICMP) traffic flow.
tcp	Specifies the timeout for NAT64 established TCP traffic flow.
tcp-transient	Specifies the timeout for NAT64 transient TCP traffic flow.
udp	Specifies the timeout for NAT64 UDP traffic flow.
seconds	Traffic timeout, in seconds. Valid values are from 1 to 536870.

Command Default

NAT64 translation is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.4(2)T	This command was integrated into Cisco IOS Release 15.4(2)T.

Usage Guidelines

The **nat64 translation timeout** command overrides the default aging timeout for NAT64 translations.

A transient TCP session has three possible conditions: a synchronize (SYN) handshake is started, but it is not complete; a reset (RST) packet is received; or a finished (FIN) packet is received in both directions.

Examples

The following example shows how to set the NAT64 translation maximum entry limit to 500:

```
Device(config)# nat64 translation max-entries 500
```

The following example shows how to set the NAT64 translation timeout for TCP to 20,000 seconds:

```
Device(config)# nat64 translation timeout tcp 20000
```

Related Commands

Command	Description
nat64 enable	Enables NAT64 on an interface.

nat64 v4

To enable Network Address Translation 64 (NAT64) IPv4 configuration, use the **nat64 v4** command in global configuration mode. To disable the NAT64 IPv4 configuration, use the **no** form of this command.

nat64 v4 pool *pool-name start-address-range end-address-range*
no nat64 v4 pool *pool-name* [**forced** | *start-address-range end-address-range* [**forced**]]

Syntax Description

pool	Configures an IPv4 address pool.
pool-name	Name of the IPv4 address pool.
start-address-range	Starting address of the address pool range.
end-address-range	Ending address of the address pool range.
forced	(Optional) Removes the configuration even when the NAT64 translation exists for the configuration.

Command Default

The NAT64 IPv4 configuration is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.4(2)T	This command was integrated into Cisco IOS Release 15.4(2)T.

Usage Guidelines

In Cisco IOS XE Release 3.4S, the Stateful NAT64 feature supports only single range pools.

Examples

The following example shows how to enable the NAT64 IPv4 pool configuration:

```
Device(config)# nat64 v4 pool pool1 192.168.0.2 192.168.0.254
```

Related Commands

Command	Description
nat64 enable	Enables NAT64 on an interface.

nat64 v4v6

To translate an IPv4 source address to an IPv6 source address and an IPv6 destination address to an IPv4 destination address for Network Address Translation 64 (NAT64), use the **nat64 v4v6** command in global configuration mode. To disable the translation, use the **no** form of this command.

nat64 v4v6 static {*ipv4-address ipv6-address* | **tcp** *ipv4-address port ipv6-address port* | **udp** *ipv4-address port ipv6-address port*}[**redundancy** *group-id* **mapping-id** *id*]
no nat64 v4v6 static {*ipv4-address ipv6-address* | [**forced**] | **tcp** *ipv4-address port ipv6-address port* | **udp** *ipv4-address port ipv6-address port*} [**forced**] [**redundancy** *group-id* **mapping-id** *id*]

Syntax Description

static	Associates an IPv6 address to an IPv4 host statically.
ipv4-address	Address of the IPv4 host.
ipv6-address	IPv6 address to which the IPv4 host is mapped to in the IPv6 network.
tcp	Applies static mapping to TCP protocol packets.
port	Port number of the IPv6 or IPv4 address. Valid values are from 1 to 65535.
udp	Applies static mapping to UDP protocol packets.
redundancy *group-id*	(Optional) Configures a redundancy group (RG) with the specified ID. Valid values are 1 and 2.
mapping-id *id*	(Optional) Configures a unique ID for mapping devices. The same ID should be configured on both active and standby devices. Valid values are from 1 to 20480.
forced	(Optional) Removes the configuration even when the NAT64 translation exists for the configuration.

Command Default

NAT64 IPv4-to-IPv6 translation is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was modified. The **redundancy** *group-id* and **mapping-id** *id* keyword-argument pairs were added.
15.4(2)T	This command was integrated into Cisco IOS Release 15.4(2)T.

Examples

The following example shows how to enable static mapping of an IPv4 address to an IPv6 address:

```
Device(config)# nat64 v4v6 static 192.168.0.1 2001:DB8:0::1
```

The following example shows how to configure a redundancy group to a static IPv4-to-IPv6 address configuration:

```
Device(config)# nat64 v4v6 static 192.168.0.1 2001:DB8:0::1 redundancy 1 mapping-id 101
```

Related Commands

Command	Description
nat64 v6v4	Translates an IPv6 source address to an IPv4 source address and an IPv4 destination address to an IPv6 destination address for NAT64.

nat64 v6v4

To translate an IPv6 source address to an IPv4 source address and an IPv4 destination address to an IPv6 destination address for Network Address Translation 64 (NAT64), use the **nat64 v6v4** command in global configuration mode. To disable the translation, use the **no** form of this command.

nat64 v6v4 {**list** *access-list-name* **pool** *pool-name* [**overload**] | **static** {*ipv6-address ipv4-address* | **tcp** *ipv6-address port ipv4-address port* | **udp** *ipv6-address port ipv4-address port*}}[**redundancy** *group-id* **mapping-id** *id*]
no nat64 v6v4 {**list** *access-list-name* **pool** *pool-name* [**overload**] | **static** {*ipv6-address ipv4-address* | **tcp** *ipv6-address port ipv4-address port* | **udp** *ipv6-address port ipv4-address port*}} [**forced**][**redundancy** *group-id* **mapping-id** *id*]

Syntax Description

list	Associates an IPv4 pool with the filtering mechanism that decides when to apply an IPv6 address mapping.
access-list-name	Name of the IPv6 access list.
pool	Specifies the NAT64 pool for dynamic mapping of addresses.
pool-name	Name of the NAT64 pool.
overload	(Optional) Enables NAT64 overload address translation.
static	Enables NAT64 static mapping of addresses.
ipv6-address	IPv6 address of the IPv6 host to which static mapping is applied.
ipv4-address	IPv4 address that represents the IPv6 host for static mapping in the IPv4 network.
tcp	Applies static mapping to TCP protocol packets.
port	Port number of the IPv6 or IPv4 address. Valid values are from 1 to 65535.
udp	Applies static mapping to UDP protocol packets.
redundancy *group-id*	(Optional) Configures a redundancy group (RG). Valid values are 1 and 2.
mapping-id *id*	(Optional) Configures a unique ID for mapping devices. The same ID should be configured on both active and standby devices. Valid values are from 1 to 20480.
forced	(Optional) Removes the configuration even when the NAT64 translation exists for the configuration.

Command Default

NAT64 IPv6-to-IPv4 translation is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was modified. The **redundancy** *group-id* and **mapping-id** *id* keyword-argument pairs were added.
15.4(2)T	This command was integrated into Cisco IOS Release 15.4(2)T.

Examples

The following example shows how to enable dynamic mapping of an IPv6 address to an IPv4 address pool:

```
Device(config)# nat64 v6v4 list list1 pool pool1
```

The following example shows how to configure an RG for a dynamic IPv6-to-IPv4 address pool:

```
Device(config)# nat64 v6v4 list list1 pool pool1 redundancy 1 mapping-id 203
```

Related Commands

Command	Description
nat64 v4v6	Translates an IPv4 source address to an IPv6 source address and an IPv6 destination address to an IPv4 destination address for NAT64.

nat66 inside

To configure NPTv6 inside network interface, use the **nat66 inside** command in interface configuration mode. To remove the nat66 inside network address prefix, use the **no** form of this command.

nat66 inside
no nat66 inside

Syntax Description

This command has no arguments or keywords.

Command Default

The NPTv6 inside network address prefix is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Denali 16.2	This command was introduced.

Usage Guidelines

In Cisco IOS XE Denali 16.2 release, ASR1K NPTv6 feature does not support VRF and Multicast.

The following example shows how to configure NPTv6 inside network interface:

```
Device(config-if)# nat66 inside
```

Related Commands

Command	Description
nat66 outside	Specifies the IPv6 interface of the outside network for NAT66.

nat66 outside

To configure NPTv6 outside network interface, use the **nat66 outside** command in interface configuration mode. To remove the nat66 outside network address prefix, use the **no** form of this command.

nat66 outside
no nat66 outside

Syntax Description

This command has no arguments or keywords.

Command Default

The NPTv6 outside network interface is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Denali 16.2	This command was introduced.

Usage Guidelines

In Cisco IOS XE Denali 16.2 release, ASR1K NPTv6 feature does not support VRF and Multicast.

The following example shows how to configure NPTv6 outside network interface:

```
Device(config-if)# nat66 outside
```

Related Commands

Command	Description
nat66 inside	Specifies the IPv6 interface of the inside network for NAT66.

nat66 prefix

To configure NPTv6 inside network address prefix and outside network address prefix for NPTv6 translation, use the **nat66 prefix** command in global configuration mode. To remove the IPv6 prefix to IPv6 prefix translation, use the **no** form of this command.

nat66 prefix *inside prefix/prefix-length outside prefix/prefix-length*
no nat66 prefix *inside prefix/prefix-length outside prefix/prefix-length*

Syntax Description

inside	Specifies the IPv6 inside network.
outside	Specifies the IPv6 outside network.
prefix	Specifies the IPv6 network prefix.
prefix-length	Specifies the length of the IPv6 address prefix.

Command Default

The IPv6 address prefixes for NPTv6 translation is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Denali 16.2	This command was introduced.

Usage Guidelines

Configure IPv6 inside and outside network in interface configuration mode before configuring NPTv6 translation.

The following example shows how to configure IPv6 to IPv6 network address prefix translation:

```
Device(config)# nat66 prefix inside 2002:AB01::/64 outside 2002:AB02::/64
```

Related Commands

Command	Description
nat66 inside	Specifies the IPv6 interface of the inside network for NAT66.
nat66 outside	Specifies the IPv6 interface of the outside network for NAT66.

netbios-name-server

To configure NetBIOS Windows Internet Naming Service (WINS) name servers that are available to Microsoft Dynamic Host Configuration Protocol (DHCP) clients, use the **netbios-name-server** command in DHCP pool configuration. To remove the NetBIOS name server list, use the no form of this command.

netbios-name-server *address* [*address2 ... address8*]
no netbios-name-server

Syntax Description

address	Specifies the IP address of the NetBIOS WINS name server. One IP address is required, although you can specify up to eight addresses in one command line.
address2 ...address8	(Optional) Specifies up to eight addresses in the command line.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

One IP address is required, although you can specify up to eight addresses in one command line. Servers are listed in order of preference (address1 is the most preferred server, address2 is the next most preferred server, and so on).

Examples

The following example specifies the IP address of a NetBIOS name server available to the client:

```
netbios-name-server 10.12.1.90
```

Related Commands

Command	Description
dns-server	Specifies the DNS IP servers available to a DHCP client.
domain-name (DHCP)	Specifies the domain name for a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP Server and enters DHCP pool configuration mode.
netbios-node-type	Configures the NetBIOS node type for Microsoft DHCP clients.

netbios-node-type

To configure the NetBIOS node type for Microsoft Dynamic Host Configuration Protocol (DHCP) clients, use the **netbios-node-type** command in DHCP pool configuration mode. To remove the NetBIOS node type, use the no form of this command.

netbios-node-type *type*
no netbios-node-type

Syntax Description

type	Specifies the NetBIOS node type. Valid types are: • **b-node** --Broadcast • **p-node** --Peer-to-peer • **m-node** --Mixed • **h-node** --Hybrid (recommended)

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The recommended type is h-node (hybrid).

Examples

The following example specifies the client's NetBIOS type as hybrid:

```
netbios node-type h-node
```

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP Server and enters DHCP pool configuration mode.
netbios name-server	Configures NetBIOS WINS name servers that are available to Microsoft DHCP clients.

network (DHCP)

To configure the network number and mask for a Dynamic Host Configuration Protocol (DHCP) address pool primary or secondary subnet on a Cisco IOS DHCP server, use the **network** command in DHCP pool configuration mode. To remove the subnet number and mask, use the **no** form of this command.

Syntax Description

network-number	The IP address of the primary DHCP address pool.
mask	(Optional) The bit combination that renders which portion of the address of the DHCP address pool refers to the network or subnet and which part refers to the host.
/ *prefix-length*	(Optional) The number of bits that comprise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).
secondary	(Optional) The network address specifies a secondary subnet in the DHCP address pool, and the router enters DHCP pool secondary subnet configuration mode. **Note** To configure a secondary subnet, you must also specify the *mask* argument or the p*refix-length* argument.

Command Default

This command is disabled by default.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was modified. The **secondary** keyword was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

This command is valid for DHCP subnetwork address pools only.

The DHCP server assumes that all host addresses are available. The system administrator can exclude subsets of the address space by using the **ip dhcp excluded-address** global configuration command. However, the **ip dhcp excluded-address** command cannot be used to exclude addresses from virtual routing and forwarding (VRF)-associated pools.

You cannot configure manual bindings within the same pool that is configured with the **network** command.

If a default router list is configured for the pool or subnet from which the address was allocated, the DHCP server selects an IP address from that default router list and provides it to the client. The DHCP client uses that router as the first hop for forwarding messages.

Removing a secondary subnet also removes the default router list for that subnet. Removing the primary subnet removes only the primary subnet definition but not the network-wide default router list.

To display the DHCP address pool information configured by the **network** command, use the **show ip dhcp pool** command.

Examples

The following example shows how to configure 172.16.0.0/12 as the subnetwork number and mask of the DHCP pool named pool1. The IP addresses in pool1 range from 172.16.0.0 to 172.31.255.255.

```
Router(config)#
ip dhcp pool pool1

Router(dhcp-config)#
network 172.16.0.0 255.240.0.0
```

The following example shows how to configure 192.0.2.0/24 as the subnetwork number and mask of the DHCP pool named pool2 and then add the DHCP pool secondary subnet specified by the subnet number and mask 192.0.4.0/30. The IP addresses in pool2 consist of two unconnected subnets: the addresses from 192.0.2.1 to 192.0.2.254 and the addresses from 192.0.4.1 to 192.0.4.2.

```
Router(config)#
ip dhcp pool pool2

Router(dhcp-config)#
network 192.0.2.0 255.255.255.0

Router(dhcp-config)#
network 192.0.4.0 255.255.255.252 secondary
```

Related Commands

Command	Description
default-router	Specifies the IP address of the default router for a DHCP client.
host	Specifies the IP address and network mask for a manual binding to a DHCP client.
ip dhcp excluded-address	Specifies IP addresses that a Cisco IOS DHCP server should not assign to DHCP clients.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.
override default-router	Configures a subnet-specific default router list for the DHCP pool secondary subnet.
show ip dhcp pool	Displays information about the DHCP address pools.

next-server

To configure the next server in the boot process of a Dynamic Host Configuration Protocol (DHCP) client, use the **next-server** command in DHCP pool configuration. To remove the boot server list, use the **no** form of this command.

next-server *address* [*address2* **...** *address8*]
no next-server *address*

Syntax Description

address	Specifies the IP address of the next server in the boot process, which is typically a Trivial File Transfer Protocol (TFTP) server. One IP address is required, but up to eight addresses can be specified in one command line.
address2 ...address8	(Optional) Specifies up to seven additional addresses in the command line.

Command Default

If the **next-server** command is not used to configure a boot server list, the DHCP Server uses inbound interface helper addresses as boot servers.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can specify up to eight servers in the list. Servers are listed in order of preference (address1 is the most preferred server, address2 is the next most preferred server, and so on).

Examples

The following example specifies 10.12.1.99 as the IP address of the next server in the boot process:

```
next-server 10.12.1.99
```

Related Commands

Command	Description
accounting (DHCP)	Specifies the name of the default boot image for a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.
ip helper-address	Forwards UDP broadcasts, including BOOTP, received on an interface.
option	Configures Cisco IOS DHCP server options.

nhrp cache limit

To configure the maximum number of entries that can be stored in the Next Hop Resolution Protocol (NHRP) cache on a device, issue the **nhrp cache limit** command in global configuration mode. To remove the maximum limit on the number of NHRP cache entries, use the **no** form of this command.

nhrp cache limit *max-entries* { **fifo** | **lifo** }

no nhrp cache limit *max-entries* { **fifo** | **lifo** }

Syntax Description

max-entries	The maximum number of entries that can be stored in the NHRP cache on the device. This limit is cumulative and is the maximum number of NHRP entries that can be cached on the device across all VRFs and NHRP instances. Range: 1 - 2147483646 Default: No limit
fifo|**lifo**	• **fifo**: The oldest cache entry is purged when the number of cache entries exceeds the configured limit. **Note** If you configure the **fifo** mode, you must delete all cache entries globally before the limit is applied in this mode. If you do not delete the cache entries, parser return code (PRC) failure occurs and the device reports the following error message: 'Please delete all NHRP Cache entries before using FIFO for limiting Cache table.' • **lifo**: The newest cache entry is purged when the number of cache entries exceeds the configured limit. In this mode, if the number of cache entries exceeds the limit at the time of configuration, the limit is applied only after the number of cache entries falls below the configured limit.

Command Default

There is no limit on the number of cache entries if this command is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.4	Command introduced.

Example

In this example, the number of NHRP cache entries is limited to 65, 536.

```
Device> enable
Device# configure terminal
Device(config)# nhrp cache limit 65536
Device(config)# end
```

Related Commands

clear ip nhrp	Clears all dynamic entries from the Next Hop Resolution Protocol (NHRP) cache.
no ip nhrp map	Clears a statically configured entry from the Next Hop Resolution Protocol (NHRP) cache.

nhrp group

To configure a Next Hop Resolution Protocol (NHRP) group on a spoke, use the **nhrp group** command in interface configuration mode. To remove an NHRP group, use the **no** form of this command.

nhrp group *group-name*
no nhrp group *group-name*

Syntax Description

group-name	Specifies an NHRP group name.

Command Default

No NHRP groups are created.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.4(1)T	This command was introduced.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

After you create an NHRP group on a spoke, you use the **nhrp map group** command to map the group to a QoS policy map.

Note This command will replace the **ip nhrp group** command in a future release.

Examples

The following example shows how to create two NHRP groups named small and large.

```
Device> enable
Device# configure terminal
Device(config)# interface Tunnel 0
Device(config-if)# nhrp group small
Device(config-if)# nhrp group large
```

Related Commands

Command	Description
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
nhrp map group	Adds NHRP groups to QoS policy mappings on a hub.
show dmvpn	Displays DMVPN-specific session information.
show nhrp	Displays NHRP mapping information.
show nhrp group-map	Displays the details of NHRP group mappings on a hub and the list of tunnels using each of the NHRP groups defined in the mappings.

Command	Description
show policy-map mgre	Displays statistics about a specific QoS policy as it is applied to a tunnel endpoint.

nhrp map group

To associate a Next Hop Resolution Protocol (NHRP) group to a QoS policy map, use the **nhrp map group** command in interface configuration mode. To remove an association, use the **no** form of this command.

nhrp map group *group-name* **service-policy output** *qos-policy-map-name*
no nhrp map group *group-name* **service-policy output** *qos-policy-map-name*

Syntax Description

service-policy	Specifies a QoS service policy
group-name	Specifies an NHRP group name.
qos-policy-map-name	Specifies a QoS policy map name.

Command Default

No mappings are created.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.4(1)T	This command was introduced.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

The command allows a QoS policy in the output direction only.

Note This command will replace the **ip nhrp map group** command in a future release.

Examples

The following example shows how to map two NHRP groups named small and large to two QoS policy maps named qos-small and qos-large respectively.

```
Device> enable
Device# configure terminal
Device(config)# interface Tunnel 0
Device(config-if)# nhrp map group small service-policy output qos-small
Device(config-if)# nhrp map group large service-policy output qos-large
```

Related Commands

Command	Description
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
nhrp group	Configures an NHRP group on a spoke.
show dmvpn	Displays DMVPN-specific session information.

Command	Description
show nhrp	Displays NHRP mapping information.
show nhrp group-map	Displays the details of NHRP group mappings on a hub and the list of tunnels using each of the NHRP groups defined in the mappings.
show policy-map mgre	Displays statistics about a specific QoS policy as it is applied to a tunnel endpoint.

nis address

To specify the network information service (NIS) address of an IPv6 server to be sent to the client, use the **nis address** command in DHCP for IPv6 pool configuration mode. To remove the NIS address, use the **no** form of this command.

nis address *ipv6-address*
no nis address *ipv6-address*

Syntax Description

ipv6-address	The NIS address of an IPv6 server to be sent to the client.

Command Default

No NIS address is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS server option provides a list of one or more IPv6 addresses of NIS servers available to send to the client. The client must view the list of NIS servers as an ordered list, and the server may list the NIS servers in the order of the server's preference.

The NIS server option code is 27. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to specify the NIS address of an IPv6 server:

```
nis address 23::1
```

Related Commands

Command	Description
import nis address	Imports the NIS server option to a DHCP for IPv6 client.
nis domain-name	Enables a server to convey a client's NIS domain name information to the client.

nis domain-name

To enable a server to convey a client's network information service (NIS) domain name information to the client, use the **nis domain-name**command in DHCP for IPv6 pool configuration mode. To remove the domain name, use the **no** form of this command.

nis domain-name *domain-name*
no nis domain-name *domain-name*

Syntax Description

domain-name	The domain name of an IPv6 server to be sent to the client.

Command Default

No NIS domain name is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS domain name option provides a NIS domain name for the client. Use the **nis domain-name** command to specify the client's NIS domain name that the server sends to the client.

The NIS domain name option code is 29. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to enable the IPv6 server to specify the NIS domain name of a client:

```
nis domain-name cisco1.com
```

Related Commands

Command	Description
import nis domain	Imports the NIS domain name option to a DHCP for IPv6 client.
nis address	Specifies the NIS address of an IPv6 server to be sent to the client.

nisp domain-name

To enable an IPv6 server to convey a client's network information service plus (NIS+) domain name information to the client, use the **nisp domain-name**command in DHCP for IPv6 pool configuration mode. To remove the domain name, use the **no** form of this command.

nisp domain-name *domain-name*
no nisp domain-name *domain-name*

Syntax Description

domain-name	The NIS+ domain name of an IPv6 server to be sent to the client.

Command Default

No NIS+ domain name is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS+ domain name option provides a NIS+ domain name for the client. Use the **nisp domain-name** command to enable a server to send the client its NIS+ domain name information.

The NIS+ domain name option code is 30. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to enable the IPv6 server to specify the NIS+ domain name of a client:

```
nisp domain-name cisco1.com
```

Related Commands

Command	Description
import nisp domain	Imports the NIS+ domain name option to a DHCP for IPv6 client.
nisp address	Specifies the NIS+ address of an IPv6 server to be sent to the client.

nisp address

To specify the network information service plus (NIS+) address of an IPv6 server to be sent to the client, use the **nisp address** command in DHCP for IPv6 pool configuration mode. To remove the NIS+ address, use the **no** form of the command.

nisp address *ipv6-address*
no nisp address *ipv6-address*

Syntax Description

ipv6-address	The NIS+ address of an IPv6 server to be sent to the client.

Command Default

No NIS+ address is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS+ servers option provides a list of one or more IPv6 addresses of NIS+ servers available to send to the client. The client must view the list of NIS+ servers as an ordered list, and the server may list the NIS+ servers in the order of the server's preference.

The NIS+ servers option code is 28. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to specify the NIS+ address of an IPv6 server:

```
nisp address 33::1
```

Related Commands

Command	Description
import nisp address	Imports the NIS+ servers option to a DHCP for IPv6 client.
nisp domain-name	Enables a server to convey a client's NIS+ domain name information to the client.

odap client

To configure On–Demand Address Pooling (ODAP) client parameters, use the **odap client** command in DHCP pool configuration mode. To remove ODAP client parameters, use the **no** form of this command.

odap client {**client-id** *id* [**interface** *type number*] [**target-server** *ip-address*] | **interface** *type number* [**client-id** *id*] [**target-server** *ip-address*] | **target-server** *ip-address* [**client-id** *id*] [**interface** *type number*]}
no odap client {**client-id** *id* [**interface** *type number*] [**target-server** *ip-address*] | **interface** *type number* [**client-id** *id*] [**target-server** *ip-address*] | **target-server** *ip-address* [**client-id** *id*] [**interface** *type number*]}

Syntax Description

client-id *id*	Configures the client ID string.
interface *type number*	(Optional) Specifies the outgoing interface for sending subnet allocation request.
target-server *ip-address*	(Optional) Configures the target ODAP server's IP address.

Command Default

The outgoing interface for sending subnet allocation request is not configured.

The Cisco IOS DHCP ODAP client module prepares the client ID to be sent in the subnet allocation request by concatenating the router hostname with the subnet pool name.

The target ODAP server's IP address is not configured.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

Release	Modification
15.2(1)T	This command was introduced.

Usage Guidelines

Use the **odap client** command to configure ODAP client parameters. You must configure one of the parameters. The parameters can be specified in any order.

Examples

The following example shows how to configure ODAP client parameters:

```
Router# configure terminal
Router(config)# ip dhcp pool pool1
Router(dhcp-config)# odap client client-id id1 interface gigabitethernet 0/0 target-server
 192.168.10.1
Eouter(dhcp-config)# end
```

Related Commands

Command	Description
odap server	Configures the ODAP server parameters.

odap server

To configure On–Demand Address Pooling (ODAP) server parameters, use the **odap server** command in DHCP pool configuration mode. To remove the ODAP server parameter settings, use the **no** form of this command.

odap server {**rebind-time** *percent-value* [**renew-time** *percent-value*] | **renew-time** *percent-value* [**rebind-time** *percent-value*]}
no odap server {**rebind-time** *percent-value* [**renew-time** *percent-value*] | **renew-time** *percent-value* [**rebind-time** *percent-value*]}

Syntax Description

rebind-time	Specifies the rebind timer.
percent-value	Percentage value of total lease.
renew-time	Specifies the renew timer.

Command Default

ODAP server parameters are not configured.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

Release	Modification
15.2(1)T	This command was introduced.

Usage Guidelines

Use the **odap server** command to configure ODAP server parameters. You must specify either the rebind time or the renew time. You can specify the rebind time and renew time in any order. The rebind time cannot be less than the renew time.

Examples

The following example shows how to configure ODAP server parameters:

```
Router# configure terminal
Router(config)# ip dhcp pool pool1
Router(dhcp-config)# odap server rebind-time 20 renew-time 10
Router(dhcp-config)# end
```

Related Commands

Command	Description
odap client	Configures ODAP client parameters.

option

To configure DHCP server options, use the **option** command in DHCP pool configuration mode. To remove the options, use the **no** form of this command.

option *code* [**instance** *number*] {**ascii** *string* | **hex** {*string* | **none**} | **ip** {*addresshostname*}}
no option *code* [**instance** *number*]

Syntax Description

code	Specifies the DHCP option code. The range is from 0 to 254.
instance *number*	(Optional) Specifies an instance number. The range is from 0 to 255. The default is 0.
ascii *string*	Specifies a network virtual terminal (NVT) ASCII character string. ASCII character strings that contain white spaces must be delimited by quotation marks. The ASCII value is truncated to 255 characters entered.
hex	Specifies dotted hexadecimal data.
string	Hexadecimal value truncated to 180 characters entered. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period, colon, or white space.
none	Specifies the zero-length hexadecimal string.
ip *address*	Specifies an IP address. More than one IP address can be specified.
ip *hostname*	Specifies the hostname. More than one hostname can be specified.

Command Default

The default instance number is 0.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(24)T	This command was modified. The **none** keyword was added.
15.1(3)S	This command was modified. A maximum limit of 180 characters was set for the dotted hexadecimal data and 255 characters for the ASCII data.

Usage Guidelines

DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. The configuration parameters and other control information are carried in tagged data items that are stored in the options field of the DHCP message. The data items themselves are also called options. The current set of DHCP options is documented in RFC 2131, *Dynamic Host Configuration Protocol*.

Examples

The following example shows how to configure DHCP option 19, which specifies whether the client should configure its IP layer for packet forwarding. A value of 0 means disable IP forwarding; a value of 1 means enable IP forwarding. IP forwarding is enabled in the following example.

```
Router(config)# ip dhcp pool red
Router(dhcp-config)# option 19 hex 01
```

The following example shows how to configure DHCP option 72, which specifies the World Wide Web servers for DHCP clients. World Wide Web servers 172.16.3.252 and 172.16.3.253 are configured in the following example.

```
Router(config)# ip dhcp pool red
Router(dhcp-config)# option 72 ip 172.16.3.252 172.16.3.253
```

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

option hex

To enable a relay agent to make forwarding decisions based on DHCP options inserted in the client-generated DHCP message, use the **option hex** command in DHCP class configuration mode. To disable this functionality, use the **no** form of this command.

option *code* **hex** *hex-pattern* [*****] [**bit** *bit-mask-pattern*]
no option *code* **hex** *hex-pattern* [*****] [**mask** *bit-mask-pattern*]

Syntax Description

code	Specifies the DHCP option code. Valid values are 60, 77, 124, and 125. All other values will be rejected with the appropriate error message.
hex-pattern	String of hexadecimal values. This string creates a pattern that is matched against the named DHCP class. The *hex-pattern* argument represents the data portion of the DHCP option format. See "Usage Guidelines" below for more information. The hexadecimal value is truncated to 180 characters entered. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period, colon, or white space.
*	(Optional) Wildcard character.
mask *bit-mask-pattern*	(Optional) String of hexadecimal values. Specifies the bit mask to be applied to the *hex-pattern* argument.

Command Default

This command is disabled by default.

Command Modes

DHCP class configuration (config-dhcp-class)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

The **option hex** command enhances DHCP class support to allow the relay agent to relay client-generated messages to different DHCP servers based on the content of the following four options:

- Option 60: vendor class identifier
- Option 77: user class
- Option 124: vendor-identifying vendor class
- Option 125: vendor-identifying vendor-specific information

Each option identifies the type of client sending the DHCP message.

The table below describes the CLI variations possible for the **hex** *hex-pattern* keyword and argument combination.

Table 6: option hex CLI Variations

Hex string format variations	CLI example	Description
Full option value as raw hex	`option 60 hex 010203`	This option has 3 bytes of data with 0x010203 hex as the content.
Bit-masked hex string	`option 60 hex 010203 mask 0000FF`	This option is the same as above except that only the first 2 bytes of data should be 0x0102.
Wild-carded hex string	`option 60 hex 010203*`	This option should have at least 3 bytes, with the first 3 bytes matching the specified hex pattern.

You must know the hexadecimal value of each byte location in the options to be able to configure the **option hex** command. The format may vary from product to product. Contact the relay agent vendor for this information.

Examples

In the following example, client-generated DHCP messages containing option 60 and belonging to class VOIP will be forwarded to the DHCP server located at 10.30.5.1:

```
!
ip dhcp class VOIP
 option 60 hex 010203
!
! The following is the relay pool
ip dhcp pool red
 relay source 10.2.2.0 255.255.255.0
 class VOIP
  relay target 10.30.5.1
```

Related Commands

Command	Description
ip dhcp class	Defines a DHCP class and enters DHCP class configuration mode.

option ext

To configure DHCP extended server options, use the **option ext** command in DHCP pool configuration mode. To remove the options, use the **no** form of this command.

option ext *code* {**ascii** *string* | **hex** *string*}
no option ext *code*

Syntax Description

code	Specifies the DHCP option code. The range is from 0 to 254. **Note** Only option 43 is supported under extended options. If you select any other option code, you will get a message that it is not supported.
ascii *string*	Specifies a network virtual terminal (NVT) ASCII character string. ASCII character strings that contain white space must be delimited by quotation marks.
hex *string*	Specifies dotted hexadecimal data. Each byte in hexadecimal character strings is two hexadecimal digits—each byte can be separated by a period, colon, or white space.

Command Default

DHCP extended server options are not configured.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

Release	Modification
Cisco IOS XE Release 3.2.1S	This command was introduced.

Usage Guidelines

Using the **option ext** command you can specify an ASCII string upto 255 characters or 255 bytes of hexadecimal data. To do this, you need to break the string into three sets and then execute the **option ext** command three times, specifying the three strings.

```
option ext 43 ascii <first 100 characters>
option ext 43 ascii <next 100 characters>
option ext 43 ascii <last 55 characters>
```

If you want to enter 220 characters of ASCII data, you need to break the string into three, for example, two containing 100 characters each and the other containing the remaining 20 characters.

```
option ext 43 ascii <first 100 characters>
option ext 43 ascii <next 100 characters>
option ext 43 ascii <last 20 characters>
```

At any time, you can append additional characters to the string if the maximum length (255 characters or bytes) is not reached.

Only single format can be used between consecutive extended commands; that is, you cannot enter the first 100 bytes in ASCII and the next 100 bytes in hexadecimal or vice versa. Also, only one type of **option** command can be used as consecutive commands. That is, you cannot enter the **option** command and then the **option ext** command.

Use the **no option** or **no option ext** command to remove the configured option and configure the new option using the **option ext** command.

Examples

The following example shows how to configure DHCP extended option 43 and an ASCII string with 25 characters. The ASCII string of 25 characters is configured using three **option ext** commands.

```
Router(config)# ip dhcp pool pool1
Router(dhcp-config)# option ext 43 ascii 1111111111
Router(dhcp-config)# option ext 43 ascii 1111111111
Router(dhcp-config)# option ext 43 ascii 11111
```

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.
option	Configures DHCP server options.
option hex	Enables the Cisco IOS relay agent to make forwarding decisions based on DHCP options inserted in the client-generated DHCP message.

origin

To configure an address pool as an on-demand address pool (ODAP) or static mapping pool, use the **origin** command in DHCP pool configuration mode. To disable the ODAP, use the **no** form of this command.

origin {**dhcp** [**number** *number* | **subnet size initial** *size* [**autogrow** *size*]] | **aaa** [**subnet size initial** *size* [**autogrow** *size*]] | **file** *url* [**refresh** [**interval** *minutes*]] | **ipcp**}
no origin {**dhcp** [**number** *number* | **subnet size initial** *size* [**autogrow** *size*]] | **aaa** [**subnet size initial** *size* [**autogrow** *size*]] | **file** *url* [**refresh** [**interval** *minutes*]] | **ipcp**}

Syntax Description

dhcp	Specifies Dynamic Host Configuration Protocol (DHCP) as the subnet allocation protocol.
number *number*	(Optional) Specifies the number of subnets to request. The range is from 1 to 5.
subnet size initial *size*	(Optional) Specifies the initial size of the first requested subnet. You can enter the value for the *size* argument as either the subnet mask (nnnn.nnnn.nnnn.nnnn) or prefix size (/nn). The valid values are /0 and /4 to /30.
autogrow *size*	(Optional) Specifies that the pool can grow incrementally. The value for the *size* argument is the size of the requested subnets when the pool requests additional subnets (upon detection of high utilization). You can enter the value for the *size* as either the subnet mask (nnnn.nnnn.nnnn.nnnn) or prefix size (/nn). The valid values are /0 and /4 to /30.
aaa	Specifies authentication, authorization, and accounting (AAA) as the subnet allocation protocol.
file *url*	Specifies the external database file that contains the static bindings assigned by the DHCP server. The *url* argument specifies the location of the external database file.
refresh	Specifies to refresh or reread the DHCP static mapping file.
interval *minutes*	Specifies the refresh or reread interval, in minutes, for DHCP static mapping file. The range is from 1 to 500.
ipcp	Specifies the IP Control Protocol (IPCP) as the subnet allocation protocol.

Command Default

The default value for the *size* argument is /0.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.3(11)T	This command was modified. The **file** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Release	Modification
15.2(1)T	This command was modified. The **number**, **refresh**, and **interval** keywords and the *number* and *minutes* arguments were added.

Usage Guidelines

If you do not configure the pool as an autogrow pool, the pool will not request additional subnets if one subnet is already in the pool.

Use the **dhcp** keyword to obtain subnets from DHCP, the **aaa** keyword to obtain subnets from the AAA server, and the **ipcp** keyword to obtain subnets from IPCP negotiation. If you expect that the utilization of the pool may grow over time, use the **autogrow** *size* option.

If a pool has been configured with the **autogrow** *size* option, ensure that the source server can provide more than one subnet to the same pool. Even though the Cisco IOS software specifies the requested subnet size, it can accept any offered subnet size from the source server.

Examples

The following example shows how to configure an address pool named pool1 to use DHCP as the subnet allocation protocol with an initial subnet size of 24 and an autogrow subnet size of 24:

```
ip dhcp pool pool1
  vrf pool1
  origin dhcp subnet size initial /24 autogrow /24
  utilization mark high 80
  utilization mark low 20
```

The following example shows how to configure the location of the external text file:

```
ip dhcp pool abcpool
 origin file tftp://10.1.0.1/staticbindingfile
```

Related Commands

Command	Description
show ip dhcp pool	Displays information about the DHCP address pools.

override default-router

To define a default router list for the DHCP pool secondary subnet, use the **override default-router** command in DHCP pool secondary subnet configuration mode. To remove the default router list for this secondary subnet, use the **no** form of this command.

override default-router *address* [*address2 ... address8*]
no override default-router

Syntax Description

address	IP address of the default router for the DHCP pool secondary subnet, preferably on the same subnet as the DHCP pool secondary client subnet.
address2 ... address8	(Optional) IP addresses of up to seven additional default routers, delimited by a single space. **Note** The ellipses in the syntax description are used to indicate a range of values. Do not use ellipses when entering IP addresses.

Command Default

No default router list is defined for the DHCP pool secondary subnet.

Command Modes

DHCP pool secondary subnet configuration

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

When an IP address is assigned to the DHCP client from a secondary subnet for which no subnet-specific default router list is defined, the default router list (configured by using the **default-router** command in DHCP pool configuration mode) will be used.

The IP address of every router in the list should be on the same subnet as the client subnet. You can specify up to eight routers in the list. Routers are listed in order of preference (*address* is the most preferred router, *address2* is the next most preferred router, and so on).

To display the default router lists, use the **show running-config** command. If default router lists are configured for a DHCP pool, the commands used to configure those lists are displayed following the **ip dhcp pool** command that configures the DHCP pool.

Examples

The following example configures 10.1.1.1/29 as the subnetwork number and mask of the DHCP pool named pool1, adds the DHCP pool secondary subnet specified by the subnet number and mask 10.1.1.17/29, then configures a subnet-specific default router list for that subnet:

```
Router(config)# dhcp pool pool1

Router(config-dhcp)# network 10.1.1.1 255.255.255.248

Router(config-dhcp)# network 10.1.1.17 255.255.255.248 secondary
```

```
Router(config-dhcp-secondary-subnet)# override default-router 10.1.1.100 10.1.1.200
```

Related Commands

Command	Description
default-router	Specifies the default router list for a DHCP client.
network (DHCP)	Configures the subnet number and mask for a DHCP address pool primary or secondary subnet on a Cisco IOS DHCP server.

override utilization high

To configure the high utilization mark of the current secondary subnet size, use the **override utilization high** command in DHCP pool secondary subnet configuration mode. To remove the high utilization mark, use the **no** form of this command.

override utilization high *percentage-number*
no override utilization high *percentage-number*

Syntax Description

percentage-number	Percentage of the current subnet size. The range is from 1 to 100 percent.

Command Default

The default high utilization mark is 100 percent of the current subnet size.

Command Modes

DHCP pool secondary subnet configuration (config-dhcp-subnet-secondary)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.

Usage Guidelines

If you use the **utilization mark** {**high** | **low**} **log** command, a system message can be generated for a DHCP secondary subnet when the subnet utilization exceeds the configured high utilization threshold. A system message can also be generated when the subnet's utilization is detected to be below the configured low utilization threshold.

The **override utilization high** command overrides the value specified by the **utilization mark high** global configuration command.

Examples

The following example shows how to set the high utilization mark of the secondary subnet to 40 percent of the current subnet size:

```
Router(config)# ip dhcp pool pool2
Router(dhcp-config)# utilization mark high 80 log
Router(dhcp-config)# utilization mark low 70 log
Router(dhcp-config)# network 192.0.2.0 255.255.255.0
Router(dhcp-config)# network 192.0.4.0 255.255.255.252 secondary
Router(config-dhcp-subnet-secondary)# override utilization high 40
Router(config-dhcp-subnet-secondary)# override utilization low 30
```

Related Commands

Command	Descriptions
override utilization low	Configures the low utilization mark of the current subnet size.
utilization mark high	Configures the high utilization mark of the current address pool size.

override utilization low

To configure the low utilization mark of the current secondary subnet size, use the **override utilization low** command in DHCP pool secondary subnet configuration mode. To remove the low utilization mark, use the **no** form of this command.

override utilization low *percentage-number*
no override utilization low *percentage-number*

Syntax Description

percentage-number	Percentage of the current subnet size. The range is from 1 to 100.

Command Default

The default low utilization mark is 0 percent of the current subnet size.

Command Modes

DHCP pool secondary subnet configuration (config-dhcp-subnet-secondary)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.

Usage Guidelines

If you use the **utilization mark**{**high**| **low**} **log** command, a system message can be generated for a DHCP secondary subnet when the subnet utilization falls below the configured low utilization threshold. A system message can also be generated when the subnet's utilization exceeds the configured high utilization threshold.

The **override utilization low** command overrides the value specified by the **utilization mark low** global configuration command.

Examples

The following example shows how to set the low utilization mark of the secondary subnet to 30 percent of the current subnet size:

```
Router(config)# ip dhcp pool pool2
Router(dhcp-config)# utilization mark high 80 log
Router(dhcp-config)# utilization mark low 70 log
Router(dhcp-config)# network 192.0.2.0 255.255.255.0
Router(dhcp-config)# network 192.0.4.0 255.255.255.252 secondary
Router(config-dhcp-subnet-secondary)# override utilization high 40
Router(config-dhcp-subnet-secondary)# override utilization low 30
```

Related Commands

Command	Description
override utilization high	Configures the high utilization mark of the current subnet size.
utilization mark low	Configures the low utilization mark of the current address pool size.

port-parameters

To configure port parameters for a Network Address Translation 64 (NAT64) mapping of addresses and ports (MAP-T) basic mapping rule (BMR), use the **port-parameters** command in NAT64 MAP-T BMR configuration mode. To remove the port parameters, use the **no** form of this command.

port-parameters share-ratio *ratio* [**port-offset-bits** *port-offset-bits* [**start-port** *port-number*] | **start-port** *port-number*][**no-eabits**]
no port-parameters

Syntax Description

share-ratio *ratio*	Specifies the NAT64 MAP-T BMR port share ratio. Valid values for the *ratio* argument are from 1 to 4096.
port-offset-bits *port-offset-bits*	(Optional) Specifies the port offset bits. Valid values for the *port-offset-bits* argument are from 1 to 16.
start-port *port -number*	(Optional) Specifies the NAT64 MAP-T BMR starting port. Valid values for the *port-number* argument are from 1024 to 65535.
no-eabits	(Optional) Specifies the no embedded address bits.

Command Default

Command Modes

NAT64 MAP-T BMR configuration (config-nat64-mapt-bmr)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.
Cisco IOS Release 15.5(2)T	This command was integrated into Cisco IOS Release 15.5(2)T.

Usage Guidelines

MAP-T or Mapping of address and port (MAP) double stateless translation-based solution (MAP-T) provides IPv4 hosts connectivity to and across an IPv6 domain. MAP-T builds on existing stateless IPv4/IPv6 address translation techniques that are specified in RFC 6052, RFC 6144, and RFC 6145.

Examples

The following example shows how to configure port parameters for a NAT64 MAP-T basic mapping rule:

```
Device(config)# nat64 map-t domain 89
Device(config-nat64-mapt)# basic-mapping-rule
Device(config-nat4-mapt-bmr)# port-parameters share-ratio 234 start-port 2300
```

Related Commands

Command	Description
basic-mapping-rule	Configures a basic mapping rule for NAT64 MAP-T.
nat64 map-t	Configures NAT64 MAP-T settings.

preempt

To enable preemption on the redundancy group, use the **preempt**command in redundancy application group configuration mode. To disable the group's preemption, use the **no** form of this command.

preempt
no preempt

Syntax Description

This command has no arguments or keywords.

Command Default

Preemption is disabled on the redundancy group.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

When the preemption is enabled, it means that a standby redundancy group should preempt an active redundancy group if its priority is higher than the active redundancy group.

Note If you allocate a large amount of memory to the log buffer (e.g. 1 GB), then the CPU and memory utilization of the router increases. This issue is compounded if small intervals are set for the hellotime and the holdtime. If you want to allocate a large amount of memory to the log buffer, we recommend that you accept the default values for the hellotime and holdtime. For the same reason, we also recommend that you do not use the **preempt** command.

Examples

The following example shows how to enable preemption on the redundancy group:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp) preempt
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
group(firewall)	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
protocol	Defines a protocol instance in a redundancy group.

preference (DHCPv6 Guard)

To enable verification that the advertised preference (in preference option) is greater than the minimum specified limit and less than the maximum specified limit, use the **preference** command in Dynamic Host Configuration Protocol version 6 (DHCPv6) guard configuration mode. To remove the preference, use the **no** form of this command.

preference {**max** | **min**}*limit*
no preference {**max** | **min**}*limit*

Syntax Description

limit	The maximum or minimum limit that the advertised preference must conform to. The acceptable range is from 0 to 255.

Command Default

No preference value is set.

Command Modes

DHCPv6 guard configuration (config-dhcp-guard)

Command History

Release	Modification
15.2(4)S	This command was introduced.

Usage Guidelines

This command enables verification that the advertised preference is not greater than the maximum specified limit or less than the minimum specified limit.

Examples

The following example defines an DHCPv6 guard policy name as policy1, places the router in DHCPv6 guard configuration mode, and enables verification that the advertised preference is not greater than 254 or less than 2:

```
Router(config)# ipv6 dhcp guard policy policy1
Router(config-dhcp-guard)# preference min 2
Router(config-dhcp-guard)# preference max 254
```

Related Commands

Command	Description
ipv6 dhcp guard policy	Defines the DHCPv6 guard policy name.

prefix-delegation

To specify a manually configured numeric prefix to be delegated to a specified client (and optionally a specified identity association for prefix delegation [IAPD] for that client), use the **prefix-delegation** command in DHCP for IPv6 pool configuration mode. To remove the prefix, use the **no** form of this command.

prefix-delegation *ipv6-prefix/prefix-length client-DUID* [**iaid** *iaid*] [*lifetime*]
no prefix-delegation *ipv6-prefix/prefix-length client-DUID* [**iaid** *iaid*]

Syntax Description

ipv6-prefix	(Optional) Specified IPv6 prefix. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/ *prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).
client-DUID	The DHCP unique identifier (DUID) of the client to which the prefix is delegated.
iaid *iaid*	(Optional) Identity association identifier (IAID), which uniquely identifies an IAPD on the client.
lifetime	(Optional) Sets a length of time over which the requesting router is allowed to use the prefix. The following values can be used: • **valid-lifetime** --The length of time, in seconds, that the prefix remains valid for the requesting router to use. • **at** --Specifies absolute points in time where the prefix is no longer valid and no longer preferred. • **infinite** --Indicates an unlimited lifetime. • **preferred-lifetime** --The length of time, in seconds, that the prefix remains preferred for the requesting router to use. • *valid-month valid-date valid-year valid-time* --A fixed duration of time for hosts to remember router advertisements. The format to be used can be **oct 24 2003 11:45** or **24 oct 2003 11:45** • *preferred-month preferred-date preferred-year preferred-time*-- A fixed duration of time for hosts to remember router advertisements. The format to be used can be **oct 24 2003 11:45** or **24 oct 2003 11:45**.

Command Default

No manually configured prefix delegations exist.

Command Modes

DHCP for IPv6 pool configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

Administrators can manually configure a list of prefixes and associated preferred and valid lifetimes for an IAPD of a specific client that is identified by its DUID. This static binding of client and prefixes can be specified based on users' subscription to an ISP using the **prefix-delegation***prefix-length* command.

The *client-DUID* argument identifies the client to which the prefix is delegated. All the configured prefixes will be assigned to the specified IAPD of the client. The IAPD to which the prefix is assigned is identified by the **iaid** argument if the **iaid** keyword is configured. If the **iaid** keyword is not configured, the prefix will be assigned to the first IAPD from the client that does not have a static binding. This function is intended to make it convenient for administrators to manually configure prefixes for a client that only sends one IAPD in case it is not easy to know the iaid in advance.

When the delegating router receives a request from a client, it checks whether there is a static binding configured for the IAPD in the client's message. If one is present, the prefixes in the binding are returned to the client. If no such binding is found, the server attempts to assign prefixes for the client from other sources.

Optionally valid and preferred lifetimes can be specified for the prefixes assigned from this pool. Users should coordinate the specified lifetimes with the lifetimes on prefixes from the upstream delegating router if the prefixes were acquired from that router.

The **lifetime**keyword can be specified in one of two ways:

- A fixed duration that stays the same in consecutive advertisements.
- Absolute expiration time in the future so that advertised lifetime decrements in real time, which will result in a lifetime of 0 at the specified time in the future.

The specified length of time is between 60 and 4294967295 seconds or infinity if the **infinite** keyword is specified.

Examples

The following example configures an IAPD for a specified client:

```
prefix-delegation 2001:0DB8::/64 00030001000BBFAA2408
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCP for IPv6 pool and enters DHCP for IPv6 pool configuration mode.
ipv6 local pool	Configures a local IPv6 prefix pool.
prefix-delegation pool	Specifies a named IPv6 local prefix pool from which prefixes are delegated to DHCP for IPv6 clients.
show ipv6 dhcp pool	Displays DHCP for IPv6 configuration pool information.

prefix-delegation aaa

To specify that prefixes are to be acquired from authorization, authentication, and accounting (AAA) servers, use the **prefix-delegation aaa**command in DHCP for IPv6 pool configuration mode. To disable this feature, use the **no** form of this command.

Cisco IOS Release 12.4(22)T and Earlier Releases and Cisco IOS Release 12.2(18)SXE, Cisco IOS XE Release 2.1, and Later Releases

prefix-delegation aaa [**method-list** *method-list* [**lifetime**] { {*valid-lifetime* | **infinite**} {*valid-lifetime* | **infinite**} | **at** {*date month year time* | *month date year time*} {*date month year time* | *month date year time*}}]

no prefix-delegation aaa method-list *method-list*

Cisco IOS Release 15.0(1)M and Later Releases

prefix-delegation aaa method-list {*method-list* | **default**} [**lifetime** {*valid-lifetime* | **infinite**} {*preferred-lifetime* | **infinite**} | **at** {*date month year time* | *month date year time*} {*date month year time* | *month date year time*}]

no prefix-delegation aaa method-list *method-list*

Syntax Description

method-list	(Optional) Indicates a method list to be defined.
method-list	Configuration type AAA authorization method list that defines how authorization will be performed.
default	Specifies the default method list, nvgened.
lifetime	(Optional) Configures prefix lifetimes.
valid-lifetime	The length of time that the prefix remains valid for the requesting router to use, in seconds. The range is from 60 to 4294967295. The default value is 2592000 seconds.
infinite	Indicates an unlimited lifetime.
preferred-lifetime	The length of time that the prefix remains preferred for the requesting router to use, in seconds. The range is from 60 to 4294967295. The default value is 604800 seconds.
at	Specifies absolute points in time where the prefix is no longer valid and no longer preferred.
date	The date for the valid lifetime to expire.
month	The month for the valid lifetime to expire.
year	The year for the valid lifetime to expire. The range is from 2003 to 2035.
time	The year for the valid lifetime to expire.

Command Default

The default time that the prefix remains valid is 2592000 seconds, and the default time that the prefix remains preferred for the requesting router to use is 604800 seconds.

Command Modes

DHCP for IPv6 pool configuration (config-dhcpv6)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(1)M	This command was modified. The **default** keyword was added and the command syntax was modified to show that **lifetime** can be configured only to a **method-list**.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

In order for the Dynamic Host Configuration Protocol (DHCP) for IPv6 server to obtain prefixes from RADIUS servers, you must also configure the AAA client and Point-to-Point Protocol (PPP) on the router. For information on how to configure the AAA client and PPP, see the "Implementing ADSL and Deploying Dial Access for IPv6" module.

Use the **aaa authorization configuration default**, **aaa group server radius**, and **radius-server host** commands to specify a named list of authorization method and RADIUS servers to contact to acquire prefixes, and then apply that named list to the **prefix-delegation aaa** command.

Valid and preferred lifetimes can be specified for the prefixes assigned from AAA servers.

The **prefix-delegation aaa** and **prefix-delegation pool** commands are mutually exclusive in a pool.

Examples

The following example shows how to specify the use of a method list named list1:

```
Router> enable
Router# configure terminal
Router(config)# ipv6 dhcp pool name
Router(config-dhcpv6)# prefix-delegation aaa method-list list1
```

Related Commands

Command	Description
aaa authorization configuration default	Downloads static route configuration information from the AAA server using TACACS+ or RADIUS.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
prefix-delegation pool	Specifies a named IPv6 local prefix pool from which prefixes are delegated to DHCP for IPv6 clients.
radius-server host	Specifies a RADIUS server host.
sip address	Configures a SIP server IPv6 address to be returned in the SIP server's IPv6 address list option to clients.

Command	Description
sip domain-name	Configures an SIP server domain name to be returned in the SIP server's domain name list option to clients.

prefix-delegation pool

To specify a named IPv6 local prefix pool from which prefixes are delegated to Dynamic Host Configuration Protocol (DHCP) for IPv6 clients, use the **prefix-delegation pool**command in DHCP for IPv6 pool configuration mode. To remove a named IPv6 local prefix pool, use the **no** form of this command.

prefix-delegation pool *poolname* [**lifetime** *valid-lifetime preferred-lifetime*]
no prefix-delegation pool *poolname*

Syntax Description

poolname	User-defined name for the local prefix pool. The pool name can be a symbolic string (such as "Engineering") or an integer (such as 0).
lifetime	(Optional) Used to set a length of time for the hosts to remember router advertisements. If the optional **lifetime** keyword is configured, both valid and preferred lifetimes must be configured.
valid-lifetime	The amount of time that the prefix remains valid for the requesting router to use. The following values can be used: • *seconds* --The length of time, in seconds, that the prefix remains valid for the requesting router to use. The range is from 60 through 4294967295. The *preferred-lifetime* value cannot exceed the *valid-lifetime* value. • **at** --Specifies absolute points in time where the prefix is no longer valid and no longer preferred. • **infinite** --Indicates an unlimited lifetime. • *valid-month valid-date valid-year valid-time* --A fixed duration of time for hosts to remember router advertisements. The format to be used can be **oct 24 2003 11:45** or **24 oct 2003 11:45**.
preferred-lifetime	The length of time, in seconds, that the prefix remains preferred for the requesting router to use. The following values can be used: • *seconds* --The length of time, in seconds, that the prefix remains valid for the requesting router to use. The range is from 60 through 4294967295. The *preferred-lifetime* value cannot exceed the *valid-lifetime* value. • **at** --Specifies absolute points in time where the prefix is no longer valid and no longer preferred. • **infinite** --Indicates an unlimited lifetime. • *preferred-month preferred-date preferred-year preferred-time*-- A fixed duration of time for hosts to remember router advertisements. The format to be used can be **oct 24 2003 11:45** or **24 oct 2003 11:45**

Command Default

No IPv6 local prefix pool is specified. Valid lifetime is 2592000 seconds (30 days). Preferred lifetime is 604800 seconds (7 days).

Command Modes

DHCP for IPv6 pool configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The **prefix-delegation pool**command specifies a named IPv6 local prefix pool from which prefixes are delegated to clients. Use the **ipv6 local pool** command to configure the named IPv6 prefix pool.

Optionally, valid and preferred lifetimes can be specified for the prefixes assigned from this pool. Users should coordinate the specified lifetimes with the lifetimes on prefixes from the upstream delegating router if the prefixes were acquired from that router.

The **lifetime**keyword can be specified in one of two ways:

- A fixed duration that stays the same in consecutive advertisements.
- Absolute expiration time in the future so that advertised lifetime decrements in real time, which will result in a lifetime of 0 at the specified time in the future.

The specified length of time is from 60 to 4,294,967,295 seconds or infinity if the **infinite** keyword is specified.

The Cisco IOS DHCP for IPv6 server can assign prefixes dynamically from an IPv6 local prefix pool, which is configured using the **ipv6 local pool** command and associated with a DHCP for IPv6 configuration pool using the **prefix-delegation pool** command. When the server receives a prefix request from a client, it attempts to obtain unassigned prefixes, if any, from the pool.

After the client releases the previously assigned prefixes, the server will return the prefixes to the pool for reassignment to other clients.

Examples

The following example specifies that prefix requests should be satisfied from the pool called client-prefix-pool. The prefixes should be delegated with the valid lifetime set to 1800 seconds, and the preferred lifetime is set to 600 seconds:

```
prefix-delegation pool client-prefix-pool lifetime 1800 600
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCP for IPv6 pool and enters DHCP for IPv6 pool configuration mode.
ipv6 local pool	Configures a local IPv6 prefix pool.
prefix-delegation	Specifies a manually configured numeric prefix that is to be delegated to a particular client's IAPD.
show ipv6 dhcp pool	Displays DHCP for IPv6 configuration pool information.

priority (firewall)

To specify a group priority and failover threshold value in a redundancy group, use the **priority** command in redundancy application group configuration mode. To disable the priority value of a group, use the **no** form of this command.

priority *value* [**failover-threshold** *value*]
no priority *value* [**failover-threshold** *value*]

Syntax Description

value	The priority value. The range is from 1 to 255.
failover-threshold *value*	(Optional) Specifies the failover threshold value. The range is from 1 to 255.

Command Default

The default priority value is 100.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The priority of the redundancy group is used to determine a redundancy group's active or standby role on the configured node. The failover threshold is used to determine when a switchover must occur. After the priority is set under threshold, the active redundancy group gives up its role.

Examples

The following example shows how to configure the priority value and threshold value for the redundancy group named group1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp) priority 100 failover-threshold 90
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
group(firewall)	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.

protocol

To define a protocol instance in a redundancy group, use the **protocol**command in redundancy application configuration mode. To remove the protocol instance from the redundancy group, use the **no** form of this command.

protocol *id*
no protocol *id*

Syntax Description

id	Redundancy group protocol ID. The range is from 1 to 8.

Command Default

Protocol instance is not defined in a redundancy group.

Command Modes

Redundancy application configuration (config-red-app)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

Protocol configuration is used to configure timers and authentication method for a control interface. Thus, a protocol instance is attached to the control interface.

Examples

The following example shows how to configure a protocol named protocol 1 to a redundancy group:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# protocol 1
Router(config-red-app-prtcl)#
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
group	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.
timers hellotime	Configures timers for hellotime and holdtime messages for a redundancy group.

rate-limit (mDNS)

To configure the rate limit of incoming multicast Domain Name System (mDNS) packets on a device, use the **rate-limit** command in mDNS configuration mode. To disable rate limit configuration of incoming mDNS packets on a device, use the **no** form of this command.

rate-limit in *rate-limit*
no rate-limit in

Syntax Description

in	Specifies that a rate limit is being applied for incoming mDNS packets.
rate-limit	Rate limit value of incoming mDNS packets. **Note** You can specify a rate limit value in the range 1-100 packets per second (p/s).

Command Default

Rate limit of incoming mDNS packets on a device is not configured.

Command Modes

Multicast DNS configuration (config-mdns)

Command History

Release	Modification
15.2(2)E	This command was introduced.
Cisco IOS XE 3.6E	This command was integrated into the Cisco IOS XE 3.6E release.
Cisco IOS XE Release 3.13S	This command was integrated into the Cisco IOS XE Release 3.13S
15.2(3)E	The rate limit value range for incoming mDNS packets on a device was changed from 1-1500 p/s to 1-100 p/s.
Cisco IOS XE 3.7E	The rate limit value range for incoming mDNS packets on a device was changed from 1-1500 p/s to 1-100 p/s.
15.2(1)SY	This command was integrated into Cisco IOS Release 15.2(1)SY.
15.5(2)S	This command was integrated into Cisco IOS Release 15.5(2)S.
Cisco IOS XE Release 3.15S	This command was integrated into the Cisco IOS XE Release 3.15S

Examples

The following example shows you how to configure the rate limit of incoming mDNS packets on a device:

```
Device> enable
Device# configure terminal
Device(config)# service-routing mdns-sd
Device(config-mdns)# rate-limit in 90
Device(config-mdns)# exit
```

Related Commands

Command	Description
service-routing mdns-sd	Enables mDNS gateway functionality for a device.
show mdns statistics	Displays mDNS statistics for the specified service-list.
show running-config mdns-sd policy	Displays current running mDNS service-policy configuration details for the device or interface.

rbe nasip

To specify the IP address of an interface on the DHCP relay agent that will be sent to the DHCP server via the agent remote ID option, use the **rbe nasip** command in global configuration mode. To remove the specification, use the **no** form of this command.

rbe nasip *interface-type number*
no rbe nasip

Syntax Description

interface-type	Interface type. For more information, use the question mark (?) online help function.
number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Default

No IP address is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.

Usage Guidelines

The **rbe nasip** command is used to configure support for the DHCP relay agent information option (option 82) for an ATM routed bridge encapsulation (RBE).

Support for the DHCP relay agent information option must be configured on the DHCP relay agent using the **ip dhcp relay information option** command for the **rbe nasip** command to be effective.

Examples

The following example shows how to enable support for DHCP option 82 on the DHCP relay agent by using the **ip dhcp relay information option** command. The **rbe nasip** command configures the router to forward the IP address for Loopback0 to the DHCP server. ATM RBE is configured on ATM subinterface 4/0.1.

```
ip dhcp-server 10.1.1.1
!
ip dhcp relay information option
!
interface Loopback0
 ip address 10.5.1.1 255.255.255.0
!
interface ATM 4/0
 no ip address
!
interface ATM 4/0.1 point-to-point
 ip unnumbered Loopback0
 ip helper-address 10.1.1.1
 atm route-bridged ip
```

```
 pvc 88/800
  encapsulation aal5snap
!
router eigrp 100
 network 10.0.0.0
!
rbe nasip loopback 0
```

Related Commands

Command	Description
ip dhcp relay information option	Enables the system to insert the DHCP relay agent information option in forwarded BOOT REQUEST messages to a Cisco IOS DHCP server.

redistribute mdns-sd

To speed up visibility of newly announced services and withdrawal of services when a service or device is turned off, use the **redistribute mdns-sd** command in interface multicast Domain Name System (mDNS) configuration mode. To stop service announcement information from being announced on other subnets, use the **no** form of this command.

Caution Redistribution of service announcements is only required in specific scenarios. Generally, services like printers or Apple TVs can be extended without any service announcement replication. However, it is a good practice to use the **withdraw-only** option. When you use this option, a service withdrawal announcement is sent to other devices when a service is removed, and the service is removed from the device's mDNS cache.

redistribute mdns-sd [**withdraw-only**]
no redistribute mdns-sd

Syntax Description

withdraw-only	(Optional) Enables redistribution of service withdrawal announcements. When you use the **withdraw-only** option, redistribution is only enabled for service withdrawal and not for the service. For example, if service withdrawal announcement for a printer service is enabled, there wont be any announcement about the availability of the printer service on other subnets. However, if the printer service is removed, withdrawal announcements will be sent to other devices which have learnt about the printer service earlier. **Note** If a service is removed, it will still be seen as available on each Service Discovery Gateway enabled device which has queried for this service earlier and stored in the respective mDNS cache. If you enable this keyword on the interface, an announcement will be forwarded to other devices and the service will be removed from each device's mDNS cache. As a result, users connected to other SDG-enabled devices will not see the withdrawn service as available. The **withdraw-only** option is not available for wireless devices.

Command Default

Redistribution of service announcement information is not enabled.

Command Modes

Interface mDNS configuration (config-if-mdns-sd)

Command History

Release	Modification
15.2(1)E	This command was introduced.
Cisco IOS XE 3.5E	This command was integrated into the Cisco IOS XE 3.5E release.
Cisco IOS XE Release 3.13S	This command was integrated into the Cisco IOS XE Release 3.13S
15.2(3)E	The **withdraw-only** keyword was added to enable redistribution of service withdrawal announcements across subnets.

Release	Modification
Cisco IOS XE 3.7E	The **withdraw-only** keyword was added to enable redistribution of service withdrawal announcements across subnets.
15.5(2)S	This command was integrated into Cisco IOS Release 15.5(2)S.
Cisco IOS XE Release 3.15S	This command was integrated into the Cisco IOS XE Release 3.15S

Usage Guidelines

Redistribution of service announcements can be enabled for an interface only and not for a device. You must ensure that there are no loops in the network topology corresponding to the interface for which service announcement redistribution is being enabled. A loop can lead to a broadcast storm.

Examples

The following example shows how to enable redistribution of service announcement information:

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 0/1
Device(config-if)# service-routing mdns-sd
Device(config-if-mdns-sd)# service-policy serv-pol1 IN
Device(config-if-mdns-sd)# redistribute mdns-sd
Device(config-if-mdns-sd)# exit
```

The following example shows how to enable service withdrawal notifications to other devices:

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 0/2
Device(config-if)# service-routing mdns-sd
Device(config-if-mdns-sd)# service-policy serv-pol3 IN
Device(config-if-mdns-sd)# redistribute mdns-sd withdraw-only
Device(config-if-mdns-sd)# exit
```

Related Commands

Command	Description
service-routing mdns-sd	Enables multicast Domain Name System (mDNS) gateway functionality for a device.
service-policy	Filters in-bound or out-bound service information for a service-list.

redundancy

To enter redundancy configuration mode, use the **redundancy**command in global configuration mode. This command does not have a **no** form.

redundancy

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)XV1	This command was introduced on the Cisco AS5800 universal access server.
12.2(4)XF	This command was introduced for the Cisco uBR10012 router.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.0(9)SL	This command was integrated into Cisco IOS Release 12.0(9)SL.
12.0(16)ST	This command was implemented on the Cisco 7500 series Internet routers.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	Support for this command was added for the Supervisor Engine 720.
12.2(18)S	This command was implemented on the Cisco 7500 series Internet routers.
12.2(20)S	This command was implemented on the Cisco 7304 router.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.3(7)T	This command was implemented on the Cisco 7500 series Internet routers.
12.2(8)MC2	This command was implemented on the MWR 1900 Mobile Wireless Edge Router (MWR).
12.3(11)T	This command was implemented on the MWR 1900 MWR.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
12.0(22)S	This command was implemented on the Cisco 10000 series Internet routers.
12.2(18)SXE2	This command was integrated into Cisco IOS Release 12.2(18)SXE2.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(44)SQ	This command was integrated into Cisco IOS Release 12.2(44)SQ. Support for the Cisco RF Gateway 10 was added.

Release	Modification
12.2(33) SRE	This command was modified. The interchassis subconfiguration mode was added.

Usage Guidelines

Use the **redundancy** command to enter redundancy configuration mode, where you can define aspects of redundancy such as shelf redundancy for the Cisco AS5800 universal access server.

Cisco 10000 Series Router

Before configuring line card redundancy, install the Y-cables. Before deconfiguring redundancy, remove the Y-cables.

The following restrictions apply to line card redundancy on the Cisco 10000 series router:

- Port-level redundancy is not supported.
- Redundant cards must occupy the two subslots within the same physical line card slot.
- The line card that will act as the primary line card must be the first line card configured, and it must occupy subslot 1.

Cisco 7600 Series Router

From redundancy configuration mode, you can enter the main CPU submode to manually synchronize the configurations that are used by the two supervisor engines.

From the main CPU submode, you can use the **auto-sync** command to use all the redundancy commands that are applicable to the main CPU.

To select the type of redundancy mode, use the **mode** command.

Nonstop forwarding (NSF) with stateful switchover (SSO) redundancy mode supports IPv4. NSF with SSO redundancy mode does not support IPv6, Internetwork Packet Exchange (IPX), and Multiprotocol Label Switching (MPLS).

After you enter redundancy configuration mode, you can use the **interchassis** command to specify the redundancy group number and enter interchassis redundancy mode. In the interchassis redundancy configuration mode, you can do the following:

- Specify a backbone interface for the redundancy group using the **backbone** command.
- Exit from interchassis configuration mode using the **exit** command.
- Specify the IP address of the remote redundancy group member using the **member ip** command.
- Specify the multichassis LACP (mLACP) node ID, system MAC address, and system priority using the **node-id**, **system-mac**, and **system-priority** commands.
- Define the peer monitoring method using the **monitor** command.

Cisco uBR10012 Universal Broadband Router

After you enter redundancy configuration mode, you can use the **main-cpu** command to enter main-CPU redundancy configuration mode, which allows you to specify which files are synchronized between the active and standby Performance Routing Engine (PRE) modules.

Cisco RF Gateway 10

At the redundancy configuration mode, you can do the following:

- Set a command to its default mode using the **default** command.
- Exit from a redundancy configuration using the **exit** command.
- Enter the line card group redundancy configuration using the **linecard-group** command.
- Enter main-CPU redundancy configuration mode using the **main-cpu** command, which allows you to specify which files are synchronized between the active and standby Supervisor cards.
- Configure the redundancy mode for the chassis using the **mode** command.
- Enforce a redundancy policy using the **policy** command.

Examples

The following example shows how to enable redundancy mode:

```
Router(config)# redundancy
Router(config-red)#
```

The following example shows how to assign the configured router shelf to the redundancy pair designated as 25. This command must be issued on both router shelves in the redundant router-shelf pair:

```
Router(config)# redundancy
Router(config-red)# failover group-number 25
```

Cisco 10000 Series Router

The following example shows how to configure two 4-port channelized T3 half eight line cards that are installed in line card slot 2 for one-to-one redundancy:

```
Router(config)# redundancy
Router(config-r)# linecard-group 1 y-cable
Router(config-r-lc)# member subslot 2/1 primary
Router(config-r-lc)# member subslot 2/0 secondary
```

Cisco 7600 Series Router

The following example shows how to enter the main CPU submode:

```
Router(config)#
redundancy
Router(config-r)#
main-cpu
Router(config-r-mc)#
```

Cisco uBR10012 Universal Broadband Router

The following example shows how to enter redundancy configuration mode and display the commands that are available in that mode on the Cisco uBR10012 router:

```
Router# configure terminal
```

```
Router(config)# redundancy

Router(config-r)# ?

Redundancy configuration commands:
  associate  Associate redundant slots
  exit       Exit from redundancy configuration mode
  main-cpu   Enter main-cpu mode
  no         Negate a command or set its defaults
```

The following example shows how to enter redundancy configuration mode and displays its associated commands on the Cisco RFGW-10 chassis:

```
Router# configure terminal
Router(config)# redundancy
Router(config-r)#?
Redundancy configuration commands:
  default         Set a command to its defaults
  exit            Exit from redundancy configuration mode
  linecard-group  Enter linecard redundancy submode
  main-cpu        Enter main-cpu mode
  mode            redundancy mode for this chassis
  no              Negate a command or set its defaults
  policy          redundancy policy enforcement
```

The following example shows how to enter redundancy configuration mode and its associated commands in the interchassis mode:

```
Router# configure terminal
Router(config)# redundancy
```

Router(config-r)#?

```
Redundancy configuration commands:
  exit          Exit from redundancy configuration mode
  interchassis  Enter interchassis mode
  no            Negate a command or set its defaults
Router(config-r)# interchassis group 100

R1(config-r-ic)# ?
Interchassis redundancy configuration commands:
  backbone  specify a backbone interface for the redundancy group
  exit      Exit from interchassis configuration mode
  member    specify a redundancy group member
  mlacp     mLACP interchassis redundancy group subcommands
  monitor   define the peer monitoring method
  no        Negate a command or set its defaults
```

Related Commands

Command	Description
associate slot	Logically associates slots for APS processor redundancy.
auto-sync	Enables automatic synchronization of the configuration files in NVRAM.
clear redundancy history	Clears the redundancy event history log.
linecard-group y-cable	Creates a line card group for one-to-one line card redundancy.

Command	Description
main-cpu	Enters main-CPU redundancy configuration mode for synchronization of the active and standby PRE modules or Supervisor cards.
member subslot	Configures the redundancy role of a line card.
mode (redundancy)	Configures the redundancy mode of operation.
redundancy force-switchover	Switches control of a router from the active RP to the standby RP.
show redundancy	Displays information about the current redundant configuration and recent changes in states or displays current or historical status and related information on planned or logged handovers. In the redundancy configuration of Cisco ASR 920 Series Routers, the commands related to MR-APS feature are only supported.

redundancy asymmetric-routing enable

To establish an asymmetric flow diversion tunnel for each redundancy group, use the **redundancy asymmetric-routing enable** command in interface configuration mode. To remove the established flow diversion tunnel, use the **no** form of this command.

redundancy asymmetric-routing enable
no redundancy asymmetric-routing enable

Syntax Description

This command has no arguments or keywords.

Command Default

An asymmetric routing traffic diversion tunnel is not configured for redundancy groups.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

You must configure this command on a traffic interface that sends or receives asymmetric routing traffic. A tunnel is established between the traffic interface and the asymmetric routing interface for each redundancy group.

Examples

The following example shows how to enable redundancy group asymmetric routing on a Gigabit Ethernet interface:

```
Router(config)# interface gigabitethernet 0/0/1
Router(config-if)# redundancy asymmetric-routing enable
```

Related Commands

Command	Description
asymmetric-routing	Sets up an asymmetric routing link interface and enables applications to divert packets received on the standby redundancy group to the active.
interface	Configures an interface and enters interface configuration mode.

redundancy group

To configure fault tolerance for the mobile router, use the **redundancy group** command in mobile router configuration mode. To disable this functionality, use the **no** form of this command.

redundancy group *name*
no redundancy group *name*

Syntax Description

name	Name of the mobile router group.

Command Default

No default behavior or values.

Command Modes

Mobile router configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

The **redundancy group** command provides f ault tolerance by selecting one mobile router in the redundancy group *name* argument to provide connectivity for the mobile networks. This mobile router is in the active state. The other mobile routers are passive and wait until the active mobile router fails before a new active mobile router is selected. Only the active mobile router registers and sets up proper routing for the mobile networks. The redundancy state is either active or passive.

Examples

The following example selects the mobile router in the sanjose group, to provide fault tolerance:

```
ip mobile router
 redundancy group sanjose
 address 10.1.1.10 255.255.255.0
 home-agent 10.1.1.20
 register lifetime 600
```

Related Commands

Command	Description
standby name	Configures the name of the standby group, which is associated with the mobile router.

redundancy group (interface)

To enable the redundancy group (RG) traffic interface configuration, use the **redundancy group** command in interface configuration mode. To remove the redundancy group traffic interface configuration, use the **no** form of this command.

redundancy group *id* {**ip** *virtual-ip* | **ipv6** {*link-local-address* | *ipv6-address*/*prefix-length*} | **autoconfig**} [**exclusive**] [**decrement** *value*]
no redundancy group *id* {**ip** | **ipv6** {*link-local-address* | *ipv6-address*/*prefix-length*}}

Syntax Description

id	Redundancy group ID. Valid values are from 1 and 2.
ip *virtual-ip*	Enables IPv4 RGs and sets a virtual IPv4 address.
ipv6	Enables IPv6 RGs.
link-local-address	Link local address.
ipv6-address/*prefix-length*	IPv6 address and the length of the IPv6 prefix. IPv6 prefix is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
autoconfig	Obtains IP addresses through autoconfiguration.
exclusive	(Optional) Specifies whether the interface is exclusive to an RG.
decrement *number*	(Optional) Specifies the number that is decremented from the priority when the state of an interface goes down. The configured decrement value overrides the default number that is configured for an RG. Valid values are from 1 to 255.

Command Default

Redundancy group traffic interface configuration is not enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.
Cisco IOS XE Release 3.7S	This command was modified. The *virtual-ip*, *link-local-address*, *ipv6-address*/*prefix-length* arguments and **ip**, **ipv6**, and **autoconfig** keywords were added.

Usage Guidelines

Use this command to configure a redundancy group for stateful switchover.

The virtual IP address and the physical address must be in the same subnet.

When autoconfiguration is enabled, the interface obtains an IP address automatically.

Examples

The following example shows how to enable the IPv6 redundancy group traffic interface configuration:

```
Device(config)# interface gigabitethernet 0/0/1
Device(config-if)# redundancy group 2 ipv6 FE80::260:3EFF:FE11:6770 exclusive
```

Related Commands

Command	Description
control	Configures the control interface type and number for a redundancy group.
data	Configures the data interface type and number for a redundancy group.
interface	Configures an interface and enters interface configuration mode.
name	Configures the name of a redundancy group.
preempt	Enables preemption on a redundancy group.
protocol	Defines a protocol instance in a redundancy group.
redundancy rii	Configures an RII for a redundancy group.

relay agent information

To enter relay agent information option configuration mode, use the **relay agent information**command in DHCP class configuration mode. To disable this functionality, use the **no** form of this command.

relay agent information
no relay agent information

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

DHCP class configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

If this command is omitted for Dynamic Host Configuration Protocol (DHCP) class-based address allocation, then the DHCP class matches to any relay agent information option, whether it is present or not.

Using the **no relay agent information** command removes all patterns in the DHCP class configured by the **relay-information hex** command.

Examples

The following example shows the relay information patterns configured for DHCP class 1.

```
ip dhcp class CLASS1
 relay agent information
  relay-information hex 01030a0b0c02050000000123
  relay-information hex 01030a0b0c02*
  relay-information hex 01030a0b0c02050000000000 bitmask 000000000000000000000000FF
ip dhcp class CLASS2
 relay agent information
```

Related Commands

Command	Description
relay-information hex	Specifies a hexadecimal string for the full relay agent information option.

relay destination

To configure an IP address for a relay destination to which packets are forwarded by a Dynamic Host Configuration Protocol (DHCP) relay agent functioning as a DHCP server, use the **relay destination** command in DHCP pool configuration mode. To disable the IP address, use the **no** form of this command.

relay destination [**vrf** *vrf-name* | **global**] *ip-address*
no relay destination [**vrf** *vrf-name* | **global**] *ip-address*

Syntax Description

vrf	(Optional) Virtual routing and forwarding (VRF) instance that is associated with the relay destination address. The *vrf-name* argument specifies the name of the VRF table.
global	(Optional) IP address selected from the global address space. If the pool does not have any VRF configuration, then the relay destination address defaults to the global address space.
ip-address	IPv4 address of the remote DHCP server to which the DHCP client packets are relayed.

Command Default

No destination IP address to which packets are forwarded is configured.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The **relay destination** command serves the same function as the **relay target**command, except that the **relay target** command specifies the DHCP server to which packets should be forwarded only for the class under which it is configured, and the **relay destination** command specifies the DHCP server to which packets should be forwarded for the pool itself. The **relay target** command overrides the **relay destination** command in cases in which the configured class name has been specified by the service gateway (SG).

When using the **relay destination** command, the *ip-address* argument is assumed to be in the same VRF as the address pool under which the command was configured. If the relay destination IP address is in a different VRF, or in the global address space, then the **vrf** *vrf-name* or **global** keywords need to be specified.

relay source

To configure an IP address for a relay source from which packets are forwarded by a Dynamic Host Configuration Protocol (DHCP) server, use the **relay source** command in DHCP-pool configuration mode. To disable the IP address, use the **no** form of this command.

relay source *ip-address subnet-mask*
no relay source *ip-address subnet-mask*

Syntax Description

ip-address	IPv4 address of DHCP server from which the DHCP client packets are relayed.
subnet-mask	Subnet mask that matches the subnet of the incoming interface of the DHCP client packet.

Command Default

No IP address from which IP packets are forwarded is configured.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Examples

The following example shows how to configure a source IP address from which DHCP client packets are relayed:

```
ip dhcp pool abc1
 relay source 10.0.0.0 255.255.0.0
 relay destination 10.5.1.1
```

Related Commands

Command	Description
relay destination	Configures an IP address for a relay destination to which packets are forwarded by a DHCP server.
relay target	Configures an IP address for a relay target to which packets are forward by a DHCP server.

relay target

To configure an IP address for a relay target to which packets are forwarded by a Dynamic Host Configuration Protocol (DHCP) server, use the **relay target**command in DHCP pool class configuration mode. To disable the IP address, use the **no** form of this command.

relay target [**vrf** *vrf-name* | **global**] *ip-address*
no relay target [**vrf** *vrf-name* | **global**] *ip-address*

Syntax Description

vrf	(Optional) Configured virtual routing and forwarding (VRF) that is associated with the relay destination address. The *vrf-name* argument specifies the name of the VRF table. **Note** If the **vrf** keyword is not specified, the target address is assumed to be in the same address space as the DHCP pool. If the **vrf** keyword is specified, the same VRF is assumed to apply here. However, if the target IP address is actually in the global address space, the **global** keyword should be specified.
global	(Optional) IP address selected from the global address space. If the pool does not have any VRF configuration, then the relay destination address defaults to the global address space.
ip-address	IPv4 address of the remote DHCP server to which the DHCP client packets are relayed.

Command Default

No target IP address is configured.

Command Modes

DHCP pool class configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The **relay target** command serves the same function as the **relay destination** command, except that the **relay target** command specifies the DHCP server to which packets should be forwarded only for the class under which it is configured, and the **relay destination** command specifies the DHCP server to which packets should be forwarded for the pool itself. The **relay target** command overrides the **relay destination** command in cases in which the configured class name has been specified by the SG.

Examples

The following example shows how to configure a relay target if a service gateway (SG)-supplied class name is used to select a DHCP server to which packets are relayed:

```
ip dhcp pool abc1
 relay source 10.0.0. 255.255.0.0.
 relay destination 10.5.1.1
 class classname1
  relay target 10.1.1.1
 class classname2
  relay target 10.2.2.2
 class classname3
```

In the above example, classname1 relays the DHCP DISCOVER packet to the server at 10.1.1.1, while classname2 relays the DHCP DISCOVER packet to the server at 10.2.2.2.

If the SG returned classname3, then the default pool at 10.5.1.1 is used. If the SG returns any other class name other than classname1, classname2, or classname3, then no relay action is taken.

The relay target configuration with respect to any configured DHCP pool works in the exact same way as a relay destination configuration works.

Related Commands

Command	Description
relay destination	Configures an IP address for a relay destination to which packets are forwarded by a DHCP server.
relay source	Configures an IP address for a relay source from which packets are forward by a DHCP server.

relay-information hex

To specify a hexadecimal string for the full relay agent information option, use the **relay-information hex** command in relay agent information option configuration mode. To remove the configuration, use the **no** form of this command.

relay-information hex *pattern* [*****] [**bitmask** *mask*]
no relay-information hex *pattern* [*****] [**bitmask** *mask*]

Syntax Description

pattern	String of hexadecimal values. This string creates a pattern that is matched against the named DHCP class.
*	(Optional) Wildcard character.
bitmask *mask*	(Optional) Hexadecimal bitmask.

Command Default

No default behavior or values

Command Modes

Relay agent information option configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

The **relay-information hex** command sets a pattern that is used to match against defined DHCP classes. You can configure multiple **relay-information hex** commands for a DHCP class. This is useful to specify a set of relay information options that can not be summarized with a wildcard or a bitmask.

The pattern itself, excluding the wildcard, must contain a whole number of bytes (a byte is two hexadecimal numbers). For example, 010203 is 3 bytes (accepted) and 01020 is 2.5 bytes (not accepted).

If you omit this command, no pattern is configured and it is considered a match to any relay agent information value, but the relay information option must be present in the DHCP packet.

You must know the hexadecimal value of each byte location in option 82 to be able to configure the **relay-information hex** command. The option 82 format may vary from product to product. Contact the relay agent vendor for this information.

Examples

The following example shows the configured relay agent information patterns. Note that CLASS 2 has no pattern configured and will “match to any” class.

```
ip dhcp class CLASS1
 relay agent information
  relay-information hex 01030a0b0c02050000000123
  relay-information hex 01030a0b0c02*
```

```
  relay-information hex 01030a0b0c02050000000000 bitmask 000000000000000000000000FF
ip dhcp class CLASS2
 relay agent information
```

release dhcp

To perform an immediate release of a Dynamic Host Configuration Protocol (DHCP) lease for an interface, use the **release dhcp** command in user EXEC or privileged EXEC mode.

release dhcp *interface-type interface-number*

Syntax Description

interface-type	Interface type. For more information, use the question mark (?) online help function.
interface-number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The **release dhcp** command immediately releases the DHCP lease on the interface specified by the *interface-type*and *interface-number*arguments. If the router interface was not assigned a DHCP IP address by the DHCP server, the **release dhcp** command fails and displays the following error message:

```
Interface does not have a DHCP originated address
```

This command does not have a **no** form.

Examples

The following example shows how to release a DHCP lease for an interface.

```
release dhcp ethernet 3/1
```

Related Commands

Command	Description
ip address dhcp	Specifies that the Ethernet interface acquires an IP address through DHCP.
lease	Configures the duration of the lease for an IP address that is assigned from a Cisco IOS DHCP server to a DHCP client.
renew dhcp	Forces the renewal of the DHCP lease for the specified interface.
show dhcp lease	Displays the DHCP addresses leased from a server.
show interface	Displays statistics for all interfaces configured on the router or access server.
show ip dhcp binding	Displays address bindings on the Cisco IOS DHCP server.
show ip interface	Displays a summary of an interface's IP information and status.

Command	Description
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific interface.
show startup-config	Displays the contents of the configuration file that will be used at the next system startup.

remote command

To execute a Cisco 7600 series router command directly on the switch console or a specified module without having to log into the Cisco 7600 series router first, use the **remote command** command in privileged EXEC mode.

remote command {**module** *num* | **standby-rp** | **switch**} *command*

Syntax Description

module *num*	Specifies the module to access; see the "Usage Guidelines" section for valid values.
standby-rp	Specifies the standby route processor.
switch	Specifies the active switch processor.
command	Command to be executed.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXD	The **standby-rp** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **module** *num* keyword and argument designate the module number. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values are from 1 to 13. The **module** *num* keyword and argument are supported on DFC-equipped modules and the standby supervisor engine only.

When you execute the **remote command switch** command, the prompt changes to Switch-sp#.

This command is supported on DFC-equipped modules and the supervisor engine only.

This command does not support command completion, but you can use shortened forms of the command (for example, entering **sh** for **show**).

Examples

This example shows how to execute the **show calendar** command from the standby route processor:

```
Router#
remote command standby-rp show calendar
Switch-sp#
09:52:50 UTC Mon Nov 12 2001
Router#
```

Related Commands

Command	Description
remote login	Accesses the Cisco 7600 series router console or a specific module.

remote login

To access the Cisco 7600 router console or a specific module, use the **remote login** command in privileged EXEC mode.

remote login {**module** *num* | **standby-rp** | **switch**}

Syntax Description

module *num*	Specifies the module to access; see the "Usage Guidelines" section for valid values.
standby-rp	Specifies the standby route processor.
switch	Specifies the active switch processor.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(140SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXD	This command was changed to include the **standby-rp** keyword.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines



Caution When you enter the **attach** or **remote login** command to access another console from your switch, if you enter global or interface configuration mode commands, the switch might reset.

The **module** *num* keyword and argument designate the module number. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values are from 1 to 13. The **module** *num* keyword and argument are supported on DFC-equipped modules and the standby supervisor engine only.

When you execute the **remote login module** *num* command, the prompt changes to Router-dfcx# or Switch-sp#, depending on the type of module to which you are connecting.

When you execute the **remote login standby-rp** command, the prompt changes to Router-sdby#.

When you execute the **remote login switch** command, the prompt changes to Switch-sp#.

The **remote login module** *num* command is identical to the **attach** command.

There are two ways to end the session:

- You can enter the **exit** command as follows:

```
Switch-sp# exit
[Connection to Switch closed by foreign host]
Router#
```

- You can press **Ctrl-C** three times as follows:

```
Switch-sp# ^C
Switch-sp# ^C
Switch-sp# ^C
Terminate remote login session? [confirm] y
[Connection to Switch closed by local host]
Router#
```

Examples

This example shows how to perform a remote login to a specific module:

```
Router# remote login module 1
Trying Switch ...
Entering CONSOLE for Switch
Type "^C^C^C" to end this session
Switch-sp#
```

This example shows how to perform a remote login to the Cisco 7600 series router processor:

```
Router# remote login switch
Trying Switch ...
Entering CONSOLE for Switch
Type "^C^C^C" to end this session
Switch-sp#
```

This example shows how to perform a remote login to the standby route processor:

```
Router# remote login standby-rp
Trying Switch ...
Entering CONSOLE for Switch
Type "^C^C^C" to end this session
Router-sdby#
```

Related Commands

Command	Description
attach	Connects to a specific module from a remote location.

remote-ip (IPC transport-SCTP remote)

To define at least one IP address of the redundant peer that is used to communicate with the local device, use the **remote-ip**command in IPC transport-SCTP remote configuration mode. To remove one or all IP addresses from your configuration, use the **no** form of this command.

remote-ip *peer-real-ip-address* [*peer-real-ip-address2*]
no remote-ip *peer-real-ip-address* [*peer-real-ip-address2*]

Syntax Description

peer-real-ip-address	IP address of the remote peer. The remote IP addresses must match the local IP addresses on the peer router. There can be either one or two IP addresses, which must be in the global Virtual Private Network (VPN) routing and forwarding (VRF). A virtual IP (VIP) address cannot be used.
peer-real-ip-address2	(Optional) IP address of the remote peer.

Command Default

No IP addresses are defined.

Command Modes

IPC transport-SCTP remote configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use the **remote-ip** command to help associate Stream Control Transmission Protocol (SCTP) as the transport protocol between the local and remote peer.

This command is part of a suite of commands used to configure the Stateful Switch Over (SSO) protocol. SSO is necessary for IP Security (IPSec) and Internet Key Exchange (IKE) to learn about the redundancy state of the network and to synchronize their internal application state with their redundant peers.

Examples

The following example shows how to enable SSO:

```
redundancy inter-device
 scheme standby HA-in
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 10.0.0.1
   remote-port 5000
    remote-ip 10.0.0.2
```

Related Commands

Command	Description
local-ip	Defines at least one local IP address that is used to communicate with the local peer.

Command	Description
remote-port	Defines the remote SCTP that is used to communicate with the redundant peer.

remote-port

To define the remote Stream Control Transmission Protocol (SCTP) port that is used to communicate with the redundant peer, use the **remote-port**command in SCTP protocol configuration mode.

remote-port *remote-port-number*

Syntax Description

remote-port-number	Remote port number, which should be the same as the local port number on the peer router (which is specified via the **local-port** command).

Command Default

A remote SCTP port is not defined.

Command Modes

SCTP protocol configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

The **remote-port** command enters IPC transport-SCTP remote configuration mode, which allows you to specify at least one remote IP address (via the **remote-ip** command) that is used to communicate with the redundant peer.

Examples

The following example shows how to enable Stateful Switchover (SSO):

```
redundancy inter-device
 scheme standby HA-in
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 10.0.0.1
   remote-port 5000
    remote-ip 10.0.0.2
```

Related Commands

Command	Description
local-port	Defines the local SCTP port that is used to communicate with the redundant peer.
remote-ip	Defines at least one IP address of the redundant peer that is used to communicate with the local device.

remote-span

To configure a virtual local area network (VLAN) as a remote switched port analyzer (RSPAN) VLAN, use the **remote-span** command in config-VLAN mode. To remove the RSPAN designation, use the **no** form of this command.

remote-span
no remote-span

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Config-VLAN mode

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported in the VLAN database mode.

You can enter the **show vlan remote-span** command to display the RSPAN VLANs in the Cisco 7600 series router.

Examples

This example shows how to configure a VLAN as an RSPAN VLAN:

```
Router(config-vlan)# remote-span
Router(config-vlan)
```

This example shows how to remove the RSPAN designation:

```
Router(config-vlan)# no remote-span
Router(config-vlan)
```

Related Commands

Connect	Description
show vlan remote-span	Displays a list of RSPAN VLANs.

renew deny unknown

To configure the renewal policy for unknown DHCP clients, use the **renew deny unknown**command in DHCP pool configuration mode. To disable the renewal policy, use the no form of this command.

renew deny unknown
no renew deny unknown

Syntax Description

This command has no arguments or keywords.

Command Default

The DHCP server ignores a client request for an IP address that is not leased to the client.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.2 SXH	This command was integrated into Cisco IOS Release 12.2SXH

Usage Guidelines

In some usage scenarios, such as a wireless hotspot, where both DHCP and secure ARP are configured, a connected client device might go to sleep or suspend for a period of time. If the suspended time period is greater than the secure ARP timeout (default of 91 seconds), but less than the DHCP lease time, the client can awake with a valid lease, but the secure ARP timeout has caused the lease binding to be removed because the client has been inactive. When the client awakes, the client still has a lease on the client side but is blocked from sending traffic. The client will try to renew its IP address but the DHCP server will ignore the request because the DHCP server has no lease for the client. The client must wait for the lease to expire before being able to recover and send traffic again.

To remedy this situation, use the **renew deny unknown** command in DHCP pool configuration mode. This command forces the DHCP server to reject renewal requests from clients if the requested address is present at the server but is not leased. The DHCP server sends a DHCPNAK denial message to the client, which forces the client back to its initial state. The client can then negotiate for a new lease immediately, instead of waiting for its old lease to expire.

Examples

The following example shows how to secure ARP table entries to DHCP leases. The **renew deny unknown** command allows the DHCP server to renew the lease of a DHCP client whose lease has been cleared because of a secure ARP timeout.

```
Router# configure
 terminal

Router(config)# ip dhcp pool red
Router(dhcp-config)# update arp
Router(dhcp-config)# renew deny unknown
```

Related Commands

Command	Description
update arp	Secures dynamic ARP entries in the ARP table to their corresponding DHCP bindings.

renew dhcp

To perform an immediate renewal of a Dynamic Host Configuration Protocol (DHCP) lease for an interface, use the **renew dhcp** command in user EXEC or privileged EXEC mode.

renew dhcp *interface-type interface-number*

Syntax Description

interface-type	Interface type. For more information, use the question mark (?) online help function.
interface-number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The **renew dhcp** command immediately renews the DHCP lease for the interface specified by the *interface-type* and *interface-number* arguments. If the router interface was not assigned an IP address by the DHCP server, the **renew dhcp** command fails and displays the following error message:

```
Interface does not have a DHCP originated address
```

This command does not have a **no** form.

Examples

The following example shows how to renew a DHCP lease for an interface:

```
renew dhcp Ethernet 3/1
```

Related Commands

Command	Description
ip address dhcp	Specifies that the Ethernet interface acquires an IP address through DHCP.
lease	Configures the duration of the lease for an IP address that is assigned from a Cisco IOS DHCP server to a DHCP client.
release dhcp	Releases the DHCP lease on the specified interface.
show dhcp lease	Displays the DHCP addresses leased from a server.
show interface	Displays statistics for all interfaces configured on the router or access server.
show ip dhcp binding	Displays address bindings on the Cisco IOS DHCP server.
show ip interface	Displays a summary of an interface's IP information and status.

Command	Description
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific interface.
show startup-config	Displays the contents of the configuration file that will be used at the next system startup.



reserved-only through show ip irdp

- reserved-only, on page 673
- restrict authenticated, on page 674
- restrict name-group, on page 676
- restrict source access-group, on page 678
- service dhcp, on page 680
- service-instance mdns-sd, on page 682
- service-list mdns-sd, on page 684
- service-policy, on page 686
- service-policy-proximity, on page 687
- service-policy-query, on page 689
- service-policy-query (interface), on page 690
- service-routing mdns-sd, on page 692
- service-type-enumeration period, on page 694
- set ip next-hop dynamic dhcp, on page 695
- set platform software trace forwarding-manager alg, on page 696
- show alg sip, on page 698
- show arp, on page 700
- show arp application, on page 705
- show arp ha, on page 708
- show arp summary, on page 712
- show auto-ip-ring, on page 715
- show hosts, on page 718
- show ip aliases, on page 721
- show ip arp, on page 723
- show ip arp inspection, on page 725
- show ip arp inspection log, on page 728
- show ip arp poll, on page 729
- show ip ddns update, on page 730
- show ip ddns update method, on page 731
- show ip dhcp binding, on page 732
- show ip dhcp conflict, on page 735
- show ip dhcp database, on page 737
- show ip dhcp import, on page 739

- show ip dhcp limit lease, on page 740
- show ip dhcp pool, on page 741
- show ip dhcp relay information trusted-sources, on page 743
- show ip dhcp server statistics, on page 744
- show ip dhcp snooping, on page 746
- show ip dhcp snooping binding, on page 748
- show ip dhcp snooping database, on page 751
- show ip dhcp vrf, on page 753
- show ip dns name-list, on page 755
- show ip dns primary, on page 757
- show ip dns statistics, on page 759
- show ip dns view, on page 761
- show ip dns view-list, on page 764
- show ip host-list, on page 766
- show ip interface, on page 768
- show ip interface unnumbered, on page 777
- show ip irdp, on page 779

reserved-only

To restrict address assignments from the Dynamic Host Configuration Protocol (DHCP) address pool only to the preconfigured reservations, use the **reserved-only** command in DHCP pool configuration mode. To disable the configuration, use the **no** form of this command.

reserved-only
no reserved-only

Syntax Description

This command has no arguments or keywords.

Command Default

Address assignments from the DHCP address pool are not restricted only to the preconfigured reservations.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

Release	Modification
12.2(50)SE	This command was introduced.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

When the DHCP port-based assignment feature is configured on multiple switches, devices connected to one switch may receive an IP address assignment from the neighboring switches rather than from the local DHCP address pool switch. If you want the switch to serve only the client directly connected to the switch, you can configure a group of switches with pools that share a common IP subnet but ignore the requests from other clients (not connected to this switch).

Examples

The following example shows how to restrict address assignments from the DHCP address pool only to the preconfigured reservations:

```
Router# configure terminal
Router(config)# ip dhcp pool red
Router(dhcp-config)# reserved-only
```

Related Commands

Command	Description
address client-id	Reserves an IP address for a DHCP client identified by client identifier.
address hardware-address	Reserves an IP address for a client identified by hardware address.

restrict authenticated

To specify that a Domain Name System (DNS) view list member cannot be used to respond to an incoming DNS query if the DNS view and the DNS client have not been authenticated, use the **restrict authenticated** command in DNS view list member configuration mode. To remove this restriction from a DNS view list member, use the **no** form of this command.

restrict authenticated
no restrict authenticated

Syntax Description

This command has no arguments or keywords.

Command Default

When determining whether the DNS view list member can be used to respond to an incoming DNS query, the Cisco IOS software does not check that the DNS view and the DNS client have been authenticated.

Command Modes

DNS view list member configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command restricts the DNS view list member from responding to an incoming DNS query unless the Cisco IOS software has verified the authentication status of the client. The view list member is rejected, and the view-selection process proceeds to the next view in the view list, if the client is not authenticated. The router that is running Split DNS determines the query client authentication status by calling any DNS client authentication functions that have been registered with Split DNS.

A client can be authenticated within a Cisco IOS environment by various methods, such as Firewall Authentication Proxy, 802.1x, and wireless authentication. Some DNS authentication functions might inspect only the source IP address or MAC address and the VRF information, while other functions might inspect the source IP address or MAC address, the VRF information, and the DNS view name.

Note In Cisco IOS Release 12.4(9)T, none of these authentication methods are implemented by any Cisco IOS authentication subsystems. As a result, if a DNS view is configured to be restricted based on client authentication, the Cisco IOS software will not use that view whenever the view is considered for handling a query. In future Cisco IOS releases, authentication subsystems will implement client authentication functions and enable them to be registered on a router running Split DNS. This will enable the Cisco IOS software to support authentication-based use restrictions on DNS views. This command is provided now for backward compatibility when DNS authentication functions are implemented.

A DNS view list member can also be restricted from responding to an incoming DNS query based on the query source IP address (configured by using the **restrict source access-group** command) or the query hostname (configured by using the **restrict name-group** command).

Note If a DNS view list member is configured with multiple usage restrictions, that DNS view can be used to respond to a DNS query only if the view is associated with the source VRF of the query and all configured usage restrictions are met by the query.

To display the usage restrictions for a DNS view list member, use the **show ip dns view-list** command.

Examples

The following example shows how to create the DNS view list userlist5 so that it contains the two DNS views:

```
Router(config)# ip dns view-list userlist5

Router(cfg-dns-view-list)# view vrf vpn101 user1 20

Router(cfg-dns-view-list-member)# exit

Router(cfg-dns-view-list)# view vrf vpn201 user2 35

Router(cfg-dns-view-list-member)# restrict authenticated
```

Both view list members are restricted from responding to an incoming DNS query unless the query is from the same VRF as the VRF with which the view is associated.

The first view list member (the view named user1 and associated with the VRF vpn101) has no further restrictions placed on its use.

The second view list member (the view named user2 and associated with the VRF vpn201) is further restricted from responding to an incoming DNS query unless the Cisco IOS software can verify the authentication status of the client.

Related Commands

Command	Description
restrict name-group	Restricts the use of the DNS view list member to DNS queries for which the query hostname matches a particular DNS name list.
restrict source access-group	Restricts the use of the DNS view list member to DNS queries for which the query source IP address matches a particular standard ACL.
show ip dns view-list	Displays information about a particular DNS view list or about all configured DNS view lists.

restrict name-group

To specify that a Domain Name System (DNS) view list member cannot be used to respond to a DNS query unless the query hostname matches a permit clause in a particular DNS name list and none of the deny clauses, use the **restrict name-group** command in DNS view list member configuration mode. To remove this restriction from a DNS view list member, use the **no** form of this command.

restrict name-group *name-list-number*
no restrict name-group *name-list-number*

Syntax Description

name-list-number	Integer from 1 to 500 that identifies an existing DNS name list.

Command Default

When determining whether the DNS view list member can be used to respond to an incoming DNS query, the Cisco IOS software does not check that the query hostname matches a permit clause in a particular DNS name list.

Command Modes

DNS view list member configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command restricts the DNS view list member from responding to an incoming DNS query if a permit clause in the specified DNS name list specifies a regular expression that matches the query hostname. The view list member is rejected, and the view-selection process proceeds to the next view in the view list, if an explicit deny clause in the name list (or the implicit deny clause at the end of the name list) matches the query hostname. To configure a DNS name list, use the **ip dns name-list** command.

A DNS view list member can also be restricted from responding to an incoming DNS query based on the source IP address of the incoming DNS query. To configure this type of restriction, use the **restrict source access-group** command.

Note If a DNS view list member is configured with multiple usage restrictions, that DNS view can be used to respond to a DNS query only if the view is associated with the source VRF of the query and all configured usage restrictions are met by the query.

To display the usage restrictions for a DNS view list member, use the **show ip dns view-list** command.

Note The *name-list-number* argument referenced in this command is configured using the **ip dns name-list** command. The DNS name list is referred to as a "name list" when it is defined and as a "name group" when it is referenced in other commands.

Examples

The following example shows how to specify that DNS view user3 associated with the global VRF, when used as a member of the DNS view list userlist5, cannot be used to respond to an incoming DNS query unless the query hostname matches the DNS name list identified by the number 1:

```
Router(config)# ip dns view-list userlist5

Router(cfg-dns-view-list)# view user3 40
Router(cfg-dns-view-list-member)# restrict name-group 1
```

Related Commands

Command	Description
ip dns name-list	Defines a list of pattern-matching rules in which each rule permits or denies the use of a DNS view list member to handle a DNS query based on whether the query hostname matches the specified regular expression.
restrict source access-group	Restricts the use of the DNS view list member to DNS queries for which the query source IP address matches a particular standard ACL.
show ip dns view-list	Displays information about a particular DNS view list or about all configured DNS view lists.

restrict source access-group

To specify that a Domain Name System (DNS) view list member cannot be used to respond to a DNS query unless the source IP address of the DNS query matches a standard access control list (ACL), use the **restrict source access-group** command in DNS view list member configuration mode. To remove this restriction from a DNS view list member, use the **no** form of this command.

restrict source access-group {*acl-nameacl-number*}
no restrict source access-group {*acl-nameacl-number*}

Syntax Description

acl-name	String (not to exceed 64 characters) that specifies a standard ACL.
acl-number	Integer from 1 to 99 that specifies a standard ACL.

Command Default

When determining whether the DNS view list member can be used to respond to an incoming DNS query, the Cisco IOS software does not check that the source IP address of the DNS query belongs to a particular standard ACL.

Command Modes

DNS view list member configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command restricts the DNS view list member from responding to an incoming DNS query if the query source IP address matches the specified standard ACL. To configure a standard ACL, use the **access-list** (IP standard) command.

A DNS view list member can also be restricted from responding to an incoming DNS query based on the the query hostname. To configure this type of restriction, use the **restrict name-group** command.

Note If a DNS view list member is configured with multiple usage restrictions, that DNS view can be used to respond to a DNS query only if the view is associated with the source Virtual Private Network (VPN) routing and forwarding (VRF) instance of the query and all configured usage restrictions are met by the query.

To display the usage restrictions for a DNS view list member, use the **show ip dns view-list** command.

Note The *acl-name* or *acl-number* argument referenced in this command is configured using the **access-list** command. The access list is referred to as a "access list" when it is defined and as a "access group" when it is referenced in other commands.

Examples

The following example shows how to specify that DNS view user4 associated with the global VRF, when used as a member of the DNS view list userlist7, cannot be used to respond to an incoming DNS query unless the query source IP address matches the standard ACL number 6:

```
Router(config)# ip dns view-list userlist7

Router(cfg-dns-view-list)# view user4 40
Router(cfg-dns-view-list-member)# restrict source access-group 6
```

Related Commands

Command	Description
access-list (IP standard)	Creates a standard ACL that defines the specific host or subnet for host-specific PAM.
restrict name-group	Restricts the use of the DNS view list member to DNS queries for which the query hostname matches a particular DNS name list.
show ip dns view-list	Displays information about a particular DNS view list or about all configured DNS view lists.

service dhcp

To enable the Dynamic Host Configuration Protocol (DHCP) server and relay agent features on your router, use the **service dhcp** command in global configuration mode. To disable the DHCP server and relay agent features, use the no form of this command.

service dhcp
no service dhcp

Syntax Description

This command has no arguments or keywords.

Command Default

DHCP is enabled. DHCP is not running. Port 67 is closed.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4	This command was modified. Port 67 is closed in the Cisco IOS DHCP/BOOTP default configuration. This command was broken into two logical parts: service enabled and service running.
12.2SXH	This command was modified. Port 67 is closed in the Cisco IOS DHCP/BOOTP default configuration. This command was broken into two logical parts: service enabled and service running.

Usage Guidelines

The BOOTP and DHCP servers in Cisco IOS software both use the Internet Control Message Protocol (ICMP) port (port 67) by default. ICMP “port unreachable messages” will only be returned to the sender if both the BOOTP server and DHCP server are disabled. Disabling only one of the servers will not result in ICMP port unreachable messages.

Port 67 is closed in the Cisco IOS DHCP/BOOTP default configuration. There are two logical parts to the **service dhcp** command: service enabled and service running. The DHCP service is enabled by default, but port 67 is not opened until the DHCP service is running. A DHCP address pool must be configured for the DHCP service to be running. If the service is running, the s**how ip sockets detail or show sockets detail**commands displays port 67 as open.

Examples

The following example shows to enable DHCP services on the DHCP server:

```
service dhcp
```

Related Commands

Command	Description
show ip sockets	Displays IP socket information.
show sockets	Displays IP socket information.

service-instance mdns-sd

To create an instance of a specific service type, use the **service-instance mdns-sd** command in global configuration mode. To remove the service-instance, use the **no** form of this command.

service-instance mdns-sd service *instance-name* **regtype** *service-type* **domain** *name*
no service-instance mdns-sd service *instance-name* **regtype** *service-type* **domain** *name*

Syntax Description

service *instance-name*	Specifies the service instance name.
regtype *service-type*	Specifies that the service instance is of the specified service type.
domain *name*	Specifies the domain with which the service-instance is being associated.

Command Default

Service instances need to be created, and are not available by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)E	This command was introduced.
Cisco IOS XE 3.6E	This command was integrated into the Cisco IOS XE 3.6E release.
15.2(1)SY	This command was integrated into Cisco IOS Release 15.2(1)SY.
15.5(2)S	This command was integrated into Cisco IOS Release 15.5(2)S.
Cisco IOS XE Release 3.15S	This command was integrated into the Cisco IOS XE Release 3.15S

Usage Guidelines

When you create a new service instance, the command enters multicast Domain Name System (mDNS) service discovery service-instance (config-mdns-sd-si) mode . In this mode, you can configure various parameters for the service instance. The options in this mode are given below:

- **ipv4addr** *ipv4-address* or **ipv6addr** *ipv6-address* - Specifies the IP address of the port on which the service is available.



Note You must specify an IPv4 or IPv6 address.

- **port** *number* - Specifies the port on which the service is available.
- (Optional). **priority** *value* - Specifies the priority. The default priority value is zero.
- **target-hostname** *host-name* - Specifies the fully qualified domain name (FQDN) of the target host.
- **txt** - Text record for the service. To associate more than one text record, separate each record by a semi-colon.
- (Optional). **weight** *value* - Specifies the weight for the service instance. The default weight value is zero.

Examples

The following example shows you how to create a service instance and configure parameters for the service instance:

```
Device> enable
Device# configure terminal
Device(config)# service-instance mdns-sd service serv-inst3 regtype _airplay._tcp domain
tcp4
Device(config-mdns-sd-si)# ipv4addr 209.165.200.230 255.255.255.224
Device(config-mdns-sd-si)# port 65
Device(config-mdns-sd-si)# target-hostname domainv6
Device(config-mdns-sd-si)# exit
```

Related Commands

Command	Description
service-routing mdns-sd	Enables mDNS gateway functionality for a device.
show mdns statistics	Displays mDNS statistics for the specified service-list.
show running-config mdns-sd service-instance	Displays current running mDNS service-instance configuration details for the device or interface.

service-list mdns-sd

To create a service-list and apply a filter on the service-list or associate a query for the service-list, use the **service-list mdns-sd** command in global configuration mode. To remove a service-list or service-list filter, or to disassociate a query for a service-list, use the **no** form of this command.

service-list mdns-sd *service-list-name* {**deny** *sequence-number* | **permit** *sequence-number* | **query**}
no service-list mdns-sd *service-list-name* [**deny** *sequence-number* | **permit** *sequence-number* | **query**]

Syntax Description

service-list-name	Service-list name. The permit, deny, and query options are applicable for the created service-list.
deny *sequence-number*	Restricts service information from being shared on a specific device, for the specified sequence number.
permit *sequence-number*	Allows service information to be shared on a specific device, for the specified sequence number.
query	Associates a query for the service-list name.

Command Default

Service-list information is not shared between devices or interfaces.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(1)E	This command was introduced.

Usage Guidelines

While creating a service-list, the permit or deny option must to be used. The permit option allows you to permit/transport specific service-list information. The deny option allows you to deny service-list information that is available to be transported to other subnets.

You need to mention a sequence number when using the permit or deny option. The same service-list name can be associated with multiple sequence numbers and each sequence number will be mapped to a rule.

Query is another option provided while creating service-lists. You can create queries using a service-list. If you want to browse for a service, then active queries can be used. This will be helpful to keep the records refreshed in the cache.

Examples

The following example shows creation of a service-list sl1. The permit option is being applied on sequence number 3:

```
Device> enable
Device# configure terminal
Device(config)# service-list mdns-sd sl1 permit 3
Device(config-mdns-sd-sl)# exit
```

Related Commands

Command	Description
match service-instance	Configures parameters for a service-list, for a specified service instance.
show mdns statistics	Displays multicast Domain Name System (mDNS) statistics for the specified service-list.

service-policy

To filter in-bound or out-bound service information for a service-list, use the **service-policy** command in the multicast DNS (mDNS) configuration or interface mDNS configuration mode. To remove a service-policy or service-list filter, or to disassociate a query for a service-list, use the **no** form of this command.

service-policy *service-policy-name* {**IN** | **OUT**}
no service-policy *service-policy-name* {**IN** | **OUT**}

Syntax Description

service-policy-name	Service-list name.
IN	Filters incoming service information for a device or interface according to the service policy.
OUT	Filters outgoing service information for a device or interface according to the service policy.

Command Default

Service information is not transported between two devices or interfaces.

Command Modes

Multicast DNS configuration (config-mdns)

Interface multicast DNS configuration (config-if-mdns)

Command History

Release	Modification
15.2(1)E	This command was introduced.

Usage Guidelines

The main purpose of creating a service-policy is to apply it at the interface level rather than at a global level.

Examples

The following example shows the application of a service-policy for an interface:

```
Device> enable
Device# configure terminal
Device(config)# service-routing mdns-sd
Device(config-mdns)# interface ethernet 0/1
Device(config-if-mdns)# service-policy serv-pol2 IN
Device(config-if-mdns)# exit
```

Related Commands

Command	Description
service-routing mdns-sd	Enables mDNS gateway functionality for a device.
show mdns statistics	Displays mDNS statistics for the specified service-list.

service-policy-proximity

To configure service policy proximity filtering on a wireless device or interface, use the **service-policy-proximity** command in multicast Domain Name System (mDNS) configuration mode or in interface mDNS configuration mode. To disable service policy proximity filtering on a wireless device or interface, use the **no** form of this command.

service-policy-proximity *service-list-name* [**limit** *number-of-services*]
no service-policy-proximity

Syntax Description

service-list-name	Service-list. Specifies that the services in the service-list are available in close proximity to the requester, and will be offered to the user when queried for.
limit *number-of-services*	(Optional) Specifies the maximum number of services that can be returned. The default value for the maximum number of services that can be returned is 50.

Command Default

Service policy proximity filtering is disabled.

Command Modes

Multicast DNS configuration (config-mdns)

Interface mDNS configuration (config-if-mdns-sd)

Command History

Release	Modification
15.2(2)E	This command was introduced.
Cisco IOS XE 3.6E	This command was integrated into the Cisco IOS XE 3.6E release.
Cisco IOS XE Release 3.13S	This command was integrated into the Cisco IOS XE Release 3.13S
15.2(1)SY	This command was integrated into Cisco IOS Release 15.2(1)SY.
15.5(2)S	This command was integrated into Cisco IOS Release 15.5(2)S.
Cisco IOS XE Release 3.15S	This command was integrated into the Cisco IOS XE Release 3.15S

Usage Guidelines

Service policy proximity filtering functionality is only available on wireless devices and their interfaces.

If service policy proximity filtering is configured on a device or interface, outbound service information is filtered first and then services in proximity are filtered and only the services in proximity are offered to the user.

Proximity based filtering applies to response filtering and not to redistribution or queries.

For example, consider this scenario. In a network, AirPlay and printer services are available, and are part of the mDNS cache. The AirPlay service is defined in the proximity group of the requesting client whereas the printer service is not. When the requesting client or device in the network queries for the AirPlay service, the out-going filter will filter all available Airplay and printer services in the mDNS cache first, and then filter Airplay services in the proximity. Only the Airplay services in the proximity are returned to the user. If the client requests printer services, all printer services in the mDNS cache are returned.

Examples

The following example shows you how to configure service policy proximity filtering on a wireless device:

```
Device> enable
Device# configure terminal
Device(config)# interface Vlan136
Device(config-if)# service-routing mdns-sd
Device(config-if-mdns-sd)# service-policy-proximity permit-airplay limit 10
Device(config-if-mdns-sd)# exit
```

Related Commands

Command	Description
service-routing mdns-sd	Enables mDNS gateway functionality for a device.
show mdns statistics	Displays mDNS statistics for the specified service-list.
show running-config mdns-sd policy	Displays current running mDNS service-policy configuration details for the device or interface.

service-policy-query

To configure an active query and active query period, use the **service-policy-query** command in multicast Domain Name System (mDNS) configuration mode. To disable an active query, use the **no** form of this command.

service-policy-query *service-list-name query-period*
no service-policy-query *service-list-name query-period*

Syntax Description

service-list-name	Service-list name; services in the specified service-list are queried according to the period specified in the *service-list-query-period* argument.
query-period	Service-list query period, in seconds.

Command Default

An active query is not configured for browsing services.

Command Modes

Multicast DNS configuration (config-mdns)

Command History

Release	Modification
15.2(1)E	This command was introduced.

Usage Guidelines

An active query enables browsing of services specified within the query. The **service-policy-query** command can only be used for enabling browsing of services periodically. Before configuring an active query for browsing services, you must create an active query and specify services within it. To create an active query, use the command **service-list mdns-sd**.

Examples

The following example shows creation of an active query and active query period:

```
Device> enable
Device# configure terminal
Device(config)# service-routing mdns-sd
Device(config-mdns)# service-policy-query sl4 100
Device(config-mdns)# exit
```



Note In the above example, **sl4** is the active query. If printer services are specified within the query, then the printer services connected to the device are browsed every 100 seconds and stored in cache.

Related Commands

Command	Description
service-routing mdns-sd	Enables mDNS gateway functionality for a device.
show running-config mdns-sd policy	Displays current running mDNS service-policy configuration details for the device or interface.

service-policy-query (interface)

To configure periodic browsing of services on an interface or to stop browsing of services on an interface, use the **service-policy-query (interface)** command in interface multicast Domain Name System (mDNS) configuration mode. To disable periodic browsing of services on an interface, use the **no** form of this command.

service-policy-query {*service-list-name* *query-period* | **disable**}
no service-policy-query

Syntax Description

service-list-name	Service-list name; services in the specified service-list are browsed periodically on the interface.
query-period	Service-list query period, in seconds.
disable	Disables browsing of specified services on the interface. **Note** There is a difference between the **no** form of this command and the **disable** option. • **no** form - If you have enabled browsing of printer services for a specific interface which has a printer connected, and if the printer is removed from the interface, then you can use the **no** form to stop browsing printer services on the interface. • **disable** option - If you have enabled browsing for specific services, such as printer services, on the device (globally configured), then printer services are periodically searched for on all the interfaces of the device. If there is an interface where there is no printer service available, you can use the **disable** option to disable browsing of printer services only for the interface.

Command Default

An active query for browsing services on an interface does not exist by default.

Command Modes

Interface mDNS configuration (config-if-mdns-sd)

Command History

Release	Modification
15.2(3)E	This command was introduced.
Cisco IOS XE 3.7E	This command was integrated into the Cisco IOS XE 3.7E release.
15.5(2)S	This command was integrated into Cisco IOS Release 15.5(2)S.
Cisco IOS XE Release 3.15S	This command was integrated into the Cisco IOS XE Release 3.15S.

Usage Guidelines



Remember You must first create an active query and specify services within it, using the **service-list mdns-sd** command. Only then can you enable periodic browsing of those services on the interface, using the **service-policy-query (interface)** command.

The **disable** option can only be used for interfaces. If you have enabled browsing of certain types of service globally, you can stop those services from being browsed on some interfaces by using this option. For example, if an active query is created for browsing printer services and applied globally, then all interfaces on the device will browse printer services periodically. If some interfaces don't have printer services, then you can disable browsing of printer services on those interfaces.

Examples

The following example shows how to enable browsing of printer services on an interface :

```
Device> enable
Device# configure terminal
Device# interface ethernet0/1
Device(config-if)# service-routing mdns-sd
Device(config-if-mdns-sd)# service-policy-query AQ-int 1000
Device(config-if-mdns-sd)# exit
Device(config-if)#
```



Note In the above example, **AQ-int** is the service-list that contains printer services. Printer services connected to the interface are browsed every 1000 seconds and stored in cache.

Related Commands

Command	Description
service-policy-query	Configures periodic browsing of services for a device.
service-routing mdns-sd	Enables mDNS gateway functionality for a device.
show running-config mdns-sd policy	Displays current running mDNS service-policy configuration details for the device or interface.

service-routing mdns-sd

To enable multicast Domain Name System (mDNS) gateway functionality for a device or interface, use the **service-routing mdns-sd** command in global or interface configuration mode. To disable mDNS gateway functionality for a device or interface, use the **no** form of this command.

service-routing mdns-sd
no service-routing mdns-sd

Syntax Description

This command has no arguments or keywords.

Command Default

The mDNS gateway functionality is disabled for a device or interface.

Command Modes

Global configuration (config)

Interface configuration (config-if)

Command History

Release	Modification
15.2(1)E	This command was introduced.
15.2(1)SY	This command was integrated into Cisco IOS Release 15.2(1)SY.
15.5(2)S	This command was integrated into Cisco IOS Release 15.5(2)S.

Usage Guidelines

The **service-routing mdns-sd** command enables you to enter multicast DNS configuration (config-mdns) mode. In this mode, you can apply in-bound and out-bound filters (using the **service-policy** command) and use active queries. When you enable mDNS gateway functionality for an interface, the command enters multicast DNS interface configuration (config-if-mdns-sd) mode.

You can use the following options in the mDNS configuration (config-mdns) mode and the mDNS interface configuration (config-if-mdns-sd) mode:

Purpose	Use this Command **Note** The complete syntax is provided in the corresponding command page.	Global and Interface Configuration Options
For a service-list, apply a filter on incoming service discovery information or outgoing service discovery information.	**service-policy**	Global and interface levels.
Set some part of the system memory for cache.	**cache-memory-max**	Global level.

Configure an active query and active query period. **Note** Service-lists of the type **query** can be used to browse services. Such queries are called active queries	**service-policy-query**	Global level.
Designate a specific device or interface in a domain for routing mDNS announcement and query information.	**designated-gateway**	Global and interface levels.
Configure service policy proximity filtering on the device.	**service-policy-proximity**	Global and interface levels.
Configure service-type enumeration period for the device.	**service-type-enumeration period**	Global level.
Specify an alternate source interface for outgoing mDNS packets on a device.	**source-interface**	Global level.
Configure the maximum rate limit of incoming mDNS packets for a device.	**rate-limit**	Global level.
Speeds up visibility of newly announced services and withdrawal of services when a service or device is turned off.	**redistribute**	Interface level.

Examples

The following example shows how to enable the mDNS gateway for a device and apply a service policy:

```
Device> enable
Device# configure terminal
Device(config)# service-routing mdns-sd
Device(config-mdns)# service-policy serv-pol1 IN
Device(config-mdns)# exit
```

Related Commands

Command	Description
service-policy	Applies a filter on incoming or outgoing service information for a service-list.
service-policy-query	Configures the service-list-query period.

service-type-enumeration period

To configure a service-type enumeration period, use the **service-type-enumeration period** command in multicast Domain Name System (mDNS) configuration mode. To disable service-type enumeration period, use the **no** form of this command.

service-type-enumeration period *period-value*
no service-type-enumeration period *period-value*

Syntax Description

period-value	Service-type enumeration period, in minutes.

Command Default

Service-type enumeration period is not configured.

Command Modes

Multicast DNS configuration (config-mdns)

Command History

Release	Modification
15.2(2)E	This command was introduced.
Cisco IOS XE 3.6E	This command was integrated into the Cisco IOS XE 3.6E release.
15.2(1)SY	This command was integrated into Cisco IOS Release 15.2(1)SY.
15.5(2)S	This command was integrated into Cisco IOS Release 15.5(2)S.

Examples

The following example shows you how to configure a service-type enumeration period of 45 minutes:

```
Device> enable
Device# configure terminal
Device(config)# service-routing mdns-sd
Device(config-mdns)# service-type-enumeration period 45
Device(config-mdns)# exit
```

Related Commands

Command	Description
service-routing mdns-sd	Enables mDNS gateway functionality for a device.
show mdns statistics	Displays mDNS statistics for the specified service-list.
show running-config mdns-sd policy	Displays current running mDNS service-policy configuration details for the device or interface.

set ip next-hop dynamic dhcp

To set the next hop to the gateway that was most recently learned by the Dynamic Host Configuration Protocol (DHCP) client, use the **set ip next-hop dynamic dhcp**command in route-map configuration mode. To restore the default setting, use the **no** form of this command.

set ip next-hop dynamic dhcp
no set ip next-hop dynamic dhcp

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Route-map configuration (config-router)

Command History

Release	Modification
12.3(2)XE	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

The **set ip next-hop dynamic dhcp**command supports only a single DHCP interface. If multiple interfaces have DHCP configured, the gateway that was most recently learned among all interfaces running DHCP will be used by the route map.

Examples

The following example shows how to configure a local routing policy that sets the next hop to the gateway that was most recently learned by the DHCP client:

```
access list 101 permit icmp any host 172.16.23.7 echo
route map MY-LOCAL-POLICY permit 10
 match ip address 101
 set ip next-hop dynamic dhcp
!
ip local policy route-map MY-LOCAL-POLICY
```

Related Commands

Command	Description
access list (IP extended)	Defines an extended IP access list.

set platform software trace forwarding-manager alg

To set the platform software trace levels for the forwarding manager application layer gateway (ALG), use the **set platform software trace forwarding-manager alg** command in privileged EXEC mode.

set platform software trace forwarding-manager {**F0** | **F1** | **FP** | **R0** | **R1** | **RP**} {**active** | **standby**} **alg** {**debug** | **emergency** | **error** | **info** | **noise** | **notice** | **verbose** | **warning**}

Syntax Description

F0	Specifies slot 0 of the Embedded Service Processor (ESP).
F1	Specifies slot 1 of the ESP.
FP	Specifies the ESP.
R0	Specifies slot 0 of the Route Processor (RP).
R1	Specifies slot 1 of the RP.
RP	Specifies the RP.
active	Specifies the active instance of the processor.
standby	Specifies the standby instance of the processor.
debug	Sets debug messages for ALGs.
emergency	Sets emergency messages for ALGs.
error	Sets error messages for ALGs.
info	Sets informational messages for ALGs.
noise	Sets the maximum message level for ALGs.
notice	Sets notice messages for ALGs.
verbose	Sets detailed debug messages for ALGs.
warning	Sets warning messages for ALGs.

Command Default

Trace levels are not set.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.11S	This command was introduced.

Usage Guidelines

Use this command to troubleshoot platform-specific ALG issues.

Examples

The following is example shows how to set platform-specific debug messages for ALGs:

```
Device# set platform software trace forwarding-manager FP active alg debug
```

Related Commands

alg sip blacklist	Configures a dynamic SIP ALG blacklist for destinations.
alg sip processor	Configures the maximum number of backlog messages that wait for shared resources.
alg sip timer	Configures a timer that SIP ALG uses to manage SIP calls.

show alg sip

To display all Session Initiation Protocol (SIP) application layer gateway (ALG) information, use the **show alg sip** command in privileged EXEC mode.

show alg sip

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.11S	This command was introduced.

Usage Guidelines

This command displays information about the configured parameters for SIP sessions.

Examples

The following is sample output from the **show alg sip** command:

```
Device# show alg sip

sip timer configuration
   Type                     Seconds
   max-call-duration        380
   call-proceeding-timeout  620

sip processor configuration
   Type           Backlog number
   session         14
   global          189

sip blacklist configuration
   dst-addr         trig-period(ms)    trig-size     block-time(sec)
   10.0.0.0             60                 30              2000
   10.1.1.1             20                 30              30
   192.0.2.115          1000                5              30
   198.51.100.34        20                 30              388
```

The table below describes the significant fields shown in the display.

Table 7: show alg sip Field Descriptions

Field	Description
sip timer configuration	Information about the configured SIP timers.
max-call-duration	Maximum call duration, in seconds, for a successful SIP call.
call-proceeding-timeout	Call proceeding time interval, in seconds, for SIP calls that do not receive a response.
sip processor configuration	Number of backlog messages that are waiting for shared resources.

Field	Description
session	Number of backlog messages in a session that are waiting for shared resources.
global	Number of backlog messages in all sessions that are waiting for shared resources.
sip blacklist configuration	Blacklist criteria configured for all destinations.
dst-addr	Destination IP address to be monitored.
trig-period (ms)	Time period, in milliseconds, during which events are monitored before a blacklist is triggered.
trig-size	Number of events that are allowed from a source before the blacklist is triggered and all packets from that source are blocked.
block-time (sec)	Time period, in seconds, when packets from a source are blocked if the configured limit exceeds.

Related Commands

alg sip blacklist	Configures a dynamic SIP ALG blacklist for destinations.
alg sip processor	Configures the maximum number of backlog messages that wait for shared resources.
alg sip timer	Configures a timer that SIP ALG uses to manage SIP calls.

show arp

To display the entries in the Address Resolution Protocol (ARP) table, use the **show arp** command in user EXEC or privileged EXEC mode.

show arp [[**vrf** *vrf-name*] [[*arp-mode*] [[*ip-address* [*mask*]] [*interface-type interface-number*]]]] [**detail**]

Syntax Description

vrf *vrf-name*	(Optional) Displays the entries under the Virtual Private Network (VPN) routing and forwarding (VRF) instance specified by the *vrf-name* argument. If this option is specified, it can be followed by any valid combination of the *arp-mode*, *ip-address*, *mask*, *interface-type*, and *interface-number* arguments and the **detail** keyword.
arp-mode	(Optional) Displays the entries that are in a specific ARP mode. This argument can be replaced by one of the following keywords: • **alias** --Displays only alias ARP entries. An alias ARP entry is a statically configured (permanent) ARP table entry that is associated with a local IP address. This type of entry can be configured or removed using the **arp** (global) command with the **alias** keyword. • **dynamic** --Displays only dynamic ARP entries. A dynamic ARP entry is learned through an ARP request and completed with the MAC address of the external host. • **incomplete** --Displays only incomplete ARP entries. An incomplete ARP entry is learned through an ARP request but has not yet been completed with the MAC address of the external host. • **interface** --Displaysonly interface ARP entries. An interface ARP entry contains a local IP address and is derived from an interface. • **static** --Displays only static ARP entries. A static ARP entry is a statically configured (permanent) ARP entry that is associated with an external host. This type of entry can be configured or removed using the **arp** (global) command. **Note** If this option is specified, it can be followed by any valid combination of the *ip-address*, *mask*, *interface-type*, and *interface-number* arguments and the **detail** keyword.
ip-address [*mask*]	(Optional) Displays the entries associated with a specific host or network. **Note** If this option is specified, it can be followed by any valid combination of the *interface-type* and *interface-number* arguments and the **detail** keyword.
interface-type interface-number	(Optional) Displays the specified entries that are also associated with this router interface. **Note** If this option is specified, it can be followed by the **detail** keyword.

detail	(Optional) Displays the specified entries with mode-specific details and information about subblocks (if any).

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.4(11)T	The **vrf** keyword and *vrf-name* argument were added to limit the display to entries under a specific VRF. The **alias**, **dynamic**, **incomplete**, **interface**, and **static** keywords were added to limit the display to entries in a specific ARP mode. The *ip-address* and *mask* arguments were added to limit the display to entries for a specific host or network. The *interface-type*and *interface-number* arguments were added to limit the display to entries for a specific interface. The **detail** keyword was added to display additional details about the entries.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

To display all entries in the ARP cache, use this command without any arguments or keywords.

Entry Selection Options

You can to limit the scope of the command output by applying various combinations of the following ARP entry selection criteria:

- Entries under a specific VRF
- Entries in a specific ARP mode
- Entries for a specific host or entries for a specific network
- Entries associated with a specific router interface



Tip The valid interface types and numbers can vary according to the router and the interfaces on the router. To list all the interfaces configured on a particular router, use the **show interfaces** command with the **summary** keyword. Use the appropriate interface specification, typed exactly as it is displayed under the Interface column of the **show interfaces** command output, to replace the *interface-type*and *interface-number* arguments in the **show arp** command.

Detailed Output Format

To include additional details about each ARP entry displayed, use this command with the **detail** keyword. When this display option is used, the following additional information is included:

- Mode-specific details (such as entry update time)
- Subblocks (if any)

ARP Adjacency Notification

If Cisco Express Forwarding (CEF) is enabled on the router, the router maintains forwarding information (outbound interface and MAC header rewrite) for adjacent nodes. A node is said to be adjacent to another node if the node can be reached with a single hop across a link layer (Layer 2). CEF stores the forwarding information in an adjacency database so that Layer 2 addressing information can be inserted into link-layer headers attached to the ARP packets.

- To verify that IPv4 CEF is running, use the **show ip cef** command.
- To verify that an adjacency exists for a connected device, that the adjacency is valid, and that the MAC header rewrite string is correct, use the **show adjacency** command.

The ARP table information is one of the sources for CEF adjacency. Whenever the ARP subsystem attaches an ARP table entry to an outbound interface with a valid hardware address, the subsystem issues an internal "ARP adjacency" notification. The notification causes an ARP background process to synchronize that ARP entry with CEF adjacency via the adjacency database. If the synchronization succeeds, IP ARP adjacency is said to be "installed"; if the synchronization fails, IP ARP adjacency is said to have been "withdrawn."



Note Attachment to an outbound interface occurs only for ARP entries in the following modes: alias, dynamic, static, Application Simple, and Application Timer.

To display detailed information about any ARP adjacency notification that may have occurred, use the **show arp** command with the **detail** keyword. You can use this information to supplement the information available through ARP/CEF adjacency debug trace. To enable debug trace for ARP/CEF adjacency interactions, use the **debug arp** command with the **adjacency** keyword.

ARP Cache Administration

To refresh all entries for the specified interface (or all interfaces) or to refresh all entries of the specified address (or all addresses) in the specified VRF table (or in the global VRF table), use the **clear arp-cache** command.

To enable debugging output for ARP transactions, use the **debug arp** command.

Examples

The following is sample output from the **show arp** command with no optional keywords or arguments specified:

```
Router# show arp

Protocol   Address          Age (min)   Hardware Addr   Type    Interface
Internet   192.0.2.112      120         0000.a710.4baf  ARPA    Ethernet3
AppleTalk  4028.5           29          0000.0c01.0e56  SNAP    Ethernet2
Internet   192.0.2.114      105         0000.a710.859b  ARPA    Ethernet3
AppleTalk  4028.9           -           0000.0c02.a03c  SNAP    Ethernet2
Internet   192.0.2.121      42          0000.a710.68cd  ARPA    Ethernet3
Internet   192.0.2.9        -           0000.3080.6fd4  SNAP    TokenRing0
AppleTalk  4036.9           -           0000.3080.6fd4  SNAP    TokenRing0
Internet   192.0.2.9        -           0000.0c01.7bbd  SNAP    Fddi0
```

The table below describes the fields shown in the display.

Table 8: show arp Field Descriptions

Field	Description
Protocol	Protocol for network address in the Address field.
Address	The network address that corresponds to the Hardware Address.
Age (min)	Age in minutes of the cache entry. A hyphen (-) means the address is local.
Hardware Addr	LAN hardware address of a MAC address that corresponds to the network address.
Type	Indicates the encapsulation type the Cisco IOS software is using for the network address in this entry. Possible values include: • ARPA--For Ethernet interfaces. • SAP--For Hewlett-Packard interfaces. • SMDS--For Switched Multimegabit Data Service (SMDS) interfaces. • SNAP--For FDDI and Token Ring interfaces. • SRP-A--For Switch Route Processor, side A (SRP-A) interfaces. • SRP-B--For Switch Route Processor, side B (SRP-B) interfaces.
Interface	Indicates the interface associated with this network address.

When this command is used to display dynamic ARP entries, the display information includes the time of the last update and the amount of time before the next scheduled refresh is to occur. The following is sample output from the **show arp** command for the dynamic ARP entry at network address 192.0.2.1:

```
Router# show arp 192.0.2.1 detail

ARP entry for 192.0.2.1, link type IP.
  Alias, last updated 13323 minutes ago.
  Encap type is ARPA, hardware address is 1234.1234.1234, 6 bytes long.
  ARP subblocks:
  * Static ARP Subblock
    Floating entry.
    Entry is complete, attached to GigabitEthernet1/1.
  * IP ARP Adjacency
    Adjacency (for 192.0.2.1 on GigabitEthernet1/1) was installed.
```

When this command is used to display floating static ARP entries, the display information includes the associated interface, if any.The following is sample output from the **show arp** command for the floating static ARP entry at network address 192.0.2.2 whose intended interface is down:

```
Router# show arp 192.0.2.2 detail

ARP entry for 192.0.2.2, link type IP.
  Alias, last updated 13327 minutes ago.
  Encap type is ARPA, hardware address is 1234.1234.1234, 6 bytes long.
  ARP subblocks:
  * Static ARP Subblock
    Floating entry.
```

```
    Entry is incomplete.
  * IP ARP Adjacency
    Adjacency (for 192.0.2.2 on GigabitEthernet1/1) was withdrawn.
```

The following is sample detailed output from the **show arp** command for the Application Alias ARP entry at network address 192.0.2.3:

```
Router# show arp 192.0.2.3 detail

ARP entry for 192.0.2.3, link type IP.
  Application Alias, via Ethernet2/2, last updated 0 minute ago.
  Created by "HSRP".
  Encap type is ARPA, hardware address is 0000.0c07.ac02, 6 bytes long.
  ARP subblocks:
  * Application Alias ARP Subblock
  * HSRP
    ARP Application entry for application HSRP.
```

The following is sample detailed output from the **show arp** command for all dynamic ARP entries:

```
Router# show arp dynamic detail

ARP entry for 192.0.2.4, link type IP.
  Dynamic, via Ethernet2/1, last updated 0 minute ago.
  Encap type is ARPA, hardware address is 0000.0000.0014, 6 bytes long.
  ARP subblocks:
  * Dynamic ARP Subblock
    Entry will be refreshed in 0 minute and 1 second.
    It has 1 chance to be refreshed before it is purged.
    Entry is complete.
  * IP ARP Adjacency
    Adjacency (for 192.0.2.4 on Ethernet2/1) was installed.
```

Related Commands

Command	Description
arp (global)	Configures a permanent entry in the ARP cache.
clear arp-cache	Refreshes dynamically learned entries in the ARP cache.
debug arp	Enables debugging output for ARP packet transactions.
show adjacency	Verifies that an adjacency exists for a connected device, that the adjacency is valid, and that the MAC header rewrite string is correct.
show arp application	Displays ARP table information for a specific ARP application or for all applications supported by ARP and running on registered clients.
show arp ha	Displays the ARP HA status and statistics.
show arp summary	Displays the number of the ARP table entries of each mode.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show ip cef	Display entries in the FIB or to display a summary of the FIB.

show arp application

To display Address Resolution Protocol (ARP) table information for a specific ARP application or for all applications supported by ARP and running on registered clients, use the **show arp application**command in user EXEC or privileged EXEC mode.

show arp application [*application-id*] [**detail**]

Syntax Description

application-id	(Optional) Displays ARP table information for a specific ARP application. The range is from 200 to 4294967295. If no ID is specified, ARP table information is displayed for all supported ARP applications running on registered clients.
detail	(Optional) Includes detailed information about subblocks for ARP table information displayed (for the specified application or for all applications supported by ARP and running on registered clients).

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

To display ARP table information about all supported ARP applications running on registered clients, use this command without any arguments or keywords.

Entry Selection Options

To display ARP table information about a single ARP application running on a registered client, use this command with the *application-ID*argument.

Detailed Output Format

To display the specified ARP table information along with detailed information about any subblocks, use this command with the **detail** keyword. The additional details consist of the following information:

- IP address or network
- ARP table entry type (dynamic, interface, static, or alias) or ARP application mode (Simple Application or Application Alias)
- Associated interface
- Brief description of the subblock data

Examples

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

```
Router# show arp application
```

```
Number of clients registered: 7
Application         ID        Num of Subblocks
ARP Backup          200       1
IP SIP              201       0
LEC                 202       0
DHCPD               203       0
IP Mobility         204       0
HSRP                209       1
IP ARP Adjacency    212       2
```

The following is sample detailed output from the **show arp application detail** command:

```
Router# show arp application detail

Number of clients registered: 7
Application         ID        Num of Subblocks
ARP Backup          200       1
ARP entry for 192.0.2.10, link type IP.
  Application Alias, via Ethernet2/2.
    Subblock data:
    Backup for Interface on Ethernet2/2
Application         ID        Num of Subblocks
IP SIP              201       0
Application         ID        Num of Subblocks
LEC                 202       0
Application         ID        Num of Subblocks
DHCPD               203       0
Application         ID        Num of Subblocks
IP Mobility         204       0
Application         ID        Num of Subblocks
HSRP                209       1
ARP entry for 192.0.2.10, link type IP.
  Application Alias, via Ethernet2/2.
    Subblock data:
    ARP Application entry for application HSRP.
Application         ID        Num of Subblocks
IP ARP Adjacency    212       2
ARP entry for 192.0.2.4, link type IP.
  Dynamic, via Ethernet2/1.
    Subblock data:
    Adjacency (for 192.0.2.4 on Ethernet2/1) was installed.
ARP entry for 192.0.2.2, link type IP.
  Dynamic, via Ethernet2/1.
    Subblock data:
    Adjacency (for 192.0.2.2 on Ethernet2/1) was installed.
```

The table below describes the significant fields shown in the display.

Table 9: show arp application Field Descriptions

Field	Description
Application	ARP application name
ID	ARP application ID number
Num of Subblocks	Number of subblocks attached

Related Commands

Command	Description
debug arp	Enables debugging output for ARP packet transactions.
show arp	Displays ARP table entries.
show arp ha	Displays the ARP HA status and statistics.
show arp summary	Displays the number of the ARP table entries of each mode.

show arp ha

To display the status and statistics of Address Resolution Protocol (ARP) high availability (HA), use the **show arp ha** command in user EXEC or privileged EXEC mode.

show arp ha

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

Use this command to display the ARP HA status and statistics.

HA-Capable Platforms

This command is available only on HA-capable platforms (that is, Cisco networking devices that support dual Route Processors [RPs]).

ARP HA Statistics

The ARP HA process collects one set of statistics for the active RP (described in the show arp ha Field Descriptions for Statistics Collected for an Active RP table below) and a different set of statistics for the standby RP (described in the show arp ha Field Descriptions for Statistics Collected for a Standby RP table below). These statistics can be used to track the RP state transitions when a user is debugging ARP HA issues.

The output from this command depends on the current and most recent states of the RP:

- For the active RP that has been the active RP since the last time the router was rebooted, this command displays the HA statistics for the active RP.
- For the active RP that had been a standby RP and became the active RP after the most recent stateful switchover (SSO) occurred, this command displays the HA statistics for the active RP plus the HA statistics collected when the RP was a standby RP.
- For a standby RP, this command displays the HA statistics for a standby RP.

Examples

The following is sample output from the **show arp ha** command on the active RP that has been the active RP since the last time the router was rebooted. ARP HA statistics are displayed for the active state only.

```
Router# show arp ha

ARP HA in active state (ARP_HA_ST_A_UP_SYNC).
  2 ARP entries in the synchronization queue.
  No ARP entry waiting to be synchronized.
  806 synchronization packets sent.
  No error in allocating synchronization packets.
```

```
  No error in sending synchronization packets.
  No error in encoding interface names.
```

The following is sample output from the **show arp ha** command on the active RP that had been a standby RP and became the active RP after the most recent SSO occurred. ARP HA statistics are displayed for the active state and also for the previous standby state.

```
Router# show arp ha

ARP HA in active state (ARP_HA_ST_A_UP).
  1 ARP entry in the synchronization queue.
  1 ARP entry waiting to be synchronized.
  No synchronization packet sent.
  No error in allocating synchronization packets.
  No error in sending synchronization packets.
  No error in encoding interface names.
Statistics collected when ARP HA in standby state:
  No ARP entry in the backup table.
  808 synchronization packets processed.
  No synchronization packet dropped in invalid state.
  No error in decoding interface names.
  2 ARP entries restored before timer.
  No ARP entry restored on timer.
  No ARP entry purged since interface is down.
  No ARP entry purged on timer.
```

The following is sample output from the **show arp ha** command on the standby RP. ARP HA statistics are displayed for the standby state only.

```
Router# show arp ha

ARP HA in standby state (ARP_HA_ST_S_UP).
  2 ARP entries in the backup table.
  806 synchronization packets processed.
  No synchronization packet dropped in invalid state.
  No error in decoding interface names.
```

The table below describes the significant fields shown in the display collected for an active RP.

Table 10: show arp ha Field Descriptions for Statistics Collected for an Active RP

Field	Description
ARP HA in active state	The current state that the event-driven state machine contains for the active RP: • ARP_HA_ST_A_BULK--Transient state in which the active RP waits for the standby RP to signal that it has finished processing of the entries sent by the bulk-synchronization operation. • ARP_HA_ST_A_SSO--Transient state in which the new active RP waits for the signal to be fully operational. • ARP_HA_ST_A_UP--Active state in which the active RP does not send entries to the standby RP. The active RP transitions into this state either because the standby RP has not come up yet or because a previous synchronization has failed. • ARP_HA_ST_A_UP_SYNC--Active state in which the active RP sends entries from the synchronization queue to the standby RP. The active RP transitions into this state when the number of entries to be synchronized reaches a threshold or when the synchronization timer expires, whichever occurs first.
ARP entries in the synchronization queue	Number of ARP entries that are queued to be synchronized or have already been synchronized to the standby RP. **Note** Entries that have already been synchronized are kept in the synchronization queue in case the standby RP reloads. After the standby RP reboots, the entire queue (including entries that were already synchronized to the standby RP before the reload) must be bulk-synchronized to the standby RP.
ARP entry waiting to be synchronized	Number of ARP entries that are queued to be synchronized to the standby RP.
synchronization packets sent	Number of synchronization packets that have been sent to the standby RP.
error in allocating synchronization packets	Number of errors that occurred while synchronization packets were being allocated.
error in sending synchronization packets.	Number of errors that occurred while synchronization packets were being sent to the standby RP.
error in encoding interface names	Number of errors that occurred while interface names were being encoded.

The table below describes the significant fields shown in the display collected for a standby RP or for an active RP that was previously in the active state.

Table 11: show arp ha Field Descriptions for Statistics Collected for a Standby RP

Field	Description
ARP HA in standby state	The current state that the event-driven state machine contains for the standby RP: • ARP_HA_ST_S_BULK--Transient state in which the standby RP processes the entries sent by the bulk-synchronization operation. After the active RP signals that it has finished sending entries, the standby RP transitions into the ARP_HA_ST_S_UP state and then signals back to the active RP that it has finished processing the entries sent by the bulk-synchronization operation. • ARP_HA_ST_S_UP--Active state in which the standby RP processes the incremental ARP synchronization entries from the active RP. When the switchover occurs, the standby RP transitions to the ARP_HA_ST_A_SSO state.
ARP entries in the backup table	Number of ARP entries contained in the backup ARP table.
synchronization packets processed	Number of synchronization packets that were processed.
synchronization packet dropped in invalid state	Number of synchronization packets that were dropped due to an invalid state.
error in decoding interface names	Number of errors that occurred in decoding interface names.
ARP entries restored before timer	Number of ARP entries that the new active RP restored prior to expiration of the “flush” timer.
ARP entry restored on timer	Number of ARP entries that the new active RP restored upon expiration of the “flush” timer.
ARP entry purged since interface is down	Number of ARP entries that the new active RP purged because the interface went down.
ARP entry purged on timer	Number of ARP entries that the new active RP purged upon expiration of the “flush” timer.

Related Commands

Command	Description
clear arp-cache counters ha	Resets the ARP HA statistics.
debug arp	Enables debugging output for ARP packet transactions.
show arp	Displays ARP table entries.
show arp application	Displays ARP table information for a specific ARP application or for all applications supported by ARP and running on registered clients.
show arp summary	Displays the number of the ARP table entries of each mode.

show arp summary

To display the total number of Address Resolution Protocol (ARP) table entries, the number of ARP table entries for each ARP entry mode, and the number of ARP table entries for each interface on the router, use the **show arp summary** command in user EXEC or privileged EXEC mode.

show arp summary

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SRD3	This command was modified. Support was added for the Cisco 7600 router.

Usage Guidelines

Use this command to display high-level statistics about the ARP table entries:

- Total number of ARP table entries
- Number of ARP table entries for each ARP mode
- Number of ARP table entries for each router interface

A maximum limit for learned ARP entries can be configured on the Cisco 7600 platform in Cisco IOS Release 12.2(33)SRD3. This is subject to memory constraints. The 7600 can support a maximum limit of 256,000 learned ARP entries, and if a memory card is installed on the router the maximum limit is extended to 512,000.

Examples

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



Note In this example the maximum limit for the number of learned ARP entries has not been configured.

```
Router# show arp summary

Total number of entries in the ARP table: 10.
Total number of Dynamic ARP entries: 4.
Total number of Incomplete ARP entries: 0.
Total number of Interface ARP entries: 4.
Total number of Static ARP entries: 2.
Total number of Alias ARP entries: 0.
Total number of Simple Application ARP entries: 0.
Total number of Application Alias ARP entries: 0.
Total number of Application Timer ARP entries: 0.
```

```
Interface Entry Count
Ethernet3/2 1
```

The following is sample output from the **show arp summary**command on a Cisco 7600 router for Cisco IOS Release 12.2(33)SRD3, after a maximum limit is set for the number of learned ARP entries:

```
Router> enable
Router# configure terminal
Router(config)# ip arp entry learn 512000
Router(config)# exit
Router# show arp summary
Total number of entries in the ARP table: 4.
Total number of Dynamic ARP entries: 0.
Total number of Incomplete ARP entries: 0.
Total number of Interface ARP entries: 3.
Total number of Static ARP entries: 1.
Total number of Alias ARP entries: 0.
Total number of Simple Application ARP entries: 0.
Total number of Application Alias ARP entries: 0.
Total number of Application Timer ARP entries: 0.
Maximum limit of Learn ARP entry : 512000.
Maximum configured Learn ARP entry limit : 512000.
Learn ARP Entry Threshold is 409600 and Permit Threshold is 486400.
Total number of Learn ARP entries: 0.
Interface              Entry Count
GigabitEthernet4/7               1
GigabitEthernet4/1.1             1
GigabitEthernet4/1               1
EOBC0/0
```

The table below describes the fields shown in the display.

Table 12: show arp summary Command Field Descriptions

Field	Description
Total Number of entries in the ARP table	Displays the number of entries in the ARP table.
Total number of Dynamic ARP entries	Displays the number of ARP entries in the dynamic state.
Total number of Incomplete ARP entries	Displays the number of ARP entries in the incomplete state.
Total number of Interface ARP entries	Displays the number of ARP entries on ARP enabled interfaces.
Total number of Static ARP entries	Displays the number of active statically configured ARP entries.
Total number of Alias ARP entries	Displays the number of active statically configured alias entries.
Total number of Simple Application ARP entries	Displays the number of ARP entries in the simple application mode.
Total number of Application Alias ARP entries	Displays the number of ARP entries in the application alias mode.

Field	Description
Total number of Application Timer ARP entries	Displays the number of ARP entries in the application timer mode.
Maximum limit of Learn ARP entry	Displays the allowed maximum limit for the learned ARP entries.
Maximum configured Learn ARP entry limit	Displays the figure the maximum learned ARP entry limit is set to.
Learn ARP Entry Threshold	Displays the value representing 80 percent of the set maximum learned ARP entry limit.
Permit Threshold	Displays the value representing 95 percent of the set maximum learned ARP entry limit.
Total number of Learn ARP entries	Displays the total number of learned ARP entries.
Interface	Lists the names of the ARP enabled interfaces.
Entry Count	Displays the number of ARP entries on each ARP enabled interface

Related Commands

Command	Description
clear arp-cache	Refreshes dynamically learned entries in the ARP cache.
ip arp entry learn	Specifies the maximum number of learned ARP entries.
show arp	Displays ARP table entries.
show arp application	Displays ARP table information for a specific ARP application or for all applications supported by ARP and running on registered clients.
show arp ha	Displays the ARP HA status and statistics.

show auto-ip-ring

To display auto-IP ring information for a specific device or auto-IP ring, use the **show auto-ip-ring** command in privileged EXEC mode.

show auto-ip-ring [*ring-id*] [**detail**]

Syntax Description

ring-id	(Optional) Auto-IP ring identification number.
detail	(Optional) Specifies detailed information for auto-IP enabled interfaces, including the neighbor interface's auto-IP address, interface IP address, and priority value. If the auto-IP enabled interface is assigned to a VRF, the VRF name is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.10S	This command was introduced.
15.3(3)S	This command was integrated into Cisco IOS Release15.3(3)S
Cisco IOS XE Release 3.12S	This command was modified. The VRF Name field was added in the command output.
15.4(2)S	This command was integrated into Cisco IOS Release15.4(2)S.

Usage Guidelines

To view auto-IP information for all auto-IP enabled node interfaces for a device, use the **show auto-ip-ring** command without the *ring-id* argument.

To view auto-IP information for a specific auto-IP ring, use the *ring-id* argument. If the auto-IP enabled interface is assigned to a VRF, use the **detail** keyword to view the VRF name.

Examples

The following is sample output for the **show auto-ip-ring detail** command. This command displays auto-IP ring information for VRF interfaces.

```
Device# show auto-ip-ring detail

Auto-IP ring 7
Auto-IP Address         : 10.1.1.11

VRF Name                : 3
Ring Port1              : Ethernet1/1
My Current-IP           : 10.1.1.11
My Priority             : 2

Rx Auto-IP Address      : 10.1.1.13
Rx Current-IP           : 10.1.1.10
Rx Priority             : 0


VRF Name                : 3
Ring Port0              : Ethernet1/0
```

```
My Current-IP           : 10.1.1.8
My Priority             : 0

Rx Auto-IP Address      : 10.1.1.9
Rx Current-IP           : 10.1.1.9
Rx Priority             : 2
```

The following is sample output for the **show auto-ip-ring** command. The example displays detailed information for the auto-IP ring on a device:



Note In this example, information for only one node interface (and corresponding neighbor interface information) is displayed. The other interface is not connected to a neighbor node interface since it is an open ring.

```
Device> enable
Device# show auto-ip-ring 4 detail


Auto-IP ring 4
Auto-IP Address : 10.1.1.3

Ring Port0 : Ethernet0/0
My Current-IP : 10.1.1.0
My Priority : 0

Rx Auto-IP Address : 10.1.1.1
Rx Current-IP : 10.1.1.1
Rx Priority : 2
```

Table 13: show auto-ip-ring Field Descriptions

Field	Description
Auto-IP ring	The auto-IP ring identification number.
Auto-IP Address	The auto IP address configured on the node interface.
VRF Name	VRF which contains auto-IP enabled interfaces. The auto-IP enabled VRF interfaces are displayed in the command output along with the VRF name.
Ring Port0	Node interface for the specified auto-IP ring. Ethernet 0/0 is one of the 2 interfaces in the specified auto-IP ring.
My Current-IP	IP address configured on the interface.
My Priority	Auto-IP TLV priority value sent from the current node interface to the neighbor node interface.

Field	Description
Rx Auto-IP Address	Auto-IP address of the neighbor node interface. This information is received from the connected, neighbor interface.
Rx Current-IP	IP address configured on the neighbor node interface. This information is received from the connected, neighbor interface.
Rx Priority	Priority value of the neighbor node interface. This information is received from the connected, neighbor interface.

Related Commands

Command	Description
auto-ip-ring	Enables the auto-IP functionality on the interfaces of a device.
debug auto-ip-ring	Debugs errors or events specific to an auto-IP ring.

show hosts

To display the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses specific to a particular Domain Name System (DNS) view or for all configured DNS views, use the **show hosts** command in privileged EXEC mode.

show hosts [**vrf** *vrf-name*] [**view** [*view-name* | **default**]] [**all**] [*hostname* | **summary**]

Syntax Description

vrf *vrf-name*	(Optional) The *vrf-name* argument specifies the name of the Virtual Private Network (VPN) routing and forwarding (VRF) instance associated with the DNS view whose hostname cache entries are to be displayed. Default is the global VRF (that is, the VRF whose name is a NULL string) with the specified or default DNS view. **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.
view *view-name*	(Optional) The *view-name* argument specifies the DNS view whose hostname cache information is to be displayed. Default is the default (unnamed) DNS view associated with the specified or global VRF. **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.
default	(Optional) Displays the default view.
all	(Optional) Display all the host tables.
hostname	(Optional) The specified hostname cache information displayed is to be limited to entries for a particular hostname. Default is the hostname cache information for all hostname entries in the cache.
summary	(Optional) The specified hostname cache information is to be displayed in brief summary format. Disabled by default.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2T	Support was added for Cisco modem user interface feature.
12.4(4)T	The **vrf**, **all**, and **summary** keywords and *vrf-name* and *hostname* arguments were added.
12.4(9)T	The **view** keyword and *view-name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views.

If you specify the **show hosts** command without any optional keywords or arguments, only the entries in the global hostname cache will be displayed.

If the output from this command extends beyond the bottom of the screen, press the Space bar to continue or press the Q key to terminate command output.

Examples

The following is sample output from the **show hosts** command with no parameters specified:

```
Router# show hosts

Default domain is CISCO.COM
Name/address lookup uses domain service
Name servers are 192.0.2.220
Host Flag Age Type Address(es)
EXAMPLE1.CISCO.COM (temp, OK) 1 IP 192.0.2.10
EXAMPLE2.CISCO.COM (temp, OK) 8 IP 192.0.2.50
EXAMPLE3.CISCO.COM (temp, OK) 8 IP 192.0.2.115
EXAMPLE4.CISCO.COM (temp, EX) 8 IP 192.0.2.111
EXAMPLE5.CISCO.COM (temp, EX) 0 IP 192.0.2.27
EXAMPLE6.CISCO.COM (temp, EX) 24 IP 192.0.2.30
```

The following is sample output from the **show hosts** command that specifies the VRF vpn101:

```
Router# show hosts vrf vpn101

Default domain is example.com
Domain list: example1.com, example2.com, example3.com
Name/address lookup uses domain service
Name servers are 192.0.2.204, 192.0.2.205, 192.0.2.206
Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
       temp - temporary, perm - permanent
       NA - Not Applicable None - Not defined
Host                    Port  Flags      Age Type   Address(es)
user                    None  (perm, OK)  0   IP    192.0.2.001
www.example.com         None  (perm, OK)  0   IP    192.0.2.111
                                                    192.0.2.112
```

The table below describes the significant fields shown in the display.

Table 14: show hosts Field Descriptions

Field	Description
Default domain	Default domain name to be used to complete unqualified names if no domain list is defined.
Domain list	List of default domain names to be tried in turn to complete unqualified names.

Field	Description
Name/address lookup	Style of name lookup service.
Name servers	List of name server hosts.
Host	Learned or statically defined hostname. Statically defined hostname-to-address mappings can be added to the DNS hostname cache for a DNS view by using the **ip hosts** command.
Port	TCP port number to connect to when using the defined hostname in conjunction with an EXEC connect or Telnet command.
Flags	Indicates additional information about the hostname-to-IP address mapping. Possible values are as follows: • EX--Entries marked EX are expired. • OK--Entries marked OK are believed to be valid. • perm--A permanent entry is entered by a configuration command and is not timed out. • temp--A temporary entry is entered by a name server; the Cisco IOS software removes the entry after 72 hours of inactivity. • ??--Entries marked ?? are considered suspect and subject to revalidation.
Age	Number of hours since the software last referred to the cache entry.
Type	Type of address. For example, IP, Connectionless Network Service (CLNS), or X.121. If you have used the **ip hp-host global** configuration command, the **show hosts** command will display these hostnames as type HP-IP.
Address(es)	IP address of the host. One host may have up to eight addresses.

Related Commands

Command	Description
clear host	Removes static hostname-to-address mappings from the hostname cache for the specified DNS view or all DNS views.
ip host	Defines static hostname-to-address mappings in the DNS hostname cache for a DNS view.

show ip aliases

To display the IP addresses that are mapped to TCP ports (aliases) and Serial Line Internet Protocol (SLIP) addresses, which are treated similar to aliases, use the **show ip aliases** command in user EXEC or privileged EXEC mode.

show ip aliases

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T. The output of the command was changed to display dynamic and interface IP addresses, even when both IP addresses are the same.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE. The output of the command was changed to display only external IP addresses. Internal IP addresses are not displayed.

Usage Guidelines

To distinguish a SLIP address from a normal alias address, the command output displays SLIP TTY1 for the port number, where 1 is the auxiliary port. The display lists the address type, the IP address, and the corresponding port number. The fields in the output are self-explanatory.

Examples

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

```
Device# show ip aliases
Address Type             IP Address           Port
Dynamic                  198.51.100.1
Dynamic                  198.51.100.22
Dynamic                  209.165.200.230
Dynamic                  203.0.113.2
Interface                203.0.113.200        SLIP TTY1
Interface                198.51.100.100       SLIP TTY1
Interface                209.165.201.20       SLIP TTY1
Dynamic                  209.165.200.226
Interface                209.165.200.225
```



Note Only external IP addresses are displayed in the **show ip aliases** command output. Internal IP addresses are not displayed.

Related Commands

Command	Description
show line	Displays the parameters of a terminal line.

show ip arp

To display the Address Resolution Protocol (ARP) cache, where Serial Line Internet Protocol (SLIP) addresses appear as permanent ARP table entries, use the **show ip arp** EXEC command.

show ip arp [*ip-address*] [*host-name*] [*mac-address*] [*interface type number*]

Syntax Description

ip-address	(Optional) ARP entries matching this IP address are displayed.
host-name	(Optional) Host name.
mac-address	(Optional) 48-bit MAC address.
interface type number	(Optional) ARP entries learned via this interface type and number are displayed.

Command Modes

EXEC

Command History

Release	Modification
9.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

ARP establishes correspondences between network addresses (an IP address, for example) and LAN hardware addresses (Ethernet addresses). A record of each correspondence is kept in a cache for a predetermined amount of time and then discarded.

Examples

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

```
Router# show ip arp
Protocol  Address              Age(min)       Hardware Addr     Type      Interface
Internet  172.16.233.229       -              0000.0c59.f892    ARPA      Ethernet0/0
Internet  172.16.233.218       -              0000.0c07.ac00    ARPA      Ethernet0/0
Internet  172.16.233.19        -              0000.0c63.1300    ARPA      Ethernet0/0
Internet  172.16.233.309       -              0000.0c36.6965    ARPA      Ethernet0/0
Internet  172.16.168.11        -              0000.0c63.1300    ARPA      Ethernet0/0
Internet  172.16.168.254       9              0000.0c36.6965    ARPA      Ethernet0/0
```

The table below describes the significant fields shown in the display.

Table 15: show ip arp Field Descriptions

Field	Description
Protocol	Protocol for network address in the Address field.
Address	The network address that corresponds to the Hardware Address.
Age (min)	Age in minutes of the cache entry. A hyphen (-) means the address is local.
Hardware Addr	LAN hardware address of a MAC address that corresponds to the network address.

Field	Description
Type	Indicates the encapsulation type the Cisco IOS software is using the network address in this entry. Possible value include: • ARPA • SNAP • SAP
Interface	Indicates the interface associated with this network address.

show ip arp inspection

To display the status of DAI for a specific range of VLANs, use the **show ip arp inspection**command in privileged EXEC mode.

show ip arp inspection [**interfaces** [**interface-name**] | **statistics** [**vlan** *vlan-range*]]

Syntax Description

interfaces *interface-name*	(Optional) Displays the trust state and the rate limit of ARP packets for the provided interface.
statistics	(Optional) Displays statistics for the following types of packets that have been processed by this feature: forwarded, dropped, MAC validation failure, and IP validation failure.
vlan *vlan-range*	(Optional) Displays the statistics for the selected range of VLANs.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you do not enter the **statistics** keyword, the configuration and operating state of DAI for the selected range of VLANs is displayed.

If you do not specify the interface name, the trust state and rate limit for all applicable interfaces in the system are displayed.

Examples

This example shows how to display the statistics of packets that have been processed by DAI for VLAN 3:

```
Router# show ip arp inspection statistics vlan 3
 Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    3          31753         102407         102407              0
 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    3          31753              0                     0
 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    3                  0                        0
```

This example shows how to display the statistics of packets that have been processed by DAI for all active VLANs:

```
Router# show ip arp inspection statistics
 Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
```

```
----      ---------         -------     ----------     ----------
   1              0              0              0              0
   2              0              0              0              0
   3          68322         220356         220356              0
   4              0              0              0              0
 100              0              0              0              0
 101              0              0              0              0
1006              0              0              0              0
1007              0              0              0              0
Vlan   DHCP Permits    ACL Permits   Source MAC Failures
----   ------------    -----------   -------------------
   1              0              0                    0
   2              0              0                    0
   3          68322              0                    0
   4              0              0                    0
 100              0              0                    0
 101              0              0                    0
1006              0              0                    0
1007              0              0                    0
Vlan   Dest MAC Failures   IP Validation Failures
----   -----------------   ----------------------
   1                  0                        0
   2                  0                        0
   3                  0                        0
   4                  0                        0
 100                  0                        0
 101                  0                        0
1006                  0                        0
1007                  0                        0
```

This example shows how to display the configuration and operating state of DAI for VLAN 1:

```
Router# show ip arp inspection vlan 1
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
    1     Enabled          Active
 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
    1     Deny             Deny
```

This example shows how to display the trust state of Fast Ethernet interface 6/3:

```
Router# show ip arp inspection interfaces fastEthernet 6/3
Interface        Trust State     Rate (pps)    Burst Interval
 ---------------  -----------     ----------    --------------
 Fa6/1            Untrusted              20                 5
```

This example shows how to display the trust state of the interfaces on the switch:

```
Router# show ip arp inspection interfaces
Interface        Trust State     Rate (pps)
 ---------------  -----------     ----------
 Gi1/1            Untrusted              15
 Gi1/2            Untrusted              15
 Gi3/1            Untrusted              15
 Gi3/2            Untrusted              15
 Fa3/3            Trusted              None
 Fa3/4            Untrusted              15
 Fa3/5            Untrusted              15
```

```
Fa3/6            Untrusted              15
Fa3/7            Untrusted              15
```

Related Commands

Command	Description
arp access-list	Configures an ARP ACL for ARP inspection and QoS filtering and enters the ARP ACL configuration submode.
clear ip arp inspection log	Clears the status of the log buffer.
show ip arp inspection	Displays the status of DAI for a specific range of VLANs.

show ip arp inspection log

To show the status of the log buffer, use the **show ip arp inspection log**command in privileged EXEC mode.

show ip arp inspection log

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to display the current contents of the log buffer before and after the buffers are cleared:

```
Router# show ip arp inspection log
Total Log Buffer Size : 10
Syslog rate : 0 entries per 10 seconds.
 Interface        Vlan   Sender MAC         Sender IP        Num of Pkts
 ---------------  -----  -----------------  ---------------  -----------
Fa6/3            1     0002.0002.0002  10.1.1.2          1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3            1     0002.0002.0002  10.1.1.3          1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3            1     0002.0002.0002  10.1.1.4          1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3            1     0002.0002.0002  10.1.1.5          1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3            1     0002.0002.0002  10.1.1.6          1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3            1     0002.0002.0002  10.1.1.7          1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3            1     0002.0002.0002  10.1.1.8          1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3            1     0002.0002.0002  10.1.1.9          1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3            1     0002.0002.0002  10.1.1.10         1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3            1     0002.0002.0002  10.1.1.11         1(12:02:52 UTC Fri Apr 25 2003)
    --            --         --               --       5(12:02:52 UTC Fri Apr 25 2003)
```

This example shows how to clear the buffer with the **clear ip arp inspection log** command:

```
Router# clear ip arp inspection log

Router# show ip arp inspection log

Total Log Buffer Size : 10
Syslog rate : 0 entries per 10 seconds.
No entries in log buffer.
```

Related Commands

Command	Description
clear ip arp inspection log	Clear the status of the log buffer.
show ip arp inspection log	Shows the status of the log buffer.

show ip arp poll

To display the IP Address Resolution Protocol (ARP) host polling status, use the **show ip arp poll** command in privileged EXEC mode.

show ip arp poll [**detail**]

Syntax Description

detail	(Optional) Displays the detailed IP ARP host polling status.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)SY	This command was introduced.

Examples

The following is sample output from the **show ip arp poll** command. The output fields are self-explanatory.

```
Device# show ip arp poll

Number of IP addresses processed for polling: 438
Number of entries in the queue: 100 (high water mark: 154, max: 1000)
Number of request dropped:
  Queue was full: 1288
  Request was throttled by incomplete ARP: 10
  Duplicate entry found in queue: 1431
```

Related Commands

Command	Description
ip arp poll	Configures IP ARP polling for unnumbered interfaces.

show ip ddns update

To display information about the Dynamic Domain Name System (DDNS) updates, use the **show ip ddns update**command in privileged EXEC mode.

show ip ddns update [*interface-type number*]

Syntax Description

interface-type number	(Optional) Displays DDNS updates configured on an interface.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)YA	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Examples

The following output shows the IP DDNS update method on loopback interface 100 and the destination:

```
Router# show ip ddns update
Dynamic DNS Update on Loopback100:
 Update Method Name     Update Destination
 testing                10.1.2.3
```

Related Commands

Command	Description
ip ddns update method	Specifies a method of DDNS updates of A and PTR RRs and the maximum interval between the updates.

show ip ddns update method

To display information about the Dynamic Domain Name System (DDNS) update method, use the **show ip ddns update method**command in privileged EXEC mode.

show ip ddns update method [*method-name*]

Syntax Description

method-name	(Optional) Name of the update method.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)YA	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Examples

The following is sample output from the **show ip ddns update method** command:

```
Router# show ip ddns update method
Dynamic DNS Update Method: test
  Dynamic DNS update in IOS internal name cache
```

Related Commands

Command	Description
ip ddns update method	Specifies a method of DDNS updates of A and PTR RRs and the maximum interval between the updates.
show ip ddns update	Displays information about the DDNS updates.
show ip host-list	Displays the assigned hosts in a list.
update dns	Dynamically updates a DNS with A and PTR RRs for some address pools.

show ip dhcp binding

To display address bindings on the Cisco IOS Dynamic Host Configuration Protocol (DHCP) server, use the **show ip dhcp binding** command in user EXEC or privileged EXEC mode.

Cisco IOS Release 12.0(1)T, 12.2(28)SB, and Later Releases
show ip dhcp binding [*ip-address*]

Cisco IOS Release 12.2(33)SRC and Later 12.2SR Releases
show ip dhcp binding [**vrf** *vrf-name*] [*ip-address*]

Syntax Description

ip-address	(Optional) IP address of the DHCP client for which bindings will be displayed. If the *ip-address* argument is used with the **vrf** *vrf-name* option, the binding in the specified VPN routing and forwarding (VRF) instance is displayed.
vrf *vrf-name*	(Optional) Specifies the name of a VRF instance.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.0(15)T	The command was modified. Support to display allocated subnets was added to the output.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC. The **vrf** keyword and *vrf-name* argument were added.
12.2(33)SB9	This command was modified. The output was modified to display the option 82 sub-options of the remote ID and circuit ID.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Usage Guidelines

This command is used to display DHCP binding information for IP address assignment and subnet allocation. If a specific IP address is not specified, all address bindings are shown. Otherwise, only the binding for the specified client is displayed. The output that is generated for DHCP IP address assignment and subnet allocation is almost identical, except that subnet leases display an IP address followed by the subnet mask (which shows the size of the allocated subnet). Bindings for individual IP address display only an IP address and are not followed by a subnet mask.

Examples

IP Address Assignment Example

The following examples show the DHCP binding address parameters, including an IP address, an associated MAC address, a lease expiration date, the type of address assignment that has occurred, and the option 82 suboptions of the remote ID and circuit ID.

The table below describes the significant fields shown in the displays.

```
Router# show ip dhcp binding 192.0.2.2
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.0.2.2           aabb.cc00.0a00          Apr 28 2010 05:00 AM    Automatic
Remote id : 020a00001400006400000000
```

Table 16: show ip dhcp binding Field Descriptions

Field	Description
IP address	The IP address of the host as recorded on the DHCP server.
Client-ID/Hardware address/User name	The MAC address or client ID of the host as recorded on the DHCP server.
Lease expiration	The lease expiration date and time of the IP address of the host.
Type	The manner in which the IP address was assigned to the host.
Remote id	Information sent to the DHCP server using a suboption of the remote ID.

Subnet Allocation Example

The following example shows the subnet lease to MAC address mapping, the lease expiration, and the lease type (subnet lease bindings are configured to be automatically created and released by default):

```
Router# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.0.2.2/24        0063.6973.636f.2d64.    Mar 29 2003 04:36 AM    Automatic
                    656d.6574.6572.2d47.
                    4c4f.4241.4c
```

The table below describes the significant fields shown in the display.

Table 17: show ip dhcp binding Field Descriptions

Field	Description
IP address	The IP address of the host as recorded on the DHCP server. The subnet that follows the IP address (/26) in the example defines this binding as a subnet allocation binding.
Hardware address	The MAC address or client identifier of the host as recorded on the DHCP server.
Lease expiration	The lease expiration date and time of the IP address of the host.
Type	The manner in which the IP address was assigned to the host.

Related Commands

Command	Description
clear ip dhcp binding	Deletes an automatic address binding from the Cisco IOS DHCP server database.
show ip dhcp vrf	Displays VRF information on the DHCP server.

show ip dhcp conflict

To display address conflicts found by a Dynamic Host Configuration Protocol (DHCP) server when addresses are offered to the client, use the **show ip dhcp conflict**commandinuser EXEC or privileged EXEC mode.

show ip dhcp conflict [*vrf vrf-name*]

Syntax Description

vrf	(Optional) Displays virtual routing and forwarding (VRF) address conflicts found by the DHCP server.
vrf-name	(Optional) The VRF name.

Command Default

If you do not enter the IP address or VRF then all dhcp conflict related information is displayed.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.6	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Usage Guidelines

The server uses a ping operation to detect conflicts. The client uses gratuitous Address Resolution Protocol (ARP) to detect clients. If an address conflict is detected, the address is removed from the pool and the address is not assigned until an administrator resolves the conflict.

Examples

The following is sample output from the show ip dhcp conflict command, which shows the detection method and detection time for all IP addresses the DHCP server has offered that have conflicts with other devices:

```
Router#
show ip dhcp conflict
IP address    Detection method     Detection time         VRF
172.16.1.32   Ping                 Feb 16 1998 12:28 PM   vrf1
172.16.1.64   Gratuitous ARP       Feb 23 1998 08:12 AM   vrf2
```

The table below describes the fields shown in the display.

Table 18: show ip dhcp conflict Field Descriptions

Field	Description
IP address	The IP address of the host as recorded on the DHCP server.
Detection method	The manner in which the IP address of the hosts were found on the DHCP server. Can be a ping or a gratuitous ARP.
Detection time	The date and time when the conflict was found.
VRF	VRFs configured on the DHCP server.

The following is sample output from the **show ip dhcp conflict vrf** command:

```
Router#
show ip dhcp conflict vrf vrf1
IP address        Detection method   Detection time          VRF
172.16.1.32       Ping               Feb 15 2009 05:39 AM    vrf1
```

See the table below for the field description.

Related Commands

Command	Description
clear ip dhcp conflict	Clears an address conflict from the Cisco IOS DHCP server database.
ip dhcp ping packets	Specifies the number of packets a Cisco IOS DHCP server sends to a pool address as part of a ping operation.
ip dhcp ping timeout	Specifies how long a Cisco IOS DHCP server waits for a ping reply from an address pool.

show ip dhcp database

To display Dynamic Host Configuration Protocol (DHCP) server database agent information, use the **show ip dhcp database** command in privileged EXEC mode.

show ip dhcp database [*url*]

Syntax Description

url	(Optional) Specifies the remote file used to store automatic DHCP bindings. Following are the acceptable URL file formats: • tftp://host/filename • ftp://user:password@host/filename • rcp://user@host/filename • flash://filename • disk0://filename

Command Default

If a URL is not specified, all database agent records are shown. Otherwise, only information about the specified agent is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows all DHCP server database agent information. The table below describes the significant fields shown in the display.

```
Router# show ip dhcp database
URL       :    ftp://user:password@172.16.4.253/router-dhcp
Read      :    Dec 01 1997 12:01 AM
Written   :    Never
Status    :    Last read succeeded. Bindings have been loaded in RAM.
Delay     :    300 seconds
Timeout   :    300 seconds
Failures  :    0
Successes :    1
```

Table 19: show ip dhcp database Field Descriptions

Field	Description
URL	Specifies the remote file used to store automatic DHCP bindings. Following are the acceptable URL file formats: • tftp://host/filename • ftp://user:password@host/filename • rcp://user@host/filename • flash://filename • disk0://filename
Read	The last date and time bindings were read from the file server.
Written	The last date and time bindings were written to the file server.
Status	Indication of whether the last read or write of host bindings was successful.
Delay	The amount of time (in seconds) to wait before updating the database.
Timeout	The amount of time (in seconds) before the file transfer is aborted.
Failures	The number of failed file transfers.
Successes	The number of successful file transfers.

Related Commands

Command	Description
ip dhcp database	Configures a Cisco IOS DHCP server to save automatic bindings on a remote host called a database agent.

show ip dhcp import

To display the option parameters that were imported into the Dynamic Host Configuration Protocol (DHCP) server database, use the **show ip dhcp import** command in privileged EXEC command.

show ip dhcp import

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Imported option parameters are not part of the router configuration and are not saved in NVRAM. Thus, the **show ip dhcp import** command is necessary to display the imported option parameters.

Examples

The following is sample output from the **show ip dhcp import** command:

```
Router# show ip dhcp import
Address Pool Name:2
Domain Name Server(s): 10.1.1.1
NetBIOS Name Server(s): 10.3.3.3
```

The following example indicates the address pool name:

```
Address Pool Name:2
```

The following example indicates the imported values, which are domain name and NetBIOS name information:

```
Domain Name Server(s): 10.1.1.1
NetBIOS Name Server(s): 10.3.3.3
```

Related Commands

Command	Description
import all	Imports option parameters into the DHCP database.
show ip dhcp database	Displays Cisco IOS server database information.

show ip dhcp limit lease

To display the number of times the lease limit threshold has been violated, use the **show ip dhcp limit lease** command in user EXEC or privileged EXEC mode.

show ip dhcp limit lease [*type number*]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (?) online help function.
number	(Optional) Interface or subinterface number. For more information about the numbering system for your networking device, use the question mark (?) online help function.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.

Usage Guidelines

You can control the number of subscribers at the global level by using the **ip dhcp limit lease per interface** command and at the interface level by using the **ip dhcp limit lease**command. The **show ip dhcp limit lease** command displays the number of lease limit violations per interface or at the global level.

Examples

In the following example, the number of lease violations is displayed. If the **ip dhcp limit lease log** command is enabled, the show output will indicate that lease limit logging is enabled:

```
Router# show ip dhcp limit lease
DHCP limit lease logging is enabled
Interface        Count
Serial0/0.1      5
Serial1          3
```

Related Commands

Command	Description
ip dhcp limit lease	Limits the number of leases offered to DHCP clients per interface.
ip dhcp limit lease log	Enables DHCP lease violation logging when a DHCP lease limit threshold is exceeded.
ip dhcp limit lease per interface	Limits the number of DHCP leases offered to DHCP clients behind an ATM RBE unnumbered or serial unnumbered interface.

show ip dhcp pool

To display information about the Dynamic Host Configuration Protocol (DHCP) address pools, use the **show ip dhcp pool** command in user EXEC or privileged EXEC mode.

show ip dhcp pool [*name*]

Syntax Description

name	(Optional) Name of the address pool.

Command Default

If a pool name is not specified, information about all address pools is displayed.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was modified. The command output was enhanced to display information about excluded addresses in network pools.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

Use this command to determine the subnets allocated and to examine the current utilization level for the pool or all the pools if the *name* argument is not used.

Examples

The following example shows DHCP address pool information for an on-demand address pool (ODAP), pool 1. The table below describes the significant fields shown in the display.

```
Router# show ip dhcp pool 1
Pool 1:
 Utilization mark (high/low)    : 85 / 15
 Subnet size (first/next)       : 24 / 24 (autogrow)
 VRF name                       : abc
 Total addresses                : 28
 Leased addresses               : 11
 Pending event                  : none
 2 subnets are currently in the pool :
 Current index        IP address range           Leased addresses
 10.1.1.12            10.1.1.1 - 10.1.1.14       11
 10.1.1.17            10.1.1.17 - 10.1.1.30      0
 Interface Ethernet0/0 address assignment
   10.1.1.1 255.255.255.248
   10.1.1.17 255.255.255.248 secondary
```

The following example shows DHCP address pool information for a network pool, pool 2. The table below describes the significant fields shown in the display.

```
Router# show ip dhcp pool 2
Pool pool2 :
Utilization mark (high/low) : 80 / 70
```

```
Subnet size (first/next) : 0 / 0
Total addresses : 256
Leased addresses : 0
Excluded addresses : 2
Pending event : none
2 subnets are currently in the pool:
Current index   IP address range         Leased/Excluded/Total
10.0.2.1        10.0.2.1 - 10.0.2.254     0     / 1     / 254
10.0.4.1        10.0.4.1 - 10.0.4.2       0     / 1     / 2
```

Table 20: show ip dhcp pool Field Descriptions

Field	Description
Pool	The name of the pool.
Utilization mark (high/low)	The configured high and low utilization level for the pool.
Subnet size (first/next)	The size of the requested subnets.
VRF name	The VRF name to which the pool is associated.
Total addresses	The total number of addresses in the pool.
Leased addresses	The number of leased addresses in the pool.
Pending event	Displays any pending events.
2 subnets are currently in the pool	The number of subnets allocated to the address pool.
Current index	Displays the current index.
IP address range	The IP address range of the subnets.
Leased addresses	The number of leased addresses from each subnet.
Excluded addresses	The number of excluded addresses.
Interface Ethernet0/0 address assignment	The first line is the primary IP address of the interface. The second line is the secondary IP address of the interface. More than one secondary address on the interface is supported.

Related Commands

Command	Description
ip dhcp excluded-address	Specifies IP addresses that a DHCP server should not assign to DHCP clients.
ip dhcp pool	Configures a DHCP address pool on a DHCP server and enters DHCP pool configuration mode.
ip dhcp subscriber-id interface-name	Automatically generates a subscriber ID value based on the short name of the interface.
ip dhcp use subscriber-id client-id	Configures the DHCP server to globally use the subscriber identifier as the client identifier on all incoming DHCP messages.

show ip dhcp relay information trusted-sources

To display all interfaces configured to be a trusted source for the Dynamic Host Configuration Protocol (DHCP) relay information option, use the **show ip dhcp relay information trusted-sources** command in user EXEC or privileged EXEC mode.

show ip dhcp relay information trusted-sources

Syntax Description

This command has no arguments or keywords.

Command Modes

user EXEC privileged EXEC

Command History

Release	Modification
12.2	This command was introduced.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

The following is sample output when the **ip dhcp relay information trusted-sources** command is configured. Note that the display output lists the interfaces that are configured to be trusted sources.

```
Router# show ip dhcp relay information trusted-sources
List of trusted sources of relay agent information option:
Ethernet1/1       Ethernet1/2       Ethernet1/3       Serial4/1.1
Serial4/1.2       Serial4/1.3
```

The following is sample output when the **ip dhcp relay information trust-all**globalconfiguration command is configured. Note that the display output does not list the individual interfaces.

```
Router# show ip dhcp relay information trusted-sources
All interfaces are trusted source of relay agent information option Serial4/1.1
```

Related Commands

Command	Description
ip dhcp relay information trusted	Configures an interface as a trusted source of the DHCP relay agent information option.
ip dhcp relay information trust-all	Configures all interfaces on a router as trusted sources of the DHCP relay agent information option.

show ip dhcp server statistics

To display Dynamic Host Configuration Protocol (DHCP) server statistics, use the **show ip dhcp server statistics** command in privileged EXEC mode.

show ip dhcp server statistics

Syntax in Cisco IOS Release 12.2(33)SRC and Subsequent 12.2SR Releases
show ip dhcp server statistics [*type number*]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (?) online help function.
number	(Optional) Interface or subinterface number. For more information about the numbering system for your networking device, use the question mark (?) online help function.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	The *type* and *number* arguments were added. The command was enhanced to display interface level DHCP statistics.

Examples

The following example displays DHCP server statistics. The table below describes the significant fields in the display.

```
Router# show ip dhcp server statistics
Memory usage          40392
Address pools         3
Database agents       1
Automatic bindings    190
Manual bindings       1
Expired bindings      3
Malformed messages    0
Secure arp entries    1
Renew messages        0
Message               Received
BOOTREQUEST           12
DHCPDISCOVER          200
DHCPREQUEST           178
DHCPDECLINE           0
DHCPRELEASE           0
DHCPINFORM            0
Message               Sent
BOOTREPLY             12
DHCPOFFER             190
```

```
DHCPACK                 172
DHCPNAK                 6
```

Table 21: show ip dhcp server statistics Field Descriptions

Field	Description
Memory usage	The number of bytes of RAM allocated by the DHCP server.
Address pools	The number of configured address pools in the DHCP database.
Database agents	The number of database agents configured in the DHCP database.
Automatic bindings	The number of IP addresses that have been automatically mapped to the MAC addresses of hosts that are found in the DHCP database.
Manual bindings	The number of IP addresses that have been manually mapped to the MAC addresses of hosts that are found in the DHCP database.
Expired bindings	The number of expired leases.
Malformed messages	The number of truncated or corrupted messages that were received by the DHCP server.
Secure arp entries	The number of ARP entries that have been secured to the MAC address of the client interface.
Renew messages	The number of renew messages for a DHCP lease. The counter is incremented when a new renew message has arrived after the first renew message.
Message	The DHCP message type that was received by the DHCP server.
Received	The number of DHCP messages that were received by the DHCP server.
Sent	The number of DHCP messages that were sent by the DHCP server.

Related Commands

Command	Description
clear ip dhcp server statistics	Resets all Cisco IOS DHCP server counters.

show ip dhcp snooping

To display DHCP snooping configuration information, use the **show ip dhcp snooping** command in privileged EXEC mode.

show ip dhcp snooping

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS Release 15.2E	This command was modified. DHCP gleaning information was added to the **show ip dhcp snooping** command output, and this command was integrated into Cisco IOS Release 15.2E.
15.4(3)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Examples

The following is sample output for the **show ip dhcp snooping** command:

```
Device# show ip dhcp snooping

Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
43,47,136
DHCP snooping is operational on following VLANs:
136
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: 0c27.2497.bd80 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
GigabitEthernet1/0/1       yes        yes             unlimited
  Custom circuit-ids:
GigabitEthernet1/0/24      yes        yes             unlimited
  Custom circuit-ids:
GigabitEthernet1/1/1       yes        yes             unlimited
```

```
Custom circuit-ids:
```

*Table 22: **show ip dhcp snooping** Field Descriptions*

Field	Description
circuit-ID default format	The default format of the circuit-ID. The circuit-ID encodes a relay-agent-local identifier of the circuit from which a DHCP client-to-server packet was received. The DHCP Snooping feature encodes circuit ID and remote ID.
remote-id	Identifies the remote host end of the circuit. The remote-ID Option-82 sub-option is used by DHCP relay agents which have mechanisms to identify the remote host end of the circuit.
hwaddr	Client hardware address.
giaddr	Gateway IP address. The relay agent stores its own IP address in the Gateway IP address field of the DHCP packet.
DHCP snooping trust/rate	DHCP snooping configuration parameters such as rate Limit and interface status (Trusted or Untrusted) information.
Rate limit	DHCP packets' rate limit, calculated in packets per second (pps).

Related Commands

Command	Description
ip dhcp snooping	Enables DHCP snooping globally.
ip dhcp snooping binding	Sets up and generates a DHCP binding configuration to restore bindings across reboots.
ip dhcp snooping database	Configures the DHCP-snooping database.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
ip dhcp snooping packets	Enables DHCP snooping on the tunnel interface.
ip dhcp snooping verify mac-address	Verifies that the source MAC address in a DHCP packet matches the client hardware address on an untrusted port.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

show ip dhcp snooping binding

To display the DHCP snooping binding entries, use the **show ip dhcp snooping binding**command in privileged EXEC mode.

show ip dhcp snooping binding [*ip-address*] [*mac-address*] [**vlan** *vlan*] [**interface** *type number*]

Syntax Description

ip-address	(Optional) IP address for the binding entries.
mac-address	(Optional) MAC address for the binding entries.
vlan *vlan*	(Optional) Specifies a valid VLAN number; valid values are from 1 to 4094.
interface *type*	(Optional) Specifies the interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, and **tengigabitethernet**.
number	Module and port number.

Command Default

If no argument is specified, the switch displays the entire DHCP snooping binding table.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.4(3)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

DHCP snooping is enabled on a VLAN only if both the global snooping and the VLAN snooping are enabled.

Examples

This example shows how to display the DHCP snooping binding entries for a switch:

```
Router# show ip dhcp snooping binding

MacAddress      IP Address   Lease(seconds)  Type           VLAN   Interface
-----------     -----------  --------------  -------------  -----  --------------
0000.0100.0201  10.0.0.1     600             dhcp-snooping  100    FastEthernet3/1
```

This example shows how to display an IP address for DHCP snooping binding entries:

```
Router# show ip dhcp snooping binding 172.16.101.102
MacAddress      IP Address      Lease (seconds)  Type           VLAN   Interface
-----------     -----------     ---------------  -------------  -----  ------------
0000.0100.0201  172.16.101.102  1600             dhcp-snooping  100    FastEthernet3/1
```

This example shows how to display the MAC address for the DHCP snooping binding entries:

```
Router# show ip dhcp snooping binding 10.5.5.2 0002.b33f.3d5f
```

```
MacAddress          IpAddress  Lease(sec)  Type           VLAN  Interface
------------------  ---------  ----------  -------------  ----  ----------------
00:02:B3:3F:3D:5F   10.5.5.2   492         dhcp-snooping  99    FastEthernet6/36 Router#
```

This example shows how to display the DHCP snooping binding entries' MAC address for a specific VLAN:

```
Router# show ip dhcp snooping binding 10.5.5.2 0002.b33f.3d5f vlan 99

MacAddress         IpAddress  Lease(sec)  Type           VLAN  Interface
-----------------  ---------  ----------  -------------  ----  ----------------
00:02:B3:3F:3D:5F  10.5.5.2   479         dhcp-snooping  99    FastEthernet6/36
```

This example shows how to display the DHCP snooping binding entries on VLAN 100:

```
Router# show ip dhcp snooping binding vlan 100
MacAddress         IP Address  Lease(seconds)  Type           VLAN  Interface
-------------      ----------  --------------  -------------  ----  --------------
0000.0100.0201     10.0.0.1    1600            dhcp-snooping  100   FastEthernet3/1
```

This example shows how to display the DHCP snooping binding entries on Fast Ethernet interface 3/1:

```
Router# show ip dhcp snooping binding interface fastethernet3/1
MacAddress         IP Address  Lease(seconds)  Type           VLAN  Interface
-------------      ----------  --------------  -------------  ----  --------------
0000.0100.0201     10.0.0.1    1600            dhcp-snooping  100   FastEthernet3/1
```

The table below describes the fields in the **show ip dhcp snooping** command output.

Table 23: show ip dhcp snooping Command Output

Field	Description
Mac Address	Client hardware MAC address.
IP Address	Client IP address assigned from the DHCP server.
Lease (seconds)	IP address lease time.
Type	Binding type; statically configured from CLI or dynamically learned.
VLAN	VLAN number of the client interface.
Interface	Interface that connects to the DHCP client host.

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping binding	Sets up and generates a DHCP binding configuration to restore bindings across reboots.
ip dhcp snooping database	Configures the DHCP-snooping database.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.

Command	Description
ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
ip dhcp snooping packets	Enables DHCP snooping on the tunnel interface.
ip dhcp snooping verify mac-address	Verifies that the source MAC address in a DHCP packet matches the client hardware address on an untrusted port.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

show ip dhcp snooping database

To display the status of the DHCP snooping database agent, use the **show ip dhcp snooping database**command in privileged EXEC mode.

show ip dhcp snooping database [**detail**]

Syntax Description

detail	(Optional) Provides additional operating state and statistics information.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.4(3)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Examples

This example shows how to display the DHCP snooping database:

```
Router# show ip dhcp snooping database
Agent URL :
Write delay Timer : 300 seconds
Abort Timer : 300 seconds
Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running
Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.
Total Attempts       :        0   Startup Failures :        0
Successful Transfers :        0   Failed Transfers :        0
Successful Reads     :        0   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :        0
Media Failures       :        0
```

This example shows how to view additional operating statistics:

```
Router# show ip dhcp snooping database detail

Agent URL : tftp://10.1.1.1/directory/file
Write delay Timer : 300 seconds
Abort Timer : 300 seconds
Agent Running : No
Delay Timer Expiry : 7 (00:00:07)
Abort Timer Expiry : Not Running
Last Succeded Time : None
Last Failed Time : 17:14:25 UTC Sat Jul 7 2001
Last Failed Reason : Unable to access URL.
Total Attempts       :       21   Startup Failures :        0
Successful Transfers :        0   Failed Transfers :       21
```

```
Successful Reads     :        0   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :       21
Media Failures       :        0
First successful access: Read
Last ignored bindings counters :
Binding Collisions    :        0   Expired leases    :        0
Invalid interfaces    :        0   Unsupported vlans :        0
Parse failures        :        0
Last Ignored Time : None
Total ignored bindings counters:
Binding Collisions    :        0   Expired leases    :        0
Invalid interfaces    :        0   Unsupported vlans :        0
Parse failures        :        0
```

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping binding	Sets up and generates a DHCP binding configuration to restore bindings across reboots.
ip dhcp snooping database	Configures the DHCP-snooping database.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
ip dhcp snooping packets	Enables DHCP snooping on the tunnel interface.
ip dhcp snooping verify mac-address	Verifies that the source MAC address in a DHCP packet matches the client hardware address on an untrusted port.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

show ip dhcp vrf

To display the VPN routing and forwarding (VRF) instance information on the Cisco IOS Dynamic Host Configuration Protocol (DHCP) server, use the **show ip dhcp vrf** command in user EXEC or privileged EXEC mode.

show ip dhcp vrf *vrf-name* **binding** {*ip-address* | *****}

Syntax Description

vrf-name	Specifies the VRF name.
binding	Displays DHCP VRF bindings.
ip-address	Specifies the IP address of the DHCP client for which bindings will be displayed.
*****	Displays all bindings in the specified VRF instance.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.

Usage Guidelines

This command is used to display VRF information on the Cisco IOS DHCP server. If an IP address is specified, VRF information for the specific client is displayed. If an asterisk (*) is specified, then VRF information for all the clients is displayed.

Examples

The following example shows the bindings associated with the VRF instance named red:

```
Router# show ip dhcp vrf red binding *
Bindings from VRF pool red:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.0.2.0           0063.6973.636f.2d30.    Mar 11 2007 04:36 AM    Automatic
                    3030.312e.3030.3131.
                    2e30.3032.342d.4574.
                    302f.30
192.0.2.1           0063.6973.636f.2d30.    Mar 11 2007 04:37 AM    Automatic
                    3032.322e.3030.3333.
                    2e30.3034.342d.4574.
                    302f.30
```

The following example shows the bindings associated with a specific IP address in the VRF instance named red:

```
Router# show ip dhcp vrf red binding 192.0.2.2
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.0.2.2           0063.6973.636f.2d30.    Mar 11 2007 04:37 AM    Automatic
```

```
3032.322e.3030.3333.
2e30.3034.342d.4574.
302f.30
```

The table below describes the significant fields shown in the displays.

Table 24: show ip dhcp vrf Field Descriptions

Field	Description
IP address	The IP address of the host as recorded on the DHCP server.
Hardware address	The MAC address or client identifier of the host as recorded on the DHCP server.
Lease expiration	The lease expiration date and time of the IP address of the host.
Type	The manner in which the IP address was assigned to the host.

Related Commands

Command	Description
clear ip dhcp binding	Deletes an automatic address binding from the Cisco IOS DHCP server database.
show ip dhcp binding	Displays address bindings on the Cisco IOS DHCP server.

show ip dns name-list

To display a particular Domain Name System (DNS) name list or all configured DNS name lists, use the **show ip dns name-list** command in privileged EXEC mode.

show ip dns name-list [*name-list-number*]

Syntax Description

name-list-number	(Optional) Integer from 1 to 500 that identifies a DNS name list.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Display a DNS name list to view the ordered list of pattern-matching rules it defines. Each rule in the name list specifies a regular expression and the type of action to be taken if the query hostname matches that expression.

If the output from this command extends beyond the bottom of the screen, press the Space bar to continue or press the Q-key to terminate command output.

Examples

The following is sample output from the **show ip dns name-list** command:

```
Router# show ip dns name-list

ip dns name-list 1
deny WWW.EXAMPLE1.COM
permit WWW.EXAMPLE.com
ip dns name-list 2
deny WWW.EXAMPLE2.COM
permit WWW.EXAMPLE3.COM
```

The table below describes the significant fields shown for each DNS name list in the display.

Table 25: show ip dns name-list Field Descriptions

Field	Description
name-list	Integer that identifies the DNS name list. Configured using the **ip dns name-list** command.
deny	Regular expression, case-insensitive, to be compared to the DNS query hostname. If the DNS query hostname matches this expression, the name list matching will terminate immediately and the name list will be determined to have not matched the hostname. A deny clause is configured by using the **ip dns name-list** command.

Field	Description
permit	Regular expression in domain name format (a sequence of case-insensitive ASCII labels separated by dots), case-insensitive, and to be compared to the DNS query hostname. If the DNS query hostname matches this expression, the name list matching will terminate immediately and the name-list will be determined to have matched the hostname. A permit clause is configured by using the **ip dns name-list** command.

Related Commands

Command	Description
debug ip dns name-list	Enables debugging output for DNS name list events.
ip dns name-list	Defines a list of pattern-matching rules in which each rule permits or denies the use of a DNS view list member to handle a DNS query based on whether the query hostname matches the specified regular expression.

show ip dns primary

To display the authority record parameters configured for the Domain Name System (DNS) server, use the **show ip dns primary** command in user EXEC or privileged EXEC mode.

show ip dns primary

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.0	This command was introduced.

Examples

The following example shows how to configure the router as a DNS server and then display the authority record parameters for the DNS server:

```
Router(conf)# ip dns server
Router(conf)# ip dns primary example.com soa ns1.example.com mb1.example.com
Router(conf)# ip host example.com ns ns1.example.com
Router(conf)# ip host ns1.example.com 209.165.201.1
Router(conf)# exit
Router# show ip dns primary
Primary for zone example.com:
  SOA information:
  Zone primary (MNAME): ns1.example.com
  Zone contact (RNAME): mb1.example.com
  Refresh (seconds):    21600
  Retry (seconds):      900
  Expire (seconds):     7776000
  Minimum (seconds):    86400
```

The table below describes the significant fields shown in the display.

Table 26: show ip dns primary Field Descriptions

Field	Description
Zone primary (MNAME)	Authoritative name server.
Zone contact (RNAME)	DNS mailbox of administrative contact.
Refresh (seconds)	Refresh time in seconds. This time interval that must elapse between each poll of the primary by the secondary name server.
Retry (seconds)	Refresh retry time in seconds. This time interval must elapse between successive connection attempts by the secondary to reach the primary name server in case the first attempt failed.
Expire (seconds)	Authority expire time in seconds. The secondary expires its data if it cannot reach the primary name server within this time interval.

Field	Description
Minimum (seconds)	Minimum Time to Live (TTL) in seconds for zone information. Other servers should cache data from the name server for this length of time.

Related Commands

Command	Description
ip dns primary	Configures router authority parameters for the DNS name server,for the DNS name server.
ip dns server	Enables the DNS server on the router.
ip host	Defines static hostname-to-address mappings in the DNS hostname cache for a DNS view.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.

show ip dns statistics

To display packet statistics for the Domain Name System (DNS) server, use the **show ip dns statistics** command in user EXEC or privileged EXEC mode.

show ip dns statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Use this command to display the number of DNS requests received and dropped by the DNS server and the number of DNS responses sent by the DNS server.

Examples

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

```
Router#
show ip dns statistics
DNS requests received = 818725 ( 818725 + 0 )
DNS requests dropped = 0 ( 0 + 0 )
DNS responses replied = 0 ( 0 + 0 )
Forwarder queue statistics:
Current size = 0
Maximum size = 400
Drops = 804613
Director queue statistics:
Current size = 0
Maximum size = 0
Drops = 0
```

The table below describes the significant fields shown in the display.

Table 27: show ip dns statistics Field Descriptions

Field	Description
DNS requests received	Total number of DNS requests received by the DNS server. Additional details are displayed in parenthesis: • Number of UDP packets received • Number of TCP packets received
DNS requests dropped	Total number of DNS requests discarded by the DNS server. Additional details are displayed in parenthesis: • Number of UDP packets dropped • Number of TCP packets dropped

Field	Description
DNS responses replied	Total number of DNS responses sent by the DNS server. Additional details are displayed in parenthesis: • Number of UDP packets dropped • Number of TCP packets dropped
Current size	Displays the current size of the queue counter.
Maximum size	Displays the maximum size of the queue counter reached since the reload. **Note** Whenever you change the queue size, the Maximum size counter will be reset to zero.
Drops	Displays the number of packets dropped when a queue function fails. **Note** Whenever you change the queue size, the Drops counter will be reset to zero.

show ip dns view

To display configuration information about a Domain Name System (DNS) view or about all configured DNS views, including the number of times the DNS view was used, the DNS resolver settings, the DNS forwarder settings, and whether logging is enabled, use the **show ip dns view** command in privileged EXEC mode.

show ip dns view [**vrf** *vrf-name*] [**default***view-name*]

Syntax Description

vrf *vrf-name*	(Optional) The *vrf-name* argument specifies the name of the Virtual Private Network (VPN) routing and forwarding (VRF) instance associated with the DNS view. Default is the global VRF (that is, the VRF whose name is a NULL string). **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.
default	(Optional) Specifies that the DNS view is unnamed. By default all configured DNS views are displayed.
view-name	(Optional) Name of the DNS view whose information is to be displayed. Default is all configured DNS views. **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Display DNS view information to view its DNS resolver settings, DNS forwarder settings, and whether logging is enabled.

If the output from this command extends beyond the bottom of the screen, press the Space bar to continue or press the Q-key to terminate command output.

Because different DNS views can be associated with the same VRF, omitting both the **default** keyword and the *view-name* argument causes this command to display information about all the views associated with the global or named VRF.

Examples

The following is sample output from the **show ip dns view** command:

```
Router# show ip dns view

DNS View default parameters:
Logging is on (view used 102 times)
DNS Resolver settings:
  Domain lookup is enabled
```

```
  Default domain name: example.com
  Domain search list: example1.com example2.com example3.com
  Domain name for multicast lookups: 192.0.2.10
  Lookup timeout: 7 seconds
  Lookup retries: 5
  Domain name-servers:
    192.168.2.204
    192.168.2.205
    192.168.2.206
  Round-robin'ing of IP addresses is enabled
DNS Server settings:
  Forwarding of queries is enabled
  Forwarder addresses:
    192.168.2.11
    192.168.2.12
    192.168.2.13
  Forwarder source interface: FastEthernet0/1
DNS View user5 parameters:
Logging is on (view used 10 times)
DNS Resolver settings:
  Domain lookup is enabled
  Default domain name: example5.net
  Domain search list:
  Lookup timeout: 3 seconds
  Lookup retries: 2
  Domain name-servers:
    192.168.2.104
    192.168.2.105
DNS Server settings:
  Forwarding of queries is enabled
  Forwarder addresses:
    192.168.2.204
DNS View user1 vrf vpn101 parameters:
Logging is on (view used 7 times)
DNS Resolver settings:
  Domain lookup is enabled
  Default domain name: example1.com
  Domain search list:
  Lookup timeout: 3 seconds
  Lookup retries: 2
  Domain name-servers:
    192.168.2.100
DNS Server settings:
  Forwarding of queries is enabled
  Forwarder addresses:
    192.168.2.200 (vrf vpn201)
```

The table below describes the significant fields shown for each DNS view in the display.

Table 28: show ip dns view Field Descriptions

Field	Description
Logging	Logging of a system message logging (syslog) message each time the DNS view is used. Configured using the **logging** command. **Note** If logging is enabled for a DNS view, the **show ip dns view** command output includes the number of times the DNS view has been used in responding to DNS queries.

Field	Description
Domain lookup	DNS lookup to resolve hostnames for internally generated queries. Enabled or disabled using the **domain lookup** command.
Default domain name	Default domain to append to hostnames without a dot. Configured using the **domain name** command.
Domain search list	List of domain names to try for hostnames without a dot. Configured using the **domain list** command.
Domain name for multicast lookups	IP address to use for multicast address lookups. Configured using the **domain multicast** command.
Lookup timeout	Time (in seconds) to wait for DNS response after sending or forwarding a query. Configured using the **domain timeout** command.
Lookup retries	Number of retries when sending or forwarding a query. Configured using the **domain retry** command.
Domain name-servers	Up to six name servers to use to resolve domain names for internally generated queries. Configured using the **domain name-server** command.
Resolver source interface	Source interface to use to resolve domain names for internally generated queries. Configured using the **ip domain lookup source-interfac**e global command.
Round robin'ing of IP addresses	Round-robin rotation of the IP addresses associated with the hostname in cache each time hostnames are looked up. Enabled or disabled using the **domain round-robin** command.
Forwarding of queries	Forwarding of incoming DNS queries. Enabled or disabled using the **dns forwarding** command.
Forwarder addresses	Up to six IP address to use to forward incoming DNS queries. Configured using the **dns forwarder** command.
Forwarder source-interface	Source interface to use to forward incoming DNS queries. Configured using the **dns forwarding source-interface** command.

show ip dns view-list

To display information about a Domain Name System (DNS) view list or about all configured DNS view lists, use the **show ip dns view-list** command in privileged EXEC mode.

show ip dns view-list [*view-list-name*]

Syntax Description

view-list-name	(Optional) Name of the DNS view list. Default is all configured DNS view lists.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

If the output from this command extends beyond the bottom of the screen, press the Space bar to continue or press the Q-key to terminate command output.

IP DNS view lists are defined by using the **ip dns view-list** command.

To display information about how DNS view lists are applied, use the **show running-config** command:

- The default DNS view list, if configured, is listed in the default DNS view information (in the **ip dns view default** command information, as the argument for the **ip dns server view-group** command).
- Any DNS view lists attached to interfaces are listed in the information for each individual interface (in the **interface** command information for that interface, as the argument for the **ip dns view-group** command).

Examples

The following is sample output from the **show ip dns view-list** command:

```
Router# show ip dns view-list

View-list userlist1:
  View user1 vrf vpn101:
    Evaluation order: 10
    Restrict to source ACL: 71
    Restrict to ip dns name-list: 151
  View user2 vrf vpn102:
    Evaluation order: 20
    Restrict to source ACL: 71
    Restrict to ip dns name-list: 151
  View user3 vrf vpn103:
    Evaluation order: 30
    Restrict to source ACL: 71
    Restrict to ip dns name-list: 151
View-list userlist2:
  View user1 vrf vpn101:
    Evaluation order: 10
    Restrict to ip dns name-list: 151
  View user2 vrf vpn102:
    Evaluation order: 20
    Restrict to ip dns name-list: 151
```

```
View user3 vrf vpn103:
  Evaluation order: 30
  Restrict to ip dns name-list: 151
```

The table below describes the significant fields shown for each DNS view list in the display.

Table 29: show ip dns view-list Field Descriptions

Field	Description
View-list	A DNS view list name. Configured using the **ip dns view** command.
View	A DNS view that is a member of this DNS view list. If the view is associated with a VRF, the VRF name is also displayed. Configured using the **ip dns view-list** command.
Evaluation order	Indication of the order in which the DNS view is checked, relative to other DNS views in the same DNS view list. Configured using the **view** command.
Restrict	Usage restrictions for the DNS view when it is a member of this DNS view list. Configured using the **restrict name-group** command or the **restrict source access-group** command.

Related Commands

Command	Description
debug ip dns view-list	Enables debugging output for DNS view list events.
interface	Configures an interface type and enter interface configuration mode so that the specific interface can be configured.
ip dns server view-group	Specifies the DNS view list to use to determine which DNS view to use handle incoming queries that arrive on an interface not configured with a DNS view list.
ip dns view-group	Specifies the DNS view list to use to determine which DNS view to use to handle incoming DNS queries that arrive on a specific interface.
ip dns view-list	Enters DNS view list configuration mode so that DNS views can be added to or removed from the ordered list of DNS views.
show running-config	Displays the contents of the currently running configuration file of your routing device.

show ip host-list

To display the assigned hosts in a list, use the **show ip host-list** command in privileged EXEC mode.

show ip host-list [*host-list-name*]

Syntax Description

host-list-name	(Optional) Name assigned to the list of hosts.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)YA	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Examples

The following is sample output from the **show ip host-list** command example for the abctest group:

```
Router# show ip host-list abctest
Host list: abctest
 ddns.abc.test
 10.2.3.4
 ddns2.unit.test
 10.3.4.5
 ddns3.com
 10.3.3.3
 e.org
 1.org.2.org
 3.com
 10.5.5.5 (VRF: def)
```

Related Commands

Command	Description
debug dhcp	Displays debugging information about the DHCP client and monitors the status of DHCP packets.
debug ip ddns update	Enables debugging for DDNS updates.
debug ip dhcp server	Enables DHCP server debugging.
host (host-list)	Specifies a list of hosts that will receive DDNS updates of A and PTR RRs.
ip ddns update hostname	Enables a host to be used for DDNS updates of A and PTR RRs.
ip ddns update method	Specifies a method of DDNS updates of A and PTR RRs and the maximum interval between the updates.
ip dhcp client update dns	Enables DDNS updates of A RRs using the same hostname passed in the hostname and FQDN options by a client.

Command	Description
ip dhcp-client update dns	Enables DDNS updates of A RRs using the same hostname passed in the hostname and FQDN options by a client.
ip dhcp update dns	Enables DDNS updates of A and PTR RRs for most address pools.
ip host-list	Specifies a list of hosts that will receive DDNS updates of A and PTR RRs.
show ip ddns update	Displays information about the DDNS updates.
show ip ddns update method	Displays information about the DDNS update method.
update dns	Dynamically updates a DNS with A and PTR RRs for some address pools.

show ip interface

To display the usability status of interfaces configured for IP, use the **show ip interface** command in privileged EXEC mode.

show ip interface [*type number*] [**brief**]

Syntax Description

type	(Optional) Interface type.
number	(Optional) Interface number.
brief	(Optional) Displays a summary of the usability status information for each interface.

Command Default

The full usability status is displayed for all interfaces configured for IP.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0(3)T	The command output was modified to show the status of the **ip wccp redirect out** and **ip wccp redirect exclude add in** commands.
12.2(14)S	The command output was modified to display the status of NetFlow on a subinterface.
12.2(15)T	The command output was modified to display the status of NetFlow on a subinterface.
12.3(6)	The command output was modified to identify the downstream VPN routing and forwarding (VRF) instance in the output.
12.3(14)YM2	The command output was modified to show the usability status of interfaces configured for Multiprocessor Forwarding (MPF) and implemented on the Cisco 7301 and Cisco 7206VXR routers.
12.2(14)SX	This command was implemented on the Supervisor Engine 720.
12.2(17d)SXB	This command was integrated into Cisco IOS 12.2(17d)SXB on the Supervisor Engine 2, and the command output was changed to include NDE for hardware flow status.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	The command output was modified to display information about the Unicast Reverse Path Forwarding (RPF) notification feature.

Release	Modification
12.4(20)T	The command output was modified to display information about the Unicast RPF notification feature.
12.2(33)SXI2	This command was modified. The command output was modified to display information about the Unicast RPF notification feature.
Cisco IOS XE Release 2.5	This command was modified. This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.9S	This command was implemented on Cisco 4400 Series ISRs.

Usage Guidelines

The Cisco IOS software automatically enters a directly connected route in the routing table if the interface is usable (which means that it can send and receive packets). If an interface is not usable, the directly connected routing entry is removed from the routing table. Removing the entry lets the software use dynamic routing protocols to determine backup routes to the network, if any.

If the interface can provide two-way communication, the line protocol is marked "up." If the interface hardware is usable, the interface is marked "up."

If you specify an optional interface type, information for that specific interface is displayed. If you specify no optional arguments, information on all the interfaces is displayed.

When an asynchronous interface is encapsulated with PPP or Serial Line Internet Protocol (SLIP), IP fast switching is enabled. A **show ip interface** command on an asynchronous interface encapsulated with PPP or SLIP displays a message indicating that IP fast switching is enabled.

You can use the **show ip interface brief** command to display a summary of the router interfaces. This command displays the IP address, the interface status, and other information.

The **show ip interface brief** command does not display any information related to Unicast RPF.

Examples

The following example shows configuration information for interface Gigabit Ethernet 0/3. In this example, the IP flow egress feature is configured on the output side (where packets go out of the interface), and the policy route map named PBRNAME is configured on the input side (where packets come into the interface).

```
Router# show running-config interface gigabitethernet 0/3
interface GigabitEthernet0/3
 ip address 10.1.1.1 255.255.0.0
 ip flow egress
 ip policy route-map PBRNAME
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
end
```

The following example shows interface information on Gigabit Ethernet interface 0/3. In this example, MPF is enabled, and both Policy Based Routing (PBR) and NetFlow features are not supported by MPF and are ignored.

```
Router# show ip interface gigabitethernet 0/3
```

```
GigabitEthernet0/3 is up, line protocol is up
  Internet address is 10.1.1.1/16
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Feature Fast switching turbo vector
  IP VPN Flow CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is enabled, using route map PBR
  Network address translation is disabled
  BGP Policy Mapping is disabled
  IP Multi-Processor Forwarding is enabled
     IP Input features, "PBR",
         are not supported by MPF and are IGNORED
     IP Output features, "NetFlow",
         are not supported by MPF and are IGNORED
```

The following example identifies a downstream VRF instance. In the example, "Downstream VPN Routing/Forwarding "D"" identifies the downstream VRF instance.

```
Router# show ip interface virtual-access 3
Virtual-Access3 is up, line protocol is up
  Interface is unnumbered. Using address of Loopback2 (10.0.0.8)
  Broadcast address is 255.255.255.255
  Peer address is 10.8.1.1
  MTU is 1492 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is enabled
  IP Flow switching is disabled
  IP CEF switching is enabled
```

```
  IP Feature Fast switching turbo vector
  IP VPN CEF switching turbo vector
  VPN Routing/Forwarding "U"
  Downstream VPN Routing/Forwarding "D"
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

The following example shows the information displayed when Unicast RPF drop-rate notification is configured:

```
Router# show ip interface ethernet 2/3
Ethernet2/3 is up, line protocol is up
  Internet address is 10.0.0.4/16
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP Flow switching is disabled
  IP CEF switching is disabled
  IP Null turbo vector
  IP Null turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are No CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

Unicast RPF Information

```
  Input features: uRPF
  IP verify source reachable-via RX, allow default
   0 verification drops
   0 suppressed verification drops
   0 verification drop-rate
Router#
```

The following example shows how to display the usability status for a specific VLAN:

```
Router# show ip interface vlan 1
Vlan1 is up, line protocol is up
  Internet address is 10.0.0.4/24
  Broadcast address is 255.255.255.255
Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Fast switching turbo vector
  IP Normal CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
  Sampled Netflow is disabled
  IP multicast multilayer switching is disabled
  Netflow Data Export (hardware) is enabled
```

The table below describes the significant fields shown in the display.

Table 30: show ip interface Field Descriptions

Field	Description
Virtual-Access3 is up	Shows whether the interface hardware is usable (up). For an interface to be usable, both the interface hardware and line protocol must be up.
Broadcast address is	Broadcast address.
Peer address is	Peer address.
MTU is	MTU value set on the interface, in bytes.
Helper address	Helper address, if one is set.
Directed broadcast forwarding	Shows whether directed broadcast forwarding is enabled.
Outgoing access list	Shows whether the interface has an outgoing access list set.
Inbound access list	Shows whether the interface has an incoming access list set.
Proxy ARP	Shows whether Proxy Address Resolution Protocol (ARP) is enabled for the interface.
Security level	IP Security Option (IPSO) security level set for this interface.
Split horizon	Shows whether split horizon is enabled.
ICMP redirects	Shows whether redirect messages will be sent on this interface.
ICMP unreachables	Shows whether unreachable messages will be sent on this interface.
ICMP mask replies	Shows whether mask replies will be sent on this interface.
IP fast switching	Shows whether fast switching is enabled for this interface. It is generally enabled on serial interfaces, such as this one.
IP Flow switching	Shows whether Flow switching is enabled for this interface.
IP CEF switching	Shows whether Cisco Express Forwarding switching is enabled for the interface.
Downstream VPN Routing/Forwarding "D"	Shows the VRF instance where the PPP peer routes and AAA per-user routes are being installed.
IP multicast fast switching	Shows whether multicast fast switching is enabled for the interface.
IP route-cache flags are Fast	Shows whether NetFlow is enabled on an interface. Displays "Flow init" to specify that NetFlow is enabled on the interface. Displays "Ingress Flow" to specify that NetFlow is enabled on a subinterface using the **ip flow ingress**command. Shows "Flow" to specify that NetFlow is enabled on a main interface using the **ip route-cache flow** command.

Field	Description
Router Discovery	Shows whether the discovery process is enabled for this interface. It is generally disabled on serial interfaces.
IP output packet accounting	Shows whether IP accounting is enabled for this interface and what the threshold (maximum number of entries) is.
TCP/IP header compression	Shows whether compression is enabled.
WCCP Redirect outbound is disabled	Shows the status of whether packets received on an interface are redirected to a cache engine. Displays "enabled" or "disabled."
WCCP Redirect exclude is disabled	Shows the status of whether packets targeted for an interface will be excluded from being redirected to a cache engine. Displays "enabled" or "disabled."
Netflow Data Export (hardware) is enabled	NetFlow Data Expert (NDE) hardware flow status on the interface.

The table below describes the significant fields shown in the display.

Display a Summary of Interfaces on Cisco 4400 Series ISR: Example

The following is a sample out of the **show ip interface brief** command displaying a summary of the interfaces and their status on the device.

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/1   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/2   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/3   unassigned      YES NVRAM  down                  down
Serial1/0/0            unassigned      YES unset  down                  down
GigabitEthernet0       unassigned      YES NVRAM  up                    up
```

Display a Summary of the Usability Status: Example

The following example shows how to display a summary of the usability status information for each interface:

```
Router# show ip interface brief
Interface     IP-Address     OK?  Method  Status                  Protocol
Ethernet0     10.108.00.5    YES  NVRAM   up                      up
Ethernet1     unassigned     YES  unset   administratively down   down
Loopback0     10.108.200.5   YES  NVRAM   up                      up
Serial0       10.108.100.5   YES  NVRAM   up                      up
Serial1       10.108.40.5    YES  NVRAM   up                      up
Serial2       10.108.100.5   YES  manual  up                      up
Serial3       unassigned     YES  unset   administratively down   down
```

Table 31: show ip interface brief Field Descriptions

Field	Description
Interface	Type of interface.
IP-Address	IP address assigned to the interface.
OK?	"Yes" means that the IP Address is valid. "No" means that the IP Address is not valid.
Method	The Method field has the following possible values: • RARP or SLARP--Reverse Address Resolution Protocol (RARP) or Serial Line Address Resolution Protocol (SLARP) request. • BOOTP--Bootstrap protocol. • TFTP--Configuration file obtained from the TFTP server. • manual--Manually changed by the command-line interface. • NVRAM--Configuration file in NVRAM. • IPCP--**ip address negotiated** command. • DHCP--**ip address dhcp** command. • unset--Unset. • other--Unknown.
Status	Shows the status of the interface. Valid values and their meanings are: • up--Interface is up. • down--Interface is down. • administratively down--Interface is administratively down.
Protocol	Shows the operational status of the routing protocol on this interface.

Related Commands

Command	Description
ip address	Sets a primary or secondary IP address for an interface.
ip vrf autoclassify	Enables VRF autoclassify on a source interface.
match ip source	Specifies a source IP address to match to required route maps that have been set up based on VRF connected routes.
route-map	Defines the conditions for redistributing routes from one routing protocol into another or to enable policy routing.
set vrf	Enables VPN VRF selection within a route map for policy-based routing VRF selection.

Command	Description
show ip arp	Displays the ARP cache, in which SLIP addresses appear as permanent ARP table entries.
show route-map	Displays static and dynamic route maps.

show ip interface unnumbered

To display the status of unnumbered interface support on interfaces configured for IP, use the **show ip interface unnumbered** command in privileged EXEC mode.

show ip interface *type number* **unnumbered** [**detail**]

Syntax Description

type number	Interface type and number.
detail	(Optional) Displays detailed IP unnumbered status information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)SY	This command was introduced.

Usage Guidelines

The interface that borrows its address from one of the device's other functional interfaces is called the *unnumbered interface*. The IP unnumbered interfaces help in conserving network and address space. Use the **show ip interface unnumbered** command to display the status of unnumbered interface support on both numbered and unnumbered interfaces.

Examples

The following is sample output from the **show ip interface unnumbered** command on a numbered interface. The output fields are self-explanatory.

```
Device(#) show ip interface loopback0 unnumbered

Number of unnumbered interfaces with polling: 10
Number of IP addresses processed for polling: 15
Number of IP addresses in queue for polling: 4
```

The following is sample output from the **show ip interface unnumbered** command on a numbered interface when the **detail** keyword is specified:

```
Device(#) show ip interface loopback0 unnumbered detail

Number of unnumbered interfaces with polling: 10
Number of IP addresses processed for polling: 15
Last 10 IP addresses processed for polling:
  10.1.1.7
  10.1.1.8
  10.1.1.9
  10.1.1.10
  10.1.1.11
  10.1.1.12
  10.1.1.13
  10.1.1.14
  10.1.1.15
  10.1.1.16
Number of IP addresses in queue for polling: 4 (high water mark: 5)
  10.1.1.17
  10.1.1.18
  10.1.1.19
```

```
  10.1.1.20
```

The following is sample output from the **show ip interface unnumbered** command on an unnumbered interface when polling is enabled:

```
Device(#) show ip interface Ethernet1/0 unnumbered

Numbered interface: Loopback0
Number of IP addresses processed for polling: 15
```

The following is sample output from the **show ip interface unnumbered** *type number* **detail** command on an unnumbered interface when polling is enabled:

```
Device(#) show ip interface Gigabitethernet1/1 unnumbered detail

Numbered interface: Loopback0
Number of IP addresses processed for polling: 15
Last 10 IP addresses processed for polling:
  10.1.1.7
  10.1.1.9
  10.1.1.10
  10.1.1.11
  10.1.1.12
  10.1.1.13
  10.1.1.14
  10.1.1.15
  10.1.1.16
```

Related Commands

Command	Description
ip unnumbered	Enables IP processing on an interface without assigning an explicit IP address to the interface.

show ip irdp

To display ICMP Router Discovery Protocol (HRDP) values, use the **show ip irdp** command in EXEC mode.

show ip irdp

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

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

```
Router# show ip irdp
Ethernet 0 has router discovery enabled
Advertisements will occur between every 450 and 600 seconds.
Advertisements are valid for 1800 seconds.
Default preference will be 100.
 --More--
Serial 0 has router discovery disabled
 --More--
Ethernet 1 has router discovery disabled
```

As the display shows, **show ip irdp**output indicates whether router discovery has been configured for each router interface, and it lists the values of router discovery configurables for those interfaces on which router discovery has been enabled. Explanations for the less obvious lines of output in the display are as follows:

```
Advertisements will occur between every 450 and 600 seconds.
```

This indicates the configured minimum and maximum advertising interval for the interface.

```
Advertisements are valid for 1800 seconds.
```

This indicates the configured holdtime values for the interface.

```
Default preference will be 100.
```

This indicates the configured (or in this case default) preference value for the interface.

Related Commands

Command	Description
ip irdp	Enables IRDP processing on an interface.



show ip masks through vrf DHCP pool

- show ip masks, on page 784
- show ip nat limits all-host, on page 785
- show ip nat limits all-vrf, on page 787
- show ip nat nvi statistics, on page 789
- show ip nat nvi translations, on page 791
- show ip nat redundancy, on page 793
- show ip nat statistics, on page 795
- show ip nat statistics platform, on page 797
- show ip nat translations, on page 799
- show ip nat translation entry-id platform, on page 803
- show ip nat translations redundancy, on page 804
- show ip nhrp, on page 805
- show ip nhrp group-map, on page 816
- show ip nhrp multicast, on page 818
- show ip nhrp multicast stats, on page 821
- show ip nhrp nhs, on page 822
- show ip nhrp redirect, on page 825
- show ip nhrp summary, on page 827
- show ip nhrp traffic, on page 828
- show ip route dhcp, on page 830
- show ip snat, on page 832
- show ip source binding, on page 833
- show ip verify source, on page 835
- show ipv6 dhcp, on page 838
- show ipv6 dhcp binding, on page 839
- show ipv6 dhcp conflict, on page 842
- show ipv6 dhcp database, on page 843
- show ipv6 dhcp guard policy, on page 845
- show ipv6 dhcp-ldra, on page 847
- show ipv6 dhcp pool, on page 850
- show ipv6 dhcp interface, on page 852
- show ipv6 dhcp relay binding, on page 855
- show ipv6 dhcp route, on page 857

- show ip nat pool platform, on page 858
- show ip nat pool name platform, on page 859
- show ipv6 nat statistics, on page 860
- show ipv6 nat translations, on page 861
- show logging ip access-list, on page 863
- show mdns cache, on page 865
- show mdns cache mac, on page 867
- show mdns cache static, on page 869
- show mdns requests, on page 871
- show mdns service-types, on page 873
- show mdns statistics, on page 875
- show nat64, on page 877
- show nat64 adjacency, on page 881
- show nat64 aliases, on page 883
- show nat64 ha status, on page 885
- show nat64 limits, on page 887
- show nat64 map-t, on page 889
- show nat64 mappings dynamic, on page 890
- show nat64 pools, on page 892
- show nat64 prefix stateful, on page 894
- show nat64 prefix stateless, on page 896
- show nat64 routes, on page 898
- show nat64 services, on page 900
- show nat64 statistics, on page 902
- show nat64 timeouts, on page 904
- show nat64 translations, on page 905
- show nat64 translations entry-type, on page 908
- show nat64 translations redundancy, on page 910
- show nat64 translations time, on page 912
- show nat64 translations total, on page 914
- show nat64 translations v4, on page 916
- show nat64 translations v6, on page 918
- show nat64 translations verbose, on page 920
- show nhrp debug-condition, on page 923
- show nhrp group-map, on page 924
- show platform hardware qfp feature, on page 926
- show platform hardware qfp feature alg statistics sip, on page 930
- show platform software trace message, on page 933
- show redundancy application control-interface group, on page 936
- show redundancy application data-interface, on page 937
- show redundancy application faults group, on page 938
- show redundancy application group, on page 939
- show redundancy application if-mgr, on page 943
- show redundancy application protocol, on page 945
- show redundancy application transport, on page 947
- show running-config mdns-sd policy, on page 948

- show running-config mdns-sd service-instance, on page 950
- show running-config mdns-sd service-list, on page 952
- show running-config vrf, on page 954
- show tech nat, on page 957
- sip address, on page 959
- sip domain-name, on page 960
- snmp-server enable traps dhcp, on page 961
- source-interface (mDNS), on page 962
- subnet prefix-length, on page 964
- term ip netmask-format, on page 967
- timers hellotime, on page 968
- trusted-port (DHCPv6 Guard), on page 970
- update arp, on page 971
- update dns, on page 973
- utilization mark high, on page 975
- utilization mark low, on page 977
- view (DNS), on page 978
- vrf (DHCP pool), on page 981
- vrf (DHCPv6 pool), on page 982

show ip masks

To display the masks used for network addresses and the number of subnets using each mask, use the **show ip masks** command in EXEC mode.

show ip masks *address*

Syntax Description

address	Network address for which a mask is required.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show ip masks** command is useful for debugging when a variable-length subnet mask (VLSM) is used. It shows the number of masks associated with the network and the number of routes for each mask.

Examples

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

```
Router# show ip masks 172.16.0.0
Mask            Reference count
255.255.255.255 2
255.255.255.0   3
255.255.0.0     1
```

show ip nat limits all-host

To display the current Network Address Translation (NAT) limit entries of all configured hosts, use the **show ip nat limits all-host** command in user EXEC or privileged EXEC mode.

show ip nat limits all-host [**host-address** *host-address* [*end-host-address*] | **number-of-sessions** {**greater-than** | **less-than**} *number*] [**total**]

Syntax Description

host-address	(Optional) Displays statistics for a given address or range of addresses.
host-address	Address of the host or the starting address in a range.
end-host-address	(Optional) Ending address in a range.
number-of-sessions	(Optional) Displays statistics for limit entries with the given number of sessions.
greater-than	(Optional) Displays statistics for limit entries with more than the given number of sessions.
less-than	(Optional) Displays statistics for limit entries with less than the given number of sessions.
number	(Optional) Number of sessions for comparison. The range is from 0 to 2147483647.
total	(Optional) Displays only the total number of entries for a given query.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

You can use the **ip nat translation max-entries all-host** command to limit the all-host NAT entries.

When you specify the **total** keyword with the **show ip nat limits all-host** command, the output displays only the total entries for a given query.

Examples

The following is sample output from the **show ip nat limits all-host** command:

```
Router# show ip nat limits all-host

Host            Max Entries  Use Count   Miss Count
------------------------------------------------

10.1.1.2         100000       1           0

Total number of limit entries: 1
```

The table below describes the significant fields shown in the display.

Table 32: show ip nat limits all-host Field Descriptions

Field	Description
Host	The inside local or the outside global IP address of the host. The host is the inside local IP address for inside source translations and the outside global IP address for outside source translations.
Max Entries	The configured maximum number of limit entries.
Use Count	The current number of translations for the limit entry.
Miss Count	Number of times a translation entry was not created because of the use count exceeding the configured maximum for the limit entry.

Related Commands

Command	Description
ip nat translation max-entries	Limits the number of NAT translations to a specified maximum.
show ip nat statistics	Displays NAT statistics

show ip nat limits all-vrf

To display the current Network Address Translation (NAT) limit entries for all configured VPN routing and forwarding (VRF) instances, use the **show ip nat limits all-vrf** command in user EXEC or privileged EXEC mode.

show ip nat limits all-vrf [**vrf-name** *name* | **number-of-sessions** {**greater-than** | **less-than**} *number*] [**total**]

Syntax Description

vrf-name	(Optional) Displays statistics for a specified VRF.
name	VRF name.
number-of-sessions	(Optional) Displays statistics for limit entries with the given number of sessions.
greater-than	(Optional) Displays statistics for limit entries with more than the given number of sessions.
less-than	(Optional) Displays statistics for limit entries with less than the given number of sessions.
number	(Optional) Number of sessions for comparison. The range is from 0 to 2147483647.
total	(Optional) Displays only the total number of entries for a given query.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

You can use the **ip nat translation all-vrf** command to limit the all-VRF NAT entries.

When you specify the **total** keyword with the **show ip nat limits all-vrf** command, the output displays only the total entries for a given query.

Examples

The following is sample output from the **show ip nat limits all-vrf** command:

```
Router# show ip nat limits all-vrf

VRF Name        Max Entries  Use Count   Miss Count
-------------------------------------------------

VRF1             100000       1           0

Total number of limit entries: 1
```

The table below describes the significant fields shown in the display.

Table 33: show ip nat limits all-vrf Field Descriptions

Field	Description
VRF Name	Name of the VRF instance.
Max Entries	The configured maximum number of limit entries.
Use Count	The current number of translations for the limit entry.
Miss Count	Number of times a translation entry was not created because of the use count exceeding the configured maximum for the limit entry.

Related Commands

Command	Description
ip nat translation max-entries	Limits the number of NAT translations to a specified maximum.
show ip nat statistics	Displays NAT statistics

show ip nat nvi statistics

To display NAT virtual interface (NVI) statistics, use the **show ip nat nvi statistics**command in user EXEC or privileged EXEC mode.

show ip nat nvi statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.

Examples

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

```
Router# show ip nat nvi statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended) NAT Enabled interfaces:
Hits: 0  Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0 Expired translations: 0 Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool pool1 refcount 1213 pool pool1: netmask 255.255.255.0
         start 192.168.1.10 end 192.168.1.253
         start 192.168.2.10 end 192.168.2.253
         start 192.168.3.10 end 192.168.3.253
         start 192.168.4.10 end 192.168.4.253
         type generic, total addresses 976, allocated 222 (22%), misses 0
[Id: 2] access-list 5 pool pool2 refcount 0 pool pool2: netmask 255.255.255.0
         start 192.168.5.2 end 192.168.5.254
         type generic, total addresses 253, allocated 0 (0%), misses 0
[Id: 3] access-list 6 pool pool3 refcount 3 pool pool3: netmask 255.255.255.0
         start 192.168.6.2 end 192.168.6.254
         type generic, total addresses 253, allocated 2 (0%), misses 0
[Id: 4] access-list 7 pool pool4 refcount 0 pool pool4 netmask 255.255.255.0
         start 192.168.7.30 end 192.168.7.200
         type generic, total addresses 171, allocated 0 (0%), misses 0
[Id: 5] access-list 8 pool pool5 refcount 109195 pool pool5: netmask 255.255.255.0
         start 192.168.10.1 end 192.168.10.253
         start 192.168.11.1 end 192.168.11.253
         start 192.168.12.1 end 192.168.12.253
         start 192.168.13.1 end 192.168.13.253
         start 192.168.14.1 end 192.168.14.253
         start 192.168.15.1 end 192.168.15.253
         start 192.168.16.1 end 192.168.16.253
         start 192.168.17.1 end 192.168.17.253
         start 192.168.18.1 end 192.168.18.253
         start 192.168.19.1 end 192.168.19.253
         start 192.168.20.1 end 192.168.20.253
         start 192.168.21.1 end 192.168.21.253
         start 192.168.22.1 end 192.168.22.253
         start 192.168.23.1 end 192.168.23.253
         start 192.168.24.1 end 192.168.24.253
         start 192.168.25.1 end 192.168.25.253
         start 192.168.26.1 end 192.168.26.253
        type generic, total addresses 4301, allocated 3707 (86%),misses 0 Queued Packets:0
```

The table below describes the fields shown in the display.

Table 34: show ip nat nvi statistics Field Descriptions

Field	Description
Total active translations	Number of translations active in the system. This number is incremented each time a translation is created and is decremented each time a translation is cleared or timed out.
NAT enabled interfaces	List of interfaces marked as NAT enabled with the **ip nat enable** command.
Hits	Number of times the software does a translations table lookup and finds an entry.
Misses	Number of times the software does a translations table lookup, fails to find an entry, and must try to create one.
CEF Translated packets	Number of packets switched via Cisco Express Forwarding (CEF).
CEF Punted packets	Number of packets punted to the process switched level.
Expired translations	Cumulative count of translations that have expired since the router was booted.
Dynamic mappings	Indicates that the information that follows is about dynamic mappings.
Inside Source	The information that follows is about an inside source translation.
access-list	Access list number being used for the translation.
pool	Name of the pool.
refcount	Number of translations using this pool.
netmask	IP network mask being used in the pool.
start	Starting IP address in the pool range.
end	Ending IP address in the pool range.
type	Type of pool. Possible types are generic or rotary.
total addresses	Number of addresses in the pool available for translation.
allocated	Number of addresses being used.
misses	Number of failed allocations from the pool.
Queued Packets	Number of packets in the queue.

Related Commands

Command	Description
show ip nat nvi translations	Displays active NAT virtual interface translations.

show ip nat nvi translations

To display active NAT virtual interface (NVI) translations, use the **show ip nat nvi translations** command in user EXEC or privileged EXEC mode.

show ip nat nvi translations [*protocol* [**global** | **vrf** *vrf-name*] | **vrf** *vrf-name* | **global**] [**verbose**]

Syntax Description

protocol	(Optional) Displays protocol entries. The protocol argument must be replaced with one of the following keywords: • **esp** --Encapsulating Security Payload (ESP) protocol entries. • **icmp** --Internet Control Message Protocol (ICMP) entries. • **pptp** --Point-to-Point Tunneling Protocol (PPTP) entries. • **tcp** --TCP protocol entries. • **udp** --User Datagram Protocol (UDP) entries.
global	(Optional) Displays entries in the global destination table.
vrf *vrf-name*	(Optional) Displays VPN routing and forwarding (VRF) traffic-related information.
verbose	(Optional) Displays additional information for each translation table entry, including how long ago the entry was created and used.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.

Examples

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

```
Router# show ip nat nvi translations
Pro    Source global        Source local         Destin  local      Destin  global
icmp   172.20.0.254:25    172.20.0.130:25      172.20.1.1:25      10.199.199.100:25
icmp   172.20.0.254:26    172.20.0.130:26      172.20.1.1:26      10.199.199.100:26
icmp   172.20.0.254:27    172.20.0.130:27      172.20.1.1:27      10.199.199.100:27
icmp   172.20.0.254:28    172.20.0.130:28      172.20.1.1:28      10.199.199.100:28
```

The table below describes the fields shown in the display.

Table 35: show ip nat nvi translations Field Descriptions

Field	Description
Pro	Protocol of the port identifying the address.
Source global	Source global address.

Field	Description
Source local	Source local address.
Destin local	Destination local address.
Destin global	Destination global address.

Related Commands

Command	Description
show ip nat nvi statistics	Displays NAT virtual interface statistics.

show ip nat redundancy

To display the Network Address Translation (NAT) high-availability information, use the **show ip nat redundancy** command in privileged EXEC mode.

show ip nat redundancy *rg-id*

Syntax Description

rg-id	Redundancy group (rg) ID. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.3(2)T	This command was introduced.

Usage Guidelines

Use the **show ip nat redundancy** command to display information about the NAT high-availability Finite State Machine (FSM) and RG statistics.

The following is sample output from the **show ip nat redundancy** command. The output fields are self-explanatory.

```
Device1# show ip nat redundancy 1

        RG ID: 1        RG Name: RG1
        Current State: IPNAT_HA_RG_ST_ACT_BULK_DONE
        Previous State: IPNAT_HA_RG_ST_ACTIVE
        Recent Events: Curr: IPNAT_HA_RG_EVT_RF_ACT_STBY_HOT
                       Prev: IPNAT_HA_RG_EVT_RF_ACT_STBY_BULK_START

        Statistics :
                Static Mappings: 1,     Dynamic Mappings: 0
                Sync-ed Entries :
                        NAT Entries: 0, Door Entries: 0
                Mapping ID Mismatches: 0
                Forwarded Packets: 0,   Dropped Packets : 0
                Redirected Packets: 0


Device2# show ip nat redundancy 1

        RG ID: 1        RG Name: RG1
        Current State: IPNAT_HA_RG_ST_STBY_HOT
        Previous State: IPNAT_HA_RG_ST_STBY_COLD
        Recent Events: Curr: IPNAT_HA_RG_EVT_RF_STBY_COLD
                       Prev: IPNAT_HA_RG_EVT_NAT_CFG_REF

        Statistics :
                Static Mappings: 1,     Dynamic Mappings: 0
                Sync-ed Entries :
                        NAT Entries: 0, Door Entries: 0
                Mapping ID Mismatches: 0
                Forwarded Packets: 0,   Dropped Packets : 0
```

```
                                Redirected Packets: 0
```

Related Commands

Command	Description
show ip nat translations redundancy	Displays active NAT translations.

show ip nat statistics

To display Network Address Translation (NAT) statistics, use the **show ip nat statistics** command in user EXEC or privileged EXEC mode.

show ip nat statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.4S	This command was modified. The NAT limit statistics for all hosts and for all VPN routing and forwarding (VRF) instances were removed from the output of this command.

Examples

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

```
Router# show ip nat statistics

Total translations: 2 (0 static, 2 dynamic; 0 extended)
Outside interfaces: Serial0
Inside interfaces: Ethernet1
Hits: 135  Misses: 5
Expired translations: 2
Dynamic mappings:
-- Inside Source
access-list 1 pool net-208 refcount 2
 pool net-208: netmask 255.255.255.240
        start 172.16.233.208 end 172.16.233.221
        type generic, total addresses 14, allocated 2 (14%), misses 0
```

The table below describes the significant fields shown in the display.

Table 36: show ip nat statistics Field Descriptions

Field	Description
Total translations	Number of translations active in the system. This number is incremented each time a translation is created and is decremented each time a translation is cleared or times out.

Field	Description
Outside interfaces	List of interfaces marked as outside with the **ip nat outside** command.
Inside interfaces	List of interfaces marked as inside with the **ip nat inside** command.
Hits	Number of times the software does a translations table lookup and finds an entry.
Misses	Number of times the software does a translations table lookup, fails to find an entry, and must try to create one.
Expired translations	Cumulative count of translations that have expired since the router was booted.
Dynamic mappings	Indicates that the information that follows is about dynamic mappings.
Inside Source	Indicates that the information that follows is about an inside source translation.
access-list	Access list number being used for the translation.
pool	Name of the pool (in this case, net-208).
refcount	Number of translations using this pool.
netmask	IP network mask being used in the pool.
start	Starting IP address in the pool range.
end	Ending IP address in the pool range.
type	Type of pool. Possible types are generic or rotary.
total addresses	Number of addresses in the pool available for translation.
allocated	Number of addresses being used.
misses	Number of failed allocations from the pool.

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Changes the amount of time after which NAT translations time out.
show ip nat translations	Displays active NAT translations.

show ip nat statistics platform

The **show ip nat statistics platform** command, displays combined results of the following commands:

- **show platform hardware qfp active feature nat datapath stats**
- **show platform software nat fp active qfp-stats**
- **show platfor software Nat fp active msg-stats**
- **show platform hardware qfp active feature nat datapath esp**
- **show platform hardware qfp active feature nat datapath door**

show ip nat statistics platform

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

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

Examples

```
Device# show ip nat statistics platform

non_extended 0 entry_timeouts 0 statics 0 static net 0 hits 1752915 flowdb_hits 0 misses 0
non_natted_in2out 0 nat_bypass 0 non_natted_out2in 17805
Proxy stats:
ipc_retry_fail 0 cfg_rcvd 2 cfg_rsp 2
Number of sess 10 udp 10 tcp 0 icmp 0
Dump NAT QFP client stats
interface add: 6, upd: 0, del: 0, ack: 6, err: 0
timeout set: 12, ack: 12, err: 0
service set: 28, ack: 28, err: 0
modify-in-progress set: 0, ack: 0, err: 0
esp set: 0, ack: 0, err: 0
dnsv6 set: 1, ack: 1, err: 0
settings set: 0, ack: 0, err: 0
PAP settings set: 0, ack: 0, err: 0
Flow entries set: 1, ack: 1, err: 0
pool add: 1, del: 0, ack: 1, err: 0
addr range add: 1, upd: 0, del: 0, ack: 1, err: 0
static mapping add: 0, upd: 0, del: 0, ack: 0, err: 0
dyn mapping add: 1, upd: 0, del: 0, ack: 1, err: 0
dyn pat mapping add: 0, del: 0, ack: 0, err: 0
porlist add: 0, del: 0, ack: 0, err: 0
```

```
Logging add: 0, upd: 0, del: 0, ack: 0, err: 0
Per-VRF logging add: 0, upd: 0, del: 0, ack: 0, err: 0
Sess replicate add: 0, upd: 0, del: 0, ack: 0, err: 0
max entry set: 1, clr: 0, ack: 1, err: 0
ifaddr change notify: 0, ack: 0, err: 0
debug set: 0, clr: 0, ack: 0, err: 0
dp static-rt add: 0, del: 0, err: 0
dp ipalias add: 1, del: 0, err: 0
dp portlist req: 0, ret: 0, err: 0
dp wlan sess est: 0, term: 0, err: 0
mib setup enable: 0, disable: 0, ack: 0, err: 0
mib addr-bind query: 0, reply: 0, err: 0
MISC settings set: 0, ack: 0, err: 0
Gatekeeper settings set: 0, ack: 0, err: 0
Dump NAT RP-FP message stats
interface cfg: 4, add: 4, del: 0, upd: 0
timeout cfg: 12, add: 12, del: 0
service cfg: 28, add: 28, del: 0, upd: 0
modify-in-progress cfg: 0, add: 0, del: 0, upd: 0
esp cfg: 0, add: 0, del: 0, upd: 0
dnsv6 cfg: 1, add: 1, del: 0, upd: 0
settings cfg: 0, add: 0, del: 0, upd: 0
PAP settings cfg: 0, add: 0, del: 0, upd: 0
non-CLI clear translations exec: 0
pool cfg: 1, add: 1, del: 0, upd: 0
addr range cfg: 1, add: 1, upd: 0, del: 0
static mapping cfg: 0, add: 0, del: 0, upd: 0
dyn mapping cfg: 1, add: 1, del: 0, upd: 0
porlist event: 0, add: 0, del: 0
logging cfg: 0, add: 0, del: 0, upd: 0
per-VRF logging cfg: 0, add: 0, del: 0, upd: 0
replicate cfg: 0, add: 0, del: 0, upd: 0
max entry cfg: 0, add: 0, del: 0, upd: 0
Flow entries cfg: 1, add: 0, del: 0, upd: 0
ifaddr change event: 0
MIB query: 0
MISC settings cfg: 0
Gatekeeper settings cfg: 0, add: 0, del: 0, upd: 0
dp static-rt add: 0, del: 0
dp ipalias add: 1, del: 0
dp portlist req: 0, ret: 0
Stale event start: 0, end: 0
static translation cfg: 0, add: 0, del: 0, upd: 0
ESP global stats: esp_count 0 esp_limit_fail_count 0
DOOR global stats: door_count 0
```

show ip nat translations

To display active Network Address Translation (NAT) translations, use the **show ip nat translations** command in EXEC mode.

show ip nat translations [**inside** *global-ip*] [**outside** *local-ip*] [**esp**] [**icmp**] [**pptp**] [**tcp**] [**udp**] [**verbose**] [**vrf** *vrf-name* [**interface** *interface-name*]]

Syntax Description

esp	(Optional) Displays Encapsulating Security Payload (ESP) entries.
icmp	(Optional) Displays Internet Control Message Protocol (ICMP) entries.
inside *global-ip*	(Optional) Displays entries for only a specific inside global IP address.
interface	(Optional) Displays NAT translations where the session's interface matches the specified output interface.
outside *local-ip*	(Optional) Displays entries for only a specific outside local IP address.
pptp	(Optional) Displays Point-to-Point Tunneling Protocol (PPTP) entries.
tcp	(Optional) Displays TCP protocol entries.
udp	(Optional) Displays User Datagram Protocol (UDP) entries.
verbose	(Optional) Displays additional information for each translation table entry, including how long ago the entry was created and used.
vrf *vrf-name*	(Optional) Displays VPN routing and forwarding (VRF) traffic-related information.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(13)T	The **vrf** *vrf-name* keyword and argument combination was added.
12.2(15)T	The **esp** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
XE 2.4.2	The **inside** and **outside** keywords were added.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Release	Modification
Cisco IOS XE Everest 16.5.1	This command was modified. The output of this command was updated to display details about NAT port parity and conservation.
26.1.1	The **interface** keyword was added.

Examples

The following is sample output from the **show ip nat translations** command. Without overloading, two inside hosts are exchanging packets with some number of outside hosts.

```
Router# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 10.69.233.209     192.168.1.95       ---                ---
--- 10.69.233.210     192.168.1.89       ---                --
```

With overloading, a translation for a Domain Name Server (DNS) transaction is still active, and translations for two Telnet sessions (from two different hosts) are also active. Note that two different inside hosts appear on the outside with a single IP address.

```
Router# show ip nat translations
Pro Inside global        Inside local       Outside local      Outside global
udp 10.69.233.209:1220  192.168.1.95:1220  172.16.2.132:53    172.16.2.132:53
tcp 10.69.233.209:11012 192.168.1.89:11012 172.16.1.220:23    172.16.1.220:23
tcp 10.69.233.209:1067  192.168.1.95:1067  172.16.1.161:23    172.16.1.161:23
```

The following is sample output that includes the **verbose** keyword:

```
Router# show ip nat translations verbose
Pro Inside global        Inside local       Outside local      Outside global
udp 172.16.233.209:1220  192.168.1.95:1220  172.16.2.132:53    172.16.2.132:53
        create 00:00:02, use 00:00:00, flags: extended
tcp 172.16.233.209:11012 192.168.1.89:11012 172.16.1.220:23    172.16.1.220:23
        create 00:01:13, use 00:00:50, flags: extended
tcp 172.16.233.209:1067  192.168.1.95:1067  172.16.1.161:23    172.16.1.161:23
        create 00:00:02, use 00:00:00, flags: extended
```

The following is sample output that includes the **vrf** keyword:

```
Router# show ip nat translations vrf
abc
Pro Inside global      Inside local       Outside local      Outside global
--- 10.2.2.1            192.168.121.113    ---                ---
--- 10.2.2.2            192.168.122.49     ---                ---
--- 10.2.2.11           192.168.11.1       ---                ---
--- 10.2.2.12           192.168.11.3       ---                ---
--- 10.2.2.13           172.16.5.20        ---                ---
Pro Inside global      Inside local       Outside local      Outside global
--- 10.2.2.3            192.168.121.113    ---                ---
--- 10.2.2.4            192.168.22.49      ---                ---
```

The following is sample output that includes the **esp** keyword:

```
Router# show ip nat translations esp

Pro Inside global         Inside local          Outside local         Outside global
esp 192.168.22.40:0      192.168.122.20:0     192.168.22.20:0      192.168.22.20:28726CD9
```

```
esp 192.168.22.40:0       192.168.122.20:2E59EEF5 192.168.22.20:0     192.168.22.20:0
```

The following is sample output that includes the **esp** and **verbose** keywords:

```
Router# show ip nat translation esp verbose

Pro Inside global         Inside local          Outside local         Outside global
esp 192.168.22.40:0      192.168.122.20:0     192.168.22.20:0      192.168.22.20:28726CD9

    create 00:00:00, use 00:00:00,
    flags:
extended, 0x100000, use_count:1, entry-id:192, lc_entries:0
esp 192.168.22.40:0       192.168.122.20:2E59EEF5 192.168.22.20:0     192.168.22.20:0
    create 00:00:00, use 00:00:00, left 00:04:59, Map-Id(In):20,
    flags:
extended, use_count:0, entry-id:191, lc_entries:0
```

The following is sample output that includes the **inside**keyword:

```
Router# show ip nat translations inside 10.69.233.209
Pro Inside global        Inside local       Outside local      Outside global
udp 10.69.233.209:1220  192.168.1.95:1220  172.16.2.132:53    172.16.2.132:53
```

The following is sample output when NAT that includes the **inside**keyword:

```
Router# show ip nat translations inside 10.69.233.209
Pro Inside global        Inside local       Outside local      Outside global
udp 10.69.233.209:1220  192.168.1.95:1220  172.16.2.132:53    172.16.2.132:53
```

The following is a sample output that displays information about NAT port parity and conservation:

```
Router# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
udp  200.200.0.100:5066    100.100.0.56:5066     200.200.0.56:5060     200.200.0.56:5060
udp  200.200.0.100:1025    100.100.0.57:10001    200.200.0.57:10001    200.200.0.57:10001
udp  200.200.0.100:10000   100.100.0.56:10000    200.200.0.56:10000    200.200.0.56:10000
udp  200.200.0.100:1024    100.100.0.57:10000    200.200.0.57:10000    200.200.0.57:10000
udp  200.200.0.100:10001   100.100.0.56:10001    200.200.0.56:10001    200.200.0.56:10001
udp  200.200.0.100:9985    100.100.0.57:5066     200.200.0.57:5060     200.200.0.57:5060
Total number of translations: 6
```

The table below describes the significant fields shown in the display.

Table 37: show ip nat translations Field Descriptions

Field	Description
Pro	Protocol of the port identifying the address.
Inside global	The legitimate IP address that represents one or more inside local IP addresses to the outside world.
Inside local	The IP address assigned to a host on the inside network; probably not a legitimate address assigned by the Network Interface Card (NIC) or service provider.
Outside local	IP address of an outside host as it appears to the inside network; probably not a legitimate address assigned by the NIC or service provider.

Field	Description
Outside global	The IP address assigned to a host on the outside network by its owner.
create	How long ago the entry was created (in hours:minutes:seconds).
use	How long ago the entry was last used (in hours:minutes:seconds).
flags	Indication of the type of translation. Possible flags are: • extended--Extended translation • static--Static translation • destination--Rotary translation • outside--Outside translation • timing out--Translation will no longer be used, due to a TCP finish (FIN) or reset (RST) flag.

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Enables a port other than the default port.
show ip nat statistics	Displays NAT statistics.

show ip nat translation entry-id platform

To display results of **show platform hardware qfp active feature nat datapath sess-key** command, use the **show ip nat translation entry-id platform** command in user EXEC or privileged EXEC mode.

show ip nat translation entry-idplatform

Syntax Description

entry-id	The hexadecimal value that can ne retrieved from the **show ip nat translation verbose** command. For example: `show ip nat translations verbose` `Pro Inside global Inside local Outside local Outside global` `udp 59.59.1.1:1024 5.0.0.2:1024 6.0.0.2:63 6.0.0.2:63` `create: 02/28/18 05:57:47, use: 02/28/18 20:55:46, timeout: 00:05:00` `Map-Id(In): 1` `Flags: unknown` `Appl type: none` `WLAN-Flags: unknown` `Mac-Address: 0000.0000.0000 Input-IDB: GigabitEthernet0/0/0` **`entry-id: 0xe8f7e230.`**

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

The following is sample output from the **show ip nat translation entry-id platform** command :

Examples

```
Device# show ip nat translation entry-id 0xe8f7e230 platform

ioaddr 5.0.0.2 ooaddr 6.0.0.2 ioport 1024 ooport 63 vrf 0 proto 17 limit type 1
itaddr 59.59.1.1 otaddr 6.0.0.2 itport 1024 otport 63 tableid 0
inmap 0xe9e455c0 outmap 0x0 nak_retry 0inmapid 1
inbindpar 0x0 outbindpar 0x0
insesspar 0x0 outsesspar 0x0
ipsec cookie or spi 0x0 timeout 300 last use ts 0xd2d9 0
appl data 0x0 flags 0x0 ifhandle 8 appl_type 43 rg 0
create time 26 refcnt 1
```

show ip nat translations redundancy

To display active Network Address Translations (NAT) redundancy information, use the **show ip nat translations redundancy** command in privileged EXEC mode.

show ip nat translations redundancy *rg-id* [**verbose**]

Syntax Description

rg-id	Redundancy group (RG) ID. Valid values are 1 and 2.
verbose	(Optional) Displays additional information for each translation table entry, including the time period when the entry was created and the duration for which it was used.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.3(2)T	This command was introduced.

Usage Guidelines

Use the **show ip nat translations redundancy** command to display information about the NAT translations that belong to a specified RG.

Examples

The following is sample output from the **show ip nat translations redundancy** command for RG ID 1. The output fields are self-explanatory.

```
Device# show ip nat translations redundancy 1 verbose
--- 10.1.1.2            192.0.2.3            ---                ---
    create 00:00:10, use 00:00:10 timeout:0,
    flags:
static, created-by-local, use_count: 0, router/rg id: 0/1 ha_entry_num: 0 mapp_id[in/out]:
 120/0, entry-id: 1, lc_entries: 0
```

Related Commands

Command	Description
show ip nat redundancy	Displays NAT redundancy information.

show ip nhrp

To display Next Hop Resolution Protocol (NHRP) mapping information, use the **show ip nhrp** command in user EXEC or privileged EXEC mode.

show ip nhrp [**dynamic** | **incomplete** | **static**] [*address interface*] [**brief** | **detail**] [**purge**] [**shortcut**] [**remote**] [**local**]

Syntax Description

dynamic	(Optional) Displays dynamic (learned) IP-to-nonbroadcast multiaccess address (NBMA) mapping entries. Dynamic NHRP mapping entries are obtained from NHRP resolution/registration exchanges. See the table below for types, number ranges, and descriptions.
incomplete	(Optional) Displays information about NHRP mapping entries for which the IP-to-NBMA is not resolved. See the table below for types, number ranges, and descriptions.
static	(Optional) Displays static IP-to-NBMA address mapping entries. Static NHRP mapping entries are configured using the **ip nhrp map** command. See the table below for types, number ranges, and descriptions.
address	(Optional) Displays NHRP mapping entries for specified protocol addresses.
interface	(Optional) Displays NHRP mapping entries for the specified interface. See the table below for types, number ranges, and descriptions.
brief	(Optional) Displays a short output of the NHRP mapping.
detail	(Optional) Displays detailed information about NHRP mapping.
purge	(Optional) Displays NHRP purge information.
shortcut	(Optional) Displays NHRP shortcut information.
remote	Displays the NHRP cache entries for remote networks. **Note** By default, cache entries for both local and remote networks are displayed.
local	Displays the NHRP cache entries for local networks. **Note** By default, cache entries for both local and remote networks are displayed.
self	(Optional) Displays the NHRP fake cache information
summary	(Optional) Displays the summary of NHRP cache

Command Modes

User EXEC (>) Privileged EXEC (#)

Command Default

Information is displayed for all NHRP mappings.

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(22)T	The output of this command was extended to display the NHRP group received from the spoke.
Cisco IOS XE Release 2.5	This command was modified. Support was added for the **shortcut** keyword.
Cisco IOS XE Release 17.7.1.a	The **remote** and **local** keywords were integrated in this release.

Usage Guidelines

The table below lists the valid types, number ranges, and descriptions for the optional *interface* argument.



Note The valid types can vary according to the platform and interfaces on the platform.

Table 38: Valid Types, Number Ranges, and Interface Description

Valid Types	Number Ranges	Interface Descriptions
async	1	Async
atm	0 to 6	ATM
bvi	1 to 255	Bridge-Group Virtual Interface
cdma-ix	1	CDMA Ix
ctunnel	0 to 2147483647	C-Tunnel
dialer	0 to 20049	Dialer
ethernet	0 to 4294967295	Ethernet
fastethernet	0 to 6	FastEthernet IEEE 802.3
lex	0 to 2147483647	Lex
loopback	0 to 2147483647	Loopback
mfr	0 to 2147483647	Multilink Frame Relay bundle
multilink	0 to 2147483647	Multilink-group
null	0	Null
port-channel	1 to 64	Port channel

Valid Types	Number Ranges	Interface Descriptions
tunnel	0 to 2147483647	Tunnel
vif	1	PGM multicast host
virtual-ppp	0 to 2147483647	Virtual PPP
virtual-template	1 to 1000	Virtual template
virtual-tokenring	0 to 2147483647	Virtual Token Ring
xtagatm	0 to 2147483647	Extended tag ATM

Examples

The following is sample output from the **show ip nhrp** command. This output shows the NHRP group received from the spoke:

```
Router# show ip nhrp
10.0.0.2/32 via 10.0.0.2, Tunnel0 created 00:17:49, expire 00:01:30
  Type: dynamic, Flags: unique registered used
  NBMA address: 172.17.0.2
  Group: test-group-0
10.0.0.3/32 via 10.0.0.3, Tunnel0 created 00:00:11, expire 01:59:48
  Type: dynamic, Flags: unique registered used
  NBMA address: 172.17.0.3
  Group: test-group-0
11.0.0.2/32 via 11.0.0.2, Tunnel1 created 00:17:49, expire 00:02:10
  Type: dynamic, Flags: unique registered used
  NBMA address: 172.17.0.2
  Group: test-group-1
```

The following is sample output from the **show ip nhrp shortcut** command:

```
Router#show ip nhrp shortcut
10.1.1.1/24 via 1.1.1.22 Tunnel0 created 00:00:05, expire 00:02:24
   Type: dynamic, Flags: router rib
   NBMA address: 10.12.1.1
10.1.1.2/24 via 1.1.1.22 Tunnel0 created 00:00:05, expire 00:02:24
   Type: dynamic, Flags: router rib nho
   NBMA address: 10.12.1.2
```

The following is sample output from the **show ip nhrp detail** command:

```
Router# show ip nhrp detail
10.1.1.1/8 via 10.2.1.1, Tunnel1 created 00:46:29, never expire
  Type: static, Flags: used
  NBMA address: 10.12.1.1
10.1.1.2/8 via 10.2.1.2, Tunnel1 created 00:00:12, expire 01:59:47
  Type: dynamic, Flags: authoritative unique nat registered used
  NBMA address: 10.12.1.2
10.1.1.4, Tunnel1 created 00:00:07, expire 00:02:57
  Type: incomplete, Flags: negative
  Cache hits: 4
```

The following is sample output from the **show ip nhrp local** command:

```
Router# show ip nhrp local
Load for five secs: 100%/36%; one minute: 99%; five minutes: 99%
```

```
No time source, *12:44:19.808 UTC Tue Dec 7 2021

192.168.0.0/16 via 10.0.0.1
   Tunnel0 created 00:00:08, never expire
   Type: static, Flags: local
   NBMA address: 1.1.1.1
    (no-socket)
```

The following is sample output from the **show ip nhrp local detail** command:

```
Router# show ip nhrp local detail
Load for five secs: 100%/48%; one minute: 99%; five minutes: 99%
No time source, *12:44:52.971 UTC Tue Dec 7 2021

192.168.0.0/16 via 10.0.0.1
   Tunnel0 created 00:00:41, never expire
   Type: static, Flags: local
   NBMA address: 1.1.1.1
   Preference: 255
    (no-socket)
```

The following is sample output from the **show ip nhrp local dynamic** command:

```
Router# show ip nhrp local dynamic
Load for five secs: 99%/29%; one minute: 99%; five minutes: 99%
No time source, *12:45:15.567 UTC Tue Dec 7 2021
```

The following is sample output from the **show ip nhrp remote** command:

```
Router# show ip nhrp remote
Load for five secs: 99%/16%; one minute: 99%; five minutes: 99%
No time source, *12:45:36.789 UTC Tue Dec 7 2021

10.1.0.1/32 via 10.1.0.1
   Tunnel0 created 00:08:41, expire 00:12:55
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.1.1
10.1.0.3/32 via 10.1.0.3
   Tunnel0 created 00:17:30, expire 00:12:36
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.3.1
10.1.0.4/32 via 10.1.0.4
   Tunnel0 created 00:13:01, expire 00:14:31
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.4.1
10.1.0.5/32 via 10.1.0.5
   Tunnel0 created 00:02:08, expire 00:12:51
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.5.1
10.1.0.6/32 via 10.1.0.6
   Tunnel0 created 00:07:19, expire 00:07:41
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.6.1
10.1.0.7/32 via 10.1.0.7
   Tunnel0 created 00:07:27, expire 00:14:57
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.7.1
10.1.0.8/32 via 10.1.0.8
   Tunnel0 created 00:08:30, expire 00:06:31
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.8.1
10.1.0.9/32 via 10.1.0.9
   Tunnel0 created 00:06:22, expire 00:12:34
```

```
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.9.1
10.1.0.10/32 via 10.1.0.10
   Tunnel0 created 00:13:05, expire 00:11:14
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.10.1
10.1.0.11/32 via 10.1.0.11
   Tunnel0 created 00:12:41, expire 00:06:29
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.11.1
10.1.0.12/32 via 10.1.0.12
   Tunnel0 created 00:07:07, expire 00:07:52
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.12.1
10.1.0.13/32 via 10.1.0.13
   Tunnel0 created 00:13:01, expire 00:14:14
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.13.1
10.1.0.14/32 via 10.1.0.14
   Tunnel0 created 00:14:01, expire 00:00:58
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.14.1
10.1.0.15/32 via 10.1.0.15
   Tunnel0 created 00:00:56, expire 00:14:03
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.15.1
10.1.0.16/32 via 10.1.0.16
   Tunnel0 created 00:13:01, expire 00:11:07
```

The following is sample output from the **show ip nhrp remote detail** command:

```
Router# show ip nhrp remote detail
Load for five secs: 99%/27%; one minute: 99%; five minutes: 99%
No time source, *12:45:49.796 UTC Tue Dec 7 2021

10.1.0.1/32 via 10.1.0.1
   Tunnel0 created 00:08:54, expire 00:12:42
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.1.1
   Preference: 192
10.1.0.3/32 via 10.1.0.3
   Tunnel0 created 00:17:43, expire 00:12:23
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.3.1
   Preference: 192
10.1.0.4/32 via 10.1.0.4
   Tunnel0 created 00:13:14, expire 00:14:18
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.4.1
   Preference: 192
10.1.0.5/32 via 10.1.0.5
   Tunnel0 created 00:02:21, expire 00:12:38
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.5.1
   Preference: 192
10.1.0.6/32 via 10.1.0.6
   Tunnel0 created 00:07:32, expire 00:07:28
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.6.1
   Preference: 192
10.1.0.7/32 via 10.1.0.7
  Tunnel0 created 00:07:40, expire 00:14:44
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.7.1
```

```
   Preference: 192
10.1.0.8/32 via 10.1.0.8
   Tunnel0 created 00:08:43, expire 00:14:47
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.8.1
   Preference: 192
10.1.0.9/32 via 10.1.0.9
   Tunnel0 created 00:06:35, expire 00:12:21
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.9.1
   Preference: 192
10.1.0.10/32 via 10.1.0.10
   Tunnel0 created 00:13:18, expire 00:11:01
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.10.1
   Preference: 192
10.1.0.11/32 via 10.1.0.11
   Tunnel0 created 00:12:54, expire 00:06:16
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.11.1
   Preference: 192
10.1.0.12/32 via 10.1.0.12
   Tunnel0 created 00:07:20, expire 00:07:39
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.12.1
   Preference: 192
10.1.0.13/32 via 10.1.0.13
   Tunnel0 created 00:13:14, expire 00:14:01
   Type: dynamic, Flags: registered nhop bfd
```

The following is sample output from the **show ip nhrp remote dynamic** command:

```
Router# show ip nhrp remote dynamic
Load for five secs: 100%/12%; one minute: 99%; five minutes: 99%
No time source, *12:48:52.151 UTC Tue Dec 7 2021

10.1.0.1/32 via 10.1.0.1
   Tunnel0 created 00:11:56, expire 00:12:31
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.1.1
10.1.0.2/32 via 10.1.0.2
   Tunnel0 created 00:02:46, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.2.1
10.1.0.3/32 via 10.1.0.3
   Tunnel0 created 00:20:45, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.3.1
10.1.0.4/32 via 10.1.0.4
   Tunnel0 created 00:16:16, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.4.1
10.1.0.5/32 via 10.1.0.5
   Tunnel0 created 00:05:23, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.5.1
10.1.0.6/32 via 10.1.0.6
   Tunnel0 created 00:10:34, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.6.1
10.1.0.7/32 via 10.1.0.7
   Tunnel0 created 00:10:42, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.7.1
```

```
10.1.0.8/32 via 10.1.0.8
   Tunnel0 created 00:11:45, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.8.1
10.1.0.9/32 via 10.1.0.9
   Tunnel0 created 00:09:38, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.9.1
10.1.0.10/32 via 10.1.0.10
   Tunnel0 created 00:16:20, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.10.1
10.1.0.11/32 via 10.1.0.11
   Tunnel0 created 00:15:56, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.11.1
10.1.0.12/32 via 10.1.0.12
   Tunnel0 created 00:10:23, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.12.1
10.1.0.13/32 via 10.1.0.13
   Tunnel0 created 00:16:16, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.13.1
10.1.0.14/32 via 10.1.0.14
   Tunnel0 created 00:17:16, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.14.1
10.1.0.15/32 via 10.1.0.15
   Tunnel0 created 00:04:11, expire 00:12:32
```

The following is sample output from the **show ip nhrp remote self** command:

```
Router# show ip nhrp remote dynamic
Load for five secs: 55%/3%; one minute: 62%; five minutes: 87%
No time source, *12:50:24.793 UTC Tue Dec 7 2021

10.0.0.1/32 via 10.0.0.1
   Tunnel0 created 06:46:47, never expire
   Type: static, Flags: router unique local
   NBMA address: 1.1.1.1
    (no-socket)
Metadata Exchange Framework:
Type State
1   Reset
MEF ext data:0x0
2   Reset
MEF ext data:0x0
3   Reset
MEF ext data:0x0
```

The following is sample output from the **show ip nhrp remote summary** command:

```
Router# show ip nhrp remote summary
Load for five secs: 20%/0%; one minute: 50%; five minutes: 79%
No time source, *12:51:38.026 UTC Tue Dec 7 2021

IP NHRP cache 10000 entries, 7680000 bytes
    1 static   9999 dynamic    0 incomplete
9999 Remote
    0 static   9999 dynamic    0 incomplete
    9999 nhop     9999 bfd
    0 default  0 temporary
```

```
    0 route
        0 rib (0 H    0 nho)
        0 bgp
    0 lfib
1 Local
    1 static   0 dynamic    0 incomplete
    0 lfib
```

The following is sample output from the **show ip nhrp remote static tu1** command:

```
Router# show ip nhrp remote static tu1
10.0.0.1/32 (VPN1) via 10.0.0.1
   Tunnel1 created 1d06h, never expire
   Type: static, Flags: bfd
   NBMA address: 1.1.1.1
spoke1#sh ip nhrp remote static tu11
10.0.0.1/32 (VPN11) via 10.0.0.1
   Tunnel11 created 1d06h, never expire
   Type: static, Flags: bfd
   NBMA address: 1.1.1.1
```

The table below describes the significant fields shown in the displays.

Table 39: show ip nhrp Field Descriptions

Field	Description
10.1.1.1/8	Target network.
via 10.2.1.1	Next Hop to reach the target network.
Tunnel1	Interface through which the target network is reached.
created 00:00:12	Length of time since the entry was created (hours:minutes:seconds).
expire 01:59:47	Time remaining until the entry expires (hours:minutes:seconds).
never expire	Indicates that static entries never expire.
Type	• dynamic--NHRP mapping is obtained dynamically. The mapping entry is created using information from the NHRP resolution and registrations. • static--NHRP mapping is configured statically. Entries configured by the **ip nhrp map** command are marked static. • incomplete--The NBMA address is not known for the target network.
NBMA address	Nonbroadcast multiaccess address of the next hop. The address format is appropriate for the type of network being used: ATM, Ethernet, Switched Multimegabit Data Service (SMDS), or multipoint tunnel.

Field	Description
Flags	• authoritative--Indicates that the NHRP information was obtained directly from the Next Hop Server or router that maintains and is authoritative for the NBMA-to-IP address mapping for a particular destination. • implicit--Indicates that the local node learned about the NHRP mapping entries from the source mapping information of an NHRP resolution request received by the local router, or from an NHRP resolution packet being forwarded through the local router. • local--Indicates NHRP mapping entries that are for networks local to this router (that is, serviced by this router). These flag entries are created when this router answers an NHRP resolution request that has this information and is used to store the transport (tunnel) IP address of all the other NHRP nodes to which it has sent this information. If for some reason this router loses access to this local network (that is, it can no longer service this network), it sends an NHRP purge message to all remote NHRP nodes that are listed in the "local" entry (in **show ip nhrp detail** command output) to tell the remote nodes to clear this information from their NHRP mapping tables. This local mapping entry times out of the local NHRP mapping database at the same time that this information (from the NHRP resolution reply) would time out of the NHRP mapping database on the remote NHRP nodes. • nat--Indicates that the remote node (NHS client) supports the new NHRP NAT extension type for dynamic spoke-spoke tunnels to/from spokes behind a NAT router. This marking does not indicate that the spoke (NHS client) is behind a NAT router.
Flags (continued)	• negative--For negative caching, indicates that the requested NBMA mapping has not yet been or could not be obtained. When NHRP sends an NHRP resolution request, an incomplete (negative) NHRP mapping entry for the address is inserted in the resolution request. This insertion suppresses any more triggering of NHRP resolution requests while the resolution request is being resolved. If configured, any encryption parameters (IKE/IPsec) for the tunnel are negotiated. • (no socket)--Indicates that the NHRP mapping entries will not trigger IPsec to set up encryption because data traffic does not need to use this tunnel. Later, if data traffic needs to use this tunnel, the flag will change from a "(no socket)" to a "(socket)" entry and IPsec will be triggered to set up the encryption for this tunnel. Local and implicit NHRP mapping entries are always initially marked as "(no socket)." By default, NHRP caches source information from NHRP resolution request or replies as they go through the system. To allow this caching to continue, but not have the entry create an IPsec socket, they are marked as (no socket). If this was not done there would be extra IPsec sockets from the hubs to the various spokes that either were not used or were used for only one or two packets while a direct spoke-to-spoke tunnel was being built. Data packets and NHRP packets that arrive on the tunnel interface and are forwarded back out the tunnel interface are not allowed to use the (no socket) NHRP mappings for forwarding. Because, in this case, the router is an intermediate node in the path between the two endpoints and we only want to create short-cut tunnels between the initial entrance and final exit point of the DMVPN (NBMA) network and not between any intermediate nodes. If at some point the router receives a data packet that has a source interface that is not the tunnel interface and it would use the (no socket) mapping entry, the router converts the (no socket) entry to a (socket) entry. In this case, this router is the entrance (or exit) point of the NBMA (for this traffic stream).

Field	Description
Flags (continued)	• (no socket) (continued)--These (no socket) mapping entries are marked (non-authoritative); only mappings from NHRP registrations are marked (authoritative). The NHRP resolution requests are also marked (authoritative), which means that the NHRP resolution request can be answered only from an (authoritative) NHRP mapping entry. A (no socket) mapping entry will not be used to answer an NHRP resolution request and the NHRP resolution request will be forwarded to the NHS of the nodes . • registered--Indicates that the mapping entry was created in response to an NHRP registration request. Although registered mapping entries are dynamic entries, they may not be refreshed through the "used" mechanism. Instead, these entries are refreshed by another NHRP registration request with the same transport (tunnel) IP to NBMA address mapping. The Next Hop Client (NHC) periodically sends NHRP registration requests to keep these mappings from expiring. • router--Indicates that NHRP mapping entries for a remote router (that is accessing a network or host behind the remote router) are marked with the router flag. • unique--NHRP registration requests have the unique flag set on by default. This flag indicates that an NHRP mapping entry cannot be overwritten by a mapping entry that has the same IP address and a different NBMA address. When a spoke has a statically configured outside IP (NBMA) address, this is used to keep another spoke that is mis-configured with the same transport (tunnel) IP address from overwriting this entry. If a spoke has a dynamic outside IP (NBMA) address, you can configure the **ip nhrp registration no-unique** command on the spoke to clear this flag. This configuration allows the registered NHRP mapping entry for that spoke on the hub to be overwritten with a new NBMA address. This is necessary in this case because the spoke's outside IP (NBMA) address can change at any time. If the "unique" flag was set, the spoke would have to wait for the mapping entry on the hub to time out before it could register its new (NBMA) mapping.
Flags (continued)	• used--When data packets are process-switched and this mapping entry was used, the mapping entry is marked as used. The mapping database is checked every 60 seconds. If the used flag is set and more than 120 seconds remain until expire time, the used flag is cleared. If fewer than 120 seconds are left, this mapping entry is "refreshed" by the transmission of another NHRP resolution request. **Note** When using DMVPN Phase 3 in 12.4(6)T, CEF switched packets will also set the "used" flag, and these entries will be timed out and refreshed as described in the "used" flag description above.

Related Commands

Command	Description
ip nhrp group	Configures a NHRP group on a spoke.
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
ip nhrp map group	Adds NHRP groups to QoS policy mappings on a hub.

Command	Description
ip nhrp shortcut	Enables shortcut switching on the tunnel interface.
show dmvpn	Displays DMVPN-specific session information.
show ip nhrp group-map	Displays the details of NHRP group mappings on a hub and the list of tunnels using each of the NHRP groups defined in the mappings.
show ip nhrp multicast	Displays NHRP multicast mapping information.
show ip nhrp nhs	Displays NHRP Next Hop Server information.
show ip nhrp summary	Displays NHRP mapping summary information.
show ip nhrp traffic	Displays NHRP traffic statistics.
show policy-map mgre	Displays statistics about a specific QoS policy as it is applied to a tunnel endpoint.

show ip nhrp group-map

To display the details of NHRP group mappings, use the **show ip nhrp group-map**command in user EXEC or privileged EXEC mode.

show ip nhrp group-map [*group-name*]

Syntax Description

group-name	(Optional) Name of an NHRP group mapping for which information will be displayed.

Command Default

Information is displayed for all NHRP group mappings.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

This command displays the details on NHRP group mappings on the hub along with the list of tunnels using each of the NHRP groups defined in the mappings. In combination with the **show ip nhrp** command, this command lets you easily determine which QoS policy map is applied to a specific tunnel endpoint.

This command displays the details of the specified NHRP group mapping. The details include the associated QoS policy name and the list of tunnel endpoints using the QoS policy. If no option is specified, it displays the details of all NHRP group mappings.

Examples

The following is sample output from the **show ip nhrp group-map**command:

```
Router# show ip nhrp group-map
Interface: Tunnel0
 NHRP group: test-group-0
  QoS policy: queueing
  Tunnels using the QoS policy:
  Tunnel destination overlay/transport address
  10.0.0.2/172.17.0.2
  10.0.0.3/172.17.0.3
Interface: Tunnel1
 NHRP group: test-group-1
  QoS policy: queueing
  Tunnels using the QoS policy:
  Tunnel destination overlay/transport address
  11.0.0.2/172.17.0.2
 NHRP group: test-group-2
  QoS policy: p1
  Tunnels using the QoS policy: None
```

The following is sample output from the **show ip nhrp group-map**command for an NHRP group named test-group-0:

```
Router# show ip nhrp group-map test-group-0
Interface: Tunnel0
 NHRP group: test-group-0
  QoS policy: queueing
```

```
Tunnels using the QoS policy:
Tunnel destination overlay/transport address
10.0.0.2/172.17.0.2
10.0.0.3/172.17.0.3
```

The table below describes the significant fields shown in the displays.

Table 40: show ip nhrp group-map Field Descriptions

Field	Description
Interface	Interface on which the policy is configured.
NHRP group	NHRP group associated with the QoS policy on the interface.
QoS policy	QoS policy configured on the interface.
Tunnels using the QoS Policy	List of tunnel endpoints using the QoS policy.
Tunnel destination overlay/transport address	Tunnel destination overlay address (such as the tunnel endpoint address).

Related Commands

Command	Description
ip nhrp group	Configures a NHRP group on a spoke.
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
ip nhrp map group	Adds NHRP groups to QoS policy mappings on a hub.
show dmvpn	Displays DMVPN-specific session information.
show ip nhrp	Displays NHRP mapping information.
show policy-map mgre	Displays statistics about a specific QoS policy as it is applied to a tunnel endpoint.

show ip nhrp multicast

To display Next Hop Resolution Protocol (NHRP) multicast mapping information, use the **show ip nhrp multicast** command in user EXEC or privileged EXEC mode.

show ip nhrp multicast [*nbma-addressinterface*]

Syntax Description

nbma-address	(Optional) Displays multicast mapping information for the specified NBMA address.
interface	(Optional) Displays all multicast mapping entries of the NHRP network for the interface. See the table below for types, number ranges, and descriptions.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.4(7)	This command was introduced.

Usage Guidelines

The table below lists the valid types, number ranges, and descriptions for the optional *interface* argument.

Note The valid types can vary according to the platform and interfaces on the platform.

Table 41: Interface Types, Valid Numbers, and Interface Descriptions

Interface Types	Valid Numbers	Interface Descriptions
async	1	Async
atm	0 to 6	ATM
bvi	1 to 255	Bridge-Group Virtual Interface
cdma-ix	1	CDMA Ix
ctunnel	0 to 2147483647	C-Tunnel
dialer	0 to 20049	Dialer
ethernet	0 to 4294967295	Ethernet
fastethernet	0 to 6	FastEthernet IEEE 802.3
lex	0 to 2147483647	Lex
loopback	0 to 2147483647	Loopback
mfr	0 to 2147483647	Multilink Frame Relay bundle

Interface Types	Valid Numbers	Interface Descriptions
multilink	0 to 2147483647	Multilink-group
null	0	Null
port-channel	1 to 64	Port channel
tunnel	0 to 2147483647	Tunnel
vif	1	PGM multicast host
virtual-ppp	0 to 2147483647	Virtual PPP
virtual-template	1 to 1000	Virtual template
virtual-tokenring	0 to 2147483647	Virtual Token Ring
xtagatm	0 to 2147483647	Extended tag ATM

Examples

The following is sample output from the **show ip nhrp multicast** command:

```
Router# show ip nhrp multicast
  I/F     NBMA address
Tunnel1    1.1.1.1         Flags: static
```

The table below describes the fields shown in the display.

Table 42: show ip nhrp Field Descriptions

Field	Description
I/F	Interface associated with the multicast mapping entry.
NBMA address	Nonbroadcast Multiaccess Address to which multicast packets will be sent. The address format is appropriate for the type of network used: ATM, Ethernet, SMDS, or multipoint tunnel.
Flags	• static—Indicates that the multicast mapping entry is configured statically by the **ip nhrp map multicast** command. • dynamic—Indicates that the multicast mapping entry is obtained dynamically. A multicast mapping entry is created for each registered Next Hop Client (NHC) when the **ip nhrp map multicast dynamic** command is configured.

Related Commands

Command	Description
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
show ip nhrp	Displays NHRP mapping information.
show ip nhrp nhs	Displays NHRP next-hop server information.

Command	Description
show ip nhrp summary	Displays NHRP mapping summary information.
show ip nhrp traffic	Displays NHRP traffic statistics.

show ip nhrp multicast stats

To display multicast mapping statistics for one or all interfaces, use the **show ip nhrp multicast stats** command in privileged EXEC mode. The command displays statistics such as the count of enqueued, dequeued, and dropped packets.

show ip nhrp multicast [*interface-name*] **stats**

Syntax Description

interface-name	Displays multicast mapping statistics for the specified interface. Example: **show ip nhrp multicast tunnel0 stats**

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 16.8.1	Command introduced.

Example

```
Router#show ip nhrp multicast stats
Legend: (m/n) - (m packets/n milliseconds)
================================================================================================

Global stats
Total multicast pkts enqueued    102
Total multicast failed to enqueue 0
Total multicast pkts dequeued     102
Invalid multicast pkts dequeued   0
Total multicast pkts dropped      0

Interface stats
                                    Enqueued/Failed             Dequeued/Rep fail       Dropped
                                ------------------------  --------------------------  ----------
 Tu0     (250    /     10)              51/0                         51/0                  0
```

show ip nhrp nhs

To display Next Hop Resolution Protocol (NHRP) next hop server (NHS) information, use the **show ip nhrp nhs**command in user EXEC or privileged EXEC mode.

show ip nhrp nhs [*interface*] [**detail**]

Syntax Description

interface	(Optional) Displays NHS information currently configured on the interface. See the table below for types, number ranges, and descriptions.
detail	(Optional) Displays detailed NHS information.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The table below lists the valid types, number ranges, and descriptions for the optional *interface*argument.

Note The valid types can vary according to the platform and interfaces on the platform.

Table 43: Valid Types, Number Ranges, and Interface Descriptions

Valid Types	Number Ranges	Interface Descriptions
async	1	Async
atm	0 to 6	ATM
bvi	1 to 255	Bridge-Group Virtual Interface
cdma-ix	1	CDMA Ix
ctunnel	0 to 2147483647	C-Tunnel
dialer	0 to 20049	Dialer
ethernet	0 to 4294967295	Ethernet
fastethernet	0 to 6	FastEthernet IEEE 802.3
lex	0 to 2147483647	Lex

Valid Types	Number Ranges	Interface Descriptions
loopback	0 to 2147483647	Loopback
mfr	0 to 2147483647	Multilink Frame Relay bundle
multilink	0 to 2147483647	Multilink-group
null	0	Null
port-channel	1 to 64	Port channel
tunnel	0 to 2147483647	Tunnel
vif	1	PGM multicast host
virtual-ppp	0 to 2147483647	Virtual PPP
virtual-template	1 to 1000	Virtual template
virtual-tokenring	0 to 2147483647	Virtual Token Ring
xtagatm	0 to 2147483647	Extended tag ATM

Examples

The following is sample output from the **show ip nhrp nhs detail** command:

```
Router# show ip nhrp nhs detail
Legend:
  E=Expecting replies
  R=Responding
Tunnel1:
  5.1.1.1           E  req-sent 128  req-failed 1  repl-recv 0
Pending Registration Requests:
Registration Request: Reqid 1, Ret 64  NHS 5.1.1.1
```

The table below describes the significant field shown in the display.

Table 44: show ip nhrp nhs Field Descriptions

Field	Description
Tunnel1	Interface through which the target network is reached.

Related Commands

Command	Description
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
show ip nhrp	Displays NHRP mapping information.
show ip nhrp multicast	Displays NHRP multicast mapping information.
show ip nhrp summary	Displays NHRP mapping summary information.

Command	Description
show ip nhrp traffic	Displays NHRP traffic statistics.

show ip nhrp redirect

To display Next Hop Resolution Protocol (NHRP) redirect table information, use the **show ip nhrp redirect**command in user EXEC or privileged EXEC mode.

show ip nhrp redirect *statistics*

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2SX	This command was introduced.

Examples

The following is sample output from the **show ip nhrp redirect** command:

```
Router# show ip nhrp redirect

I/F      NBMA address          Destination           Drop Count    Expiry

Tunnel43   10.232.195.197         10.138.140.33          2     00:00:05
Tunnel43   10.232.195.193         10.138.140.33         54     00:00:05
Tunnel43   10.232.195.185         10.138.140.33          1     00:00:06
Tunnel43   10.232.195.189         10.138.140.33          0     00:00:07
Tunnel43   10.232.195.205         10.138.153.66         52     00:00:07
```

This output shows the content of the NHRP redirect table on the node. An entry in output indicates that further redirect messages to the NBMA address for the destination will be suppressed as long as the corresponding entry doesn't expire

The table below describes the fields shown in the command output.

Table 45: show ip nhrp redirect command- Field Descriptions

Field Output	Description
NBMA Address	Displays the address where the redirect message is sent to. This is the NBMA address of the source spoke.
Destination	Displays the destination IP address from the data packet that triggered the NHRP redirect. This is the LAN address that is behind the destination spoke.
Drop Count	Displays the number of redirect messages throttled due to presence of this entry in the redirect table .
Expiry	Displays the lifetime of the redirect entry. The default max lifetime is 8 seconds. At expiry of the lifetime, the entry is deleted and new redirect messages with these details can be sent by this node if there are further data packets matching these entries .

Examples

The following is sample output from the **show ip nhrp redirect statistics** command:

```
Router# show ip nhrp redirect statistics

DMVPN Redirect Indications throttled: 7
```

show ip nhrp summary

To display Next Hop Resolution Protocol (NHRP) mapping summary information, use the **show ip nhrp summary**command in user EXEC or privileged EXEC mode.

show ip nhrp summary

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show ip nhrp summary** command:

```
Router# show ip nhrp summary
IP NHRP cache 1 entry, 256 bytes
    1 static  0 dynamic  0 incomplete
```

The table below describes the significant field shown in the display.

Table 46: show ip nhrp summary Field Descriptions

Field Output	Description
dynamic	NHRP mapping is obtained dynamically. The mapping entry is created using information from the NHRP resolution and registrations
static	NHRP mapping is configured statically. Entries configured by the **ip nhrp map** command are marked static.
incomplete	NBMA address is not known for the target network.

Related Commands

Command	Description
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
show ip nhrp	Displays NHRP mapping information.
show ip nhrp multicast	Displays NHRP multicast mapping information.
show ip nhrp nhs	Displays NHRP Next Hop Server information.
show ip nhrp traffic	Displays NHRP traffic statistics.

show ip nhrp traffic

To display Next Hop Resolution Protocol (NHRP) traffic statistics, use the **show ip nhrp traffic** command in privileged EXEC mode.

show ip nhrp traffic[**throttled** | **interface** {**tunnel** *number* | **Virtual-Access** *number*}]

Syntax Description

throttled	(Optional) Displays information about NHRP traffic that is throttled.
interface	(Optional) Displays NHRP traffic information for a given interface.
tunnel *number*	Specifies the tunnel interface number.
Virtual-Access *number*	Specifies the virtual access interface number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
10.3	This command was introduced.
12.4(6)T	This command was modified. The show output was enhanced to display information about traffic indication (redirects).
12.4(9)T	This command was modified. The **interface** and **tunnel** keywords and the *number* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.3(2)T	This command was modified. The **Virtual-Access** *number* keyword-argument pair was added.
Cisco IOS XE 16.3.2	This command was modified. The **throttled** keyword was added.

Usage Guidelines

Replacing **ip** in the command name with **ipv6** shows IPv6-specific traffic.

Examples

The following example shows sample output for NHRP traffic statistics for tunnel interface 0:

```
Device# show ip nhrp traffic interface tunnel0
Tunnel0: Max-send limit:100Pkts/10Sec, Usage:0%
   Sent: Total 79
         18 Resolution Request  10 Resolution Reply  42 Registration Request
         0 Registration Reply  3 Purge Request  6 Purge Reply
         0 Error Indication  0 Traffic Indication
```

```
   Rcvd: Total 69
         10 Resolution Request  15 Resolution Reply  0 Registration Request
         36 Registration Reply  6 Purge Request  2 Purge Reply
         0 Error Indication  0 Traffic Indication
```

The table below describes the significant fields shown in the display.

Table 47: show ip nhrp traffic Field Descriptions

Field	Description
Tunnel0	Interface type and number.
Max-send limit	Maximum number of NHRP messages that can be sent by this station in the given interval.
Resolution Request	Number of NHRP resolution request packets originated from or received by this station.
Resolution Reply	Number of NHRP resolution reply packets originated from or received by this station.
Registration Request	Number of NHRP registration request packets originated from or received by this station.
Registration Reply	Number of NHRP registration reply packets originated from or received by this station.
Purge Request	Number of NHRP purge request packets originated from or received by this station.
Purge Reply	Number of NHRP purge reply packets originated from or received by this station.
Error Indication	Number of NHRP error packets originated from or received by this station.
Traffic Indication	Number of NHRP traffic indication packets (redirects) originated from or received by this station.

The following example shows sample output for the **show ip nhrp traffic** command with the **throttled** keyword applied:

```
SPOKE1#show ip nhrp traffic throttled
Tunnel1: Max-send limit:10000Pkts/10Sec, Usage:0%
   Sent: Total 0
         0 Resolution Request  0 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
         0 Error Indication  0 Traffic Indication  0 Redirect Suppress
   Rcvd: Total 0
         0 Resolution Request  0 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
         0 Error Indication  0 Traffic Indication  0 Redirect Suppress
```

Related Commands

Command	Description
debug nhrp condition	Enables NHRP conditional debugging.
debug nhrp error	Enables NHRP error level debugging.

show ip route dhcp

To display the routes added to the routing table by the Dynamic Host Configuration Protocol (DHCP) server and relay agent, use the **show ip route dhcp** command in privileged EXEC configuration mode.

show ip route [**vrf** *vrf-name*] **dhcp** [*ip-address*]

Syntax Description

vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name of the VRF.
ip-address	(Optional) Address about which routing information should be displayed.

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To display information about global routes, use the **show ip route dhcp** command. To display routes in the VRF routing table, use the **show ip route vrf** *vrf-name* **dhcp** command.

Examples

The following is sample output from the **show ip route dhcp**command when entered without an address. This command lists all routes added by the DHCP server and relay agent.

```
Router# show ip route dhcp
  10.5.5.56/32 is directly connected, ATM0.2
  10.5.5.217/32 is directly connected, ATM0.2
```

The following is sample output from the **show ip route dhcp** command when an address is specified. The output shows the details of the address with the server address (who assigned it) and the lease expiration time.

```
Router# show ip route dhcp 10.5.5.217

  10.5.5.217 is directly connected, ATM0.2
    DHCP Server: 10.9.9.10   Lease expires at Nov 08 2001 01:19 PM
```

The following is sample output from the **show ip route vrf** *vrf-name* **dhcp**command when entered without an address:

```
Router# show ip route vrf abc dhcp
  10.5.5.218/32 is directly connected, ATM0.2
```

The following is sample output from the **show ip route vrf** *vrf-name* **dhcp**command when an address is specified. The output shows the details of the address with the server address (who assigned it) and the lease expiration time.

```
Router# show ip route vrf red dhcp 10.5.5.218
  10.5.5.218/32 is directly connected, ATM0.2
    DHCP Server: 10.9.9.10   Lease expires at Nov 08 2001 03:15PM
```

Related Commands

Command	Description
clear ip route dhcp	Removes routes from the routing table added by the DHCP server and relay agent for the DHCP clients on unnumbered interfaces.

show ip snat

To display active Stateful Network Address Translation (SNAT) translations, use the **show ip snat** command in EXEC mode.

show ip snat [**distributed** [**verbose**] | **peer** *ip-address*]

Syntax Description

distributed	(Optional) Displays information about the distributed NAT, including its peers and status.
verbose	(Optional) Displays additional information for each translation table entry, including how long ago the entry was created and used.
peer *ip-address*	(Optional) Displays TCP connection information between peer routers.

Command Modes

EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Examples

The following is sample output from the **show ip snat distributed** command for stateful NAT connected peers:

```
Router# show ip snat distributed
Stateful NAT Connected Peers
SNAT: Mode PRIMARY
:State READY
:Local Address 192.168.123.2
:Local NAT id 100
:Peer Address 192.168.123.3
:Peer NAT id 200
:Mapping List 10
```

The following is sample output from the **show ip snat distributed verbose**command for stateful NAT connected peers:

```
Router# show ip snat distributed verbose
SNAT: Mode PRIMARY
Stateful NAT Connected Peers
:State READY
:Local Address 192.168.123.2
:Local NAT id 100
:Peer Address 192.168.123.3
:Peer NAT id 200
:Mapping List 10
:InMsgs 7, OutMsgs 7, tcb 0x63EBA408, listener 0x0
```

show ip source binding

To display IP-source bindings configured on the system, use the **show ip source command** command in privileged EXEC mode.

show ip source binding [*ip-address*] [*mac-address*] [**dhcp-snooping** | **static**] [**vlan** *vlan-id*] [**interface** *type mod/port*]

Syntax Description

ip-address	(Optional) Binding IP address.
mac-address	(Optional) Binding MAC address.
dhcp-snooping	(Optional) Specifies DHCP snooping binding entry.
static	(Optional) Specifies a static binding entry.
vlan *vlan-id*	(Optional) Specifies the Layer 2 VLAN identification; valid values are from 1 to 4094.
interface *type*	(Optional) Interface type; possible valid values are **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **port-channel** *num*, and **vlan** *vlan-id*.
mod / *port*	Module and port number.

Command Default

Both static and DHCP-snooping bindings are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

Each optional parameter is used to filter the display output.

Examples

This example shows the output without entering any keywords:

Router# **show ip source binding**

```
MacAddress             IpAddress       Lease(sec) Type           VLAN Interface
------------------     --------------- ---------- ------------- ---- --------------------
00:00:00:0A:00:0B      17.16.0.1        infinite   static        10   FastEthernet6/10
00:00:00:0A:00:0A      17.16.0.2        10000      dhcp-snooping 10   FastEthernet6/11
```

This example shows how to display the static IP binding entry for a specific IP address:

```
Router# show ip source binding 17.16.0.1 0000.000A.000B static vlan 10 interface
gigabitethernet6/10
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------

00:00:00:0A:00:0B   17.16.0.1         infinite    static         10    FastEthernet6/10
```

The table below describes the significant fields in the display.

Table 48: show ip source binding Field Descriptions

Field	Description
MAC Address	Client hardware MAC address.
IP Address	Client IP address assigned from the DHCP server.
Lease (seconds)	IP address lease time.
Type	Binding type; static bindings configured from CLI to dynamic binding learned from DHCP snooping.
VLAN	VLAN number of the client interface.
Interface	Interface that connects to the DHCP client host.

Related Commands

Command	Description
ip source binding	Adds or deletes a static IP source binding entry.
ip verify source vlan dhcp-snooping	Enables or disables the per 12-port IP source guard.
show ip verify source	Displays the IP source guard configuration and filters on a particular interface.

show ip verify source

To display the IP source guard configuration and filters on a particular interface, use the **show ip verify source** command in EXEC mode.

show ip verify source [**interface** *type mod/port*] [**efp_id efp_id**]

Syntax Description

interface *type*	(Optional) Specifies the interface type; possible valid values are **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **port-channel** *num*, and **vlan** *vlan-id*.
mod / *port*	Module and port number.
efp_id	(Optional) Specifies the Ethernet flow point (EFP) (service instance) ID.
efp_id	EFP number; range is 1 to 8000.

Command Default

This command has no default settings.

Command Modes

EXEC (#)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRD	The **efp_id** *efp_id*keyword and argument were added.

Usage Guidelines

Enable port security first because the DHCP security MAC filter cannot apply to the port or VLAN.

Examples

This example shows the display when DHCP snooping is enabled on VLANs 10 to 20, the interface has IP source filter mode that is configured as IP, and there is an existing IP address binding 10.0.0.1 on VLAN 10:

```
Router# show ip verify source interface gigabitethernet6/1
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
gi6/1      ip           active       10.0.0.1                         10
gi6/1      ip           active       deny-all                        11-20
```

This example shows how to display the IP source guard configuration and filters on a specific interface:

```
Router# show ip verify source interface gigabitethernet6/1
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
gi6/1      ip           inactive-trust-port
```

This example shows the display when the interface does not have a VLAN enabled for DHCP snooping:

```
Router# show ip verify source interface gigabitethernet6/3
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
```

```
---------  -----------  -----------  ---------------  --------------  ---------
gi6/3      ip           inactive-no-snooping-vlan
```

This example shows the display when the interface has an IP source filter mode that is configured as IP MAC and an existing IP MAC binds 10.0.0.2/aaaa.bbbb.cccc on VLAN 10 and 10.0.0.1/aaaa.bbbb.cccd on VLAN 11:

```
Router# show ip verify source interface gigabitethernet6/4
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
gi6/4      ip-mac       active       10.0.0.2         aaaa.bbbb.cccc  10
gi6/4      ip-mac       active       10.0.0.1         aaaa.bbbb.cccd  11
gi6/4      ip-mac       active       deny-all         deny-all        12-20
```

This example shows the display when the interface has an IP source filter mode that is configured as IP MAC and an existing IP MAC binding 10.0.0.3/aaaa.bbbb.ccce on VLAN 10, but port security is not enabled on the interface:

```
Router# show ip verify source interface gigabitethernet6/5
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
gi6/5      ip-mac       active       10.0.0.3         permit-all      10
gi6/5      ip-mac       active       deny-all         permit-all      11-20
```

This example shows the display when the interface does not have IP source filter mode configured:

```
Router# show ip verify source interface gigabitethernet6/6
DHCP security is not configured on the interface gi6/6.
```

This example shows how to display all the interfaces on the switch that have DHCP snooping security enabled:

```
Router# show ip verify source

Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
gi6/1      ip           active       10.0.0.1                         10
gi6/1      ip           active       deny-all                         11-20
gi6/2      ip           inactive-trust-port
gi6/3      ip           inactive-no-snooping-vlan
gi6/4      ip-mac       active       10.0.0.2         aaaa.bbbb.cccc  10
gi6/4      ip-mac       active       11.0.0.1         aaaa.bbbb.cccd  11
gi6/4      ip-mac       active       deny-all         deny-all        12-20
gi6/5      ip-mac       active       10.0.0.3         permit-all      10
gi6/5      ip-mac       active       deny-all         permit-all      11-20
Router#
```

This example shows how to display all the interfaces on the switch that have DHCP snooping security enabled:

```
Router# show ip verify source interface gi5/0/0 efp_id 10
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan        EFP
ID
---------    -----------    -----------      ---------------     -----------------
----------  ----------
Gi5/0/0    ip-mac       active          123.1.1.1        00:0A:00:0A:00:0A  100        10

Gi5/0/0    ip-mac       active          123.1.1.2        00:0A:00:0A:00:0B  100        20
```

```
Gi5/0/0     ip-mac       active          123.1.1.3        00:0A:00:0A:00:0C  100         30
```

Related Commands

Command	Description
ip source binding	Adds or deletes a static IP source binding entry.
ip verify source vlan dhcp-snooping	Enables or disables the per l2-port IP source guard.
show ip source binding	Displays the IP-source bindings configured on the system.

show ipv6 dhcp

To display the Dynamic Host Configuration Protocol (DHCP) unique identifier (DUID) on a specified device, use the **show ipv6 dhcp** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

The **show ipv6 dhcp** command uses the DUID based on the link-layer address for both client and server identifiers. The device uses the MAC address from the lowest-numbered interface to form the DUID. The network interface is assumed to be permanently attached to the device. Use the **show ipv6 dhcp** command to display the DUID of a device.

Examples

The following is sample output from the **show ipv6 dhcp**command. The output is self-explanatory:

```
Router# show ipv6 dhcp
This device's DHCPv6 unique identifier(DUID): 000300010002FCA5DC1C
```

show ipv6 dhcp binding

To display automatic client bindings from the Dynamic Host Configuration Protocol (DHCP) for IPv6 server binding table, use the **show ipv6 dhcp binding** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp binding [*ipv6-address*] [**vrf** *vrf-name*]

Syntax Description

ipv6-address	(Optional) The address of a DHCP for IPv6 client.
vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4	This command was modified. Command output was updated to display a PPP username associated with a binding.
12.4(24)T	This command was modified. Command output was updated to display address bindings.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.1(2)S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
Cisco IOS XE Release 3.3S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **show ipv6 dhcp binding** command displays all automatic client bindings from the DHCP for IPv6 server binding table if the *ipv6-address* argument is not specified. When the *ipv6-address* argument is specified, only the binding for the specified client is displayed.

If the **vrf** *vrf-name*keyword and argument combination is specified, all bindings that belong to the specified VRF are displayed.

Examples

The following sample output displays all automatic client bindings from the DHCP for IPv6 server binding table:

```
Router# show ipv6 dhcp binding
Client: FE80::A8BB:CCFF:FE00:300
  DUID: 00030001AABBCC000300
  Username : client_1
  Interface: Virtual-Access2.1
  IA PD: IA ID 0x000C0001, T1 75, T2 135
    Prefix: 2001:380:E00::/64
            preferred lifetime 150, valid lifetime 300
```

```
            expires at Dec 06 2007 12:57 PM (262 seconds)
Client: FE80::A8BB:CCFF:FE00:300 (Virtual-Access2.2)
  DUID: 00030001AABBCC000300
  IA PD: IA ID 0x000D0001, T1 75, T2 135
    Prefix: 2001:0DB8:E00:1::/64
            preferred lifetime 150, valid lifetime 300
            expires at Dec 06 2007 12:58 PM (288 seconds)
```

The table below describes the significant fields shown in the display.

Table 49: show ipv6 dhcp binding Field Descriptions

Field	Description
Client	Address of a specified client.
DUID	DHCP unique identifier (DUID).
Virtual-Access2.1	First virtual client. When an IPv6 DHCP client requests two prefixes with the same DUID but a different identity association for prefix delegation (IAPD) on two different interfaces, these prefixes are considered to be for two different clients, and interface information is maintained for both.
Username : client_1	The username associated with the binding.
IA PD	Collection of prefixes assigned to a client.
IA ID	Identifier for this IAPD.
Prefix	Prefixes delegated to the indicated IAPD on the specified client.
preferred lifetime, valid lifetime	The preferred lifetime and valid lifetime settings, in seconds, for the specified client.
Expires at	Date and time at which the valid lifetime expires.
Virtual-Access2.2	Second virtual client. When an IPv6 DHCP client requests two prefixes with the same DUID but different IAIDs on two different interfaces, these prefixes are considered to be for two different clients, and interface information is maintained for both.

When the DHCPv6 pool on the Cisco IOS DHCPv6 server is configured to obtain prefixes for delegation from an authentication, authorization, and accounting (AAA) server, it sends the PPP username from the incoming PPP session to the AAA server for obtaining the prefixes. The PPP username is associated with the binding is displayed in output from the **show ipv6 dhcp binding** command. If there is no PPP username associated with the binding, this field value is displayed as "unassigned."

The following example shows that the PPP username associated with the binding is "client_1":

```
Router# show ipv6 dhcp binding
Client: FE80::2AA:FF:FEBB:CC
  DUID: 0003000100AA00BB00CC
  Username : client_1
  Interface : Virtual-Access2
  IA PD: IA ID 0x00130001, T1 75, T2 135
    Prefix: 2001:0DB8:1:3::/80
```

```
            preferred lifetime 150, valid lifetime 300
            expires at Aug 07 2008 05:19 AM (225 seconds)
```

The following example shows that the PPP username associated with the binding is unassigned:

```
Router# show ipv6 dhcp binding
Client: FE80::2AA:FF:FEBB:CC
  DUID: 0003000100AA00BB00CC
  Username : unassigned
  Interface : Virtual-Access2
  IA PD: IA ID 0x00130001, T1 150, T2 240
    Prefix: 2001:0DB8:1:1::/80
            preferred lifetime 300, valid lifetime 300
            expires at Aug 11 2008 06:23 AM (233 seconds)
```

Related Commands

Command	Description
clear ipv6 dhcp binding	Deletes automatic client bindings from the DHCP for IPv6 binding table.

show ipv6 dhcp conflict

To display address conflicts found by a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server when addresses are offered to the client, use the **show ipv6 dhcp conflict** command in privileged EXEC mode.

show ipv6 dhcp conflict [*ipv6-address*] [**vrf** *vrf-name*]

Syntax Description

ipv6-address	(Optional) The address of a DHCP for IPv6 client.
vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.1(2)S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
Cisco IOS XE Release 3.3S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

When you configure the DHCPv6 server to detect conflicts, it uses ping. The client uses neighbor discovery to detect clients and reports to the server through a DECLINE message. If an address conflict is detected, the address is removed from the pool, and the address is not assigned until the administrator removes the address from the conflict list.

Examples

The following is a sample output from the **show ipv6 dhcp conflict** command. This command shows the pool and prefix values for DHCP conflicts.:

```
Router# show ipv6 dhcp conflict
Pool 350, prefix 2001:0DB8:1005::/48
     2001:0DB8:1005::10
```

Related Commands

Command	Description
clear ipv6 dhcp conflict	Clears an address conflict from the DHCPv6 server database.

show ipv6 dhcp database

To display the Dynamic Host Configuration Protocol (DHCP) for IPv6 binding database agent information, use the **show ipv6 dhcp database** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp database [*agent-URL*]

Syntax Description

agent-URL	(Optional) A flash, NVRAM, FTP, TFTP, or remote copy protocol (RCP) uniform resource locator.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Each permanent storage to which the binding database is saved is called the database agent. An agent can be configured using the **ipv6 dhcp database** command. Supported database agents include FTP and TFTP servers, RCP, Flash file system, and NVRAM.

The **show ipv6 dhcp database**command displays DHCP for IPv6 binding database agent information. If the *agent-URL* argument is specified, only the specified agent is displayed. If the *agent-URL* argument is not specified, all database agents are shown.

Examples

The following is sample output from the **show ipv6 dhcp database**command:

```
Router# show ipv6 dhcp database
Database agent tftp://172.19.216.133/db.tftp:
  write delay: 69 seconds, transfer timeout: 300 seconds
  last written at Jan 09 2003 01:54 PM,
     write timer expires in 56 seconds
  last read at Jan 06 2003 05:41 PM
  successful read times 1
  failed read times 0
  successful write times 3172
  failed write times 2
Database agent nvram:/dhcpv6-binding:
  write delay: 60 seconds, transfer timeout: 300 seconds
  last written at Jan 09 2003 01:54 PM,
     write timer expires in 37 seconds
  last read at never
  successful read times 0
  failed read times 0
  successful write times 3325
  failed write times 0
Database agent flash:/dhcpv6-db:
  write delay: 82 seconds, transfer timeout: 3 seconds
  last written at Jan 09 2003 01:54 PM,
    write timer expires in 50 seconds
```

```
last read at never
successful read times 0
failed read times 0
successful write times 2220
failed write times 614
```

The table below describes the significant fields shown in the display.

Table 50: show ipv6 dhcp database Field Descriptions

Field	Description
Database agent	Specifies the database agent.
Write delay	The amount of time (in seconds) to wait before updating the database.
transfer timeout	Specifies how long (in seconds) the DHCP server should wait before terminating a database transfer. Transfers that exceed the timeout period are terminated.
Last written	The last date and time bindings were written to the file server.
Write timer expires...	The length of time, in seconds, before the write timer expires.
Last read	The last date and time bindings were read from the file server.
Successful/failed read times	The number of successful or failed read times.
Successful/failed write times	The number of successful or failed write times.

Related Commands

Command	Description
ipv6 dhcp database	Specifies DHCP for IPv6 binding database agent parameters.

show ipv6 dhcp guard policy

To display Dynamic Host Configuration Protocol for IPv6 (DHCPv6) guard information, use the **show ipv6 dhcp guard policy** command in privileged EXEC mode.

show ipv6 dhcp guard policy [*policy-name*]

Syntax Description

policy-name	(Optional) DHCPv6 guard policy name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)S	This command was introduced.

Usage Guidelines

If the *policy-name* argument is specified, only the specified policy information is displayed. If the *policy-name* argument is not specified, information is displayed for all policies.

Examples

The following is sample output from the **show ipv6 dhcp guard guard** command:

```
Router#show ipv6 dhcp guard policy

Dhcp guard policy: default
        Device Role: dhcp client
        Target: Et0/3

Dhcp guard policy: test1
        Device Role: dhcp server
        Target: vlan 0    vlan 1    vlan 2    vlan 3    vlan 4
        Max Preference: 200
        Min Preference: 0
        Source Address Match Access List: acl1
        Prefix List Match Prefix List: pfxlist1

Dhcp guard policy: test2
        Device Role: dhcp relay
        Target: Et0/0 Et0/1 Et0/2
```

The table below describes the significant fields shown in the display.

Table 51: show ipv6 dhcp guard Field Descriptions

Field	Description
Device Role	The role of the device. The role is either client, server or relay.

Field	Description
Target	The name of the target. The target is either an interface or a VLAN.

Related Commands

Command	Description
ipv6 dhcp guard policy	Defines the DHCPv6 guard policy name.

show ipv6 dhcp-ldra

To display configuration details and statistics for a Lightweight DHCPv6 Relay Agent (LDRA), use the **show ipv6 dhcp-ldra** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp-ldra [statistics]

Syntax Description

statistics	(Optional) Displays LDRA-related statistics.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)SG	This command was introduced.
Cisco IOS XE Release 3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.

Usage Guidelines

Use this command to view the number and type of DHCPv6 packets received or processed, the number and type of DHCPv6 messages dropped, error counters, and the interface state (client-facing trusted interface, server-facing interface, and so on).

You can also view LDRA configuration details, such as the type of LDRA configuration and the interface or VLAN where the LDRA is configured.

Example

The following sample output displays LDRA configuration details before initiating a DHCP session. The fields in the example below are self-explanatory.

```
Device> enable
Device # show ipv6 dhcp-ldra statistics


             DHCPv6 LDRA client facing statistics.

Messages received               0
Messages sent                   0
Messages discarded              0

                DHCPv6 LDRA server facing statistics.

Messages received               0
Messages sent                   0
Messages discarded              0
```

The following sample output displays LDRA configuration details after initiating a DHCP session. The fields in the example below are self-explanatory.

```
Device> enable

Device # show ipv6 dhcp-ldra statistics


               DHCPv6 LDRA client facing statistics.

Messages received               2
Messages sent                   2
Messages discarded              0

Messages                        Received
SOLICIT                         1
REQUEST                         1

Messages                        Sent
RELAY-FORWARD                   2

                DHCPv6 LDRA server facing statistics.


Messages received               2
Messages sent                   2
Messages discarded              0

Messages                        Received
RELAY-REPLY                     2

Messages                        Sent
ADVERTISE                       1
REPLY                           1
```

The following sample output displays LDRA configuration details. The fields in the example below are self-explanatory.

```
Device> enable
Device # show ipv6 dhcp-ldra



DHCPv6 LDRA is Enabled.
DHCPv6 LDRA policy: client-facing-disable
       Target: none
DHCPv6 LDRA policy: client-facing-trusted
       Target: vlan 5
DHCPv6 LDRA policy: client-facing-untrusted
       Target: none
DHCPv6 LDRA policy: server-facing
       Target: Gi1/0/7
```

Related Commands

Command	Description
ipv6 dhcp-ldra	Enables LDRA functionality on an access node.
ipv6 dhcp ldra attach-policy	Enables LDRA functionality on a VLAN.
ipv6 dhcp-ldra attach-policy	Enables LDRA functionality on an interface.

show ipv6 dhcp pool

To display Dynamic Host Configuration Protocol (DHCP) for IPv6 configuration pool information, use the **show ipv6 dhcp pool** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp pool [*poolname*]

Syntax Description

poolname	(Optional) User-defined name for the local prefix pool. The pool name can be a symbolic string (such as "Engineering") or an integer (such as 0).

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4(24)T	Command output was updated to display address pools and prefix pools.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Use the **ipv6 dhcp pool** command to create a configuration pool, and use the **ipv6 dhcp server** command to associate the configuration pool with a server on an interface.

The **show ipv6 dhcp pool** command displays DHCP for IPv6 configuration pool information. If the *poolname* argument is specified, only information on the specified pool is displayed. If the *poolname* argument is not specified, information about all pools is shown.

Examples

The following sample output displays DHCP for IPv6 configuration pool information:

```
Router# show ipv6 dhcp pool

DHCPv6 pool: svr-p1
  Static bindings:
    Binding for client 000300010002FCA5C01C
      IA PD: IA ID 00040002,
        Prefix: 3FFE:C00:C18:3::/72
                preferred lifetime 604800, valid lifetime 2592000
      IA PD: IA ID not specified; being used by 00040001
        Prefix: 3FFE:C00:C18:1::/72
                preferred lifetime 240, valid lifetime 54321
        Prefix: 3FFE:C00:C18:2::/72
                preferred lifetime 300, valid lifetime 54333
        Prefix: 3FFE:C00:C18:3::/72
                preferred lifetime 280, valid lifetime 51111
```

```
  Prefix from pool: local-p1, Valid lifetime 12345, Preferred lifetime 180
  DNS server: 1001::1
  DNS server: 1001::2
  Domain name: example1.net
  Domain name: example2.net
  Domain name: example3.net
Active clients: 2
```

The table below describes the significant fields shown in the display.

Table 52: show ipv6 dhcp pool Field Descriptions

Field	Description
DHCPv6 pool: svr-p1	The name of the pool.
IA PD	Identity association for prefix delegation (IAPD), which is a collection of prefixes assigned to a client.
IA ID	Identifier for this IAPD.
Prefix	Prefixes to be delegated to the indicated IAPD on the specified client.
preferred lifetime, valid lifetime	Lifetimes, in seconds, associated with the prefix statically assigned to the specified client.
DNS server	IPv6 addresses of the DNS servers.
Domain name	Displays the DNS domain search list.
Active clients	Total number of active clients.

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCP for IPv6 configuration information pool and enters DHCP for IPv6 pool configuration mode.
ipv6 dhcp server	Enables DHCP for IPv6 service on an interface.

show ipv6 dhcp interface

To display Dynamic Host Configuration Protocol (DHCP) for IPv6 interface information, use the **show ipv6 dhcp interface** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp interface [*type number*]

Syntax Description

type number	(Optional) Interface type and number. For more information, use the question mark (**?**) online help function.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.3(11)T	Command output was modified to allow relay agent information to be displayed on a specified interface if the relay agent feature is configured on that interface.
12.4(24)T	Command output was updated to display interface address assignments and T1 and T2 renew/rebind times.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

If no interfaces are specified, all interfaces on which DHCP for IPv6 (client or server) is enabled are shown. If an interface is specified, only information about the specified interface is displayed.

Examples

The following is sample output from the **show ipv6 dhcp interface**command. In the first example, the command is used on a router that has an interface acting as a DHCP for IPv6 server. In the second example, the command is used on a router that has an interface acting as a DHCP for IPv6 client:

```
Router1# show ipv6 dhcp interface
Ethernet2/1 is in server mode
  Using pool: svr-p1
  Preference value: 20
  Rapid-Commit is disabled
Router2# show ipv6 dhcp interface
Ethernet2/1 is in client mode
  State is OPEN (1)
  List of known servers:
    Address: FE80::202:FCFF:FEA1:7439, DUID 000300010002FCA17400
    Preference: 20
      IA PD: IA ID 0x00040001, T1 120, T2 192
```

```
    Prefix: 3FFE:C00:C18:1::/72
            preferred lifetime 240, valid lifetime 54321
            expires at Nov 08 2002 09:10 AM (54319 seconds)
    Prefix: 3FFE:C00:C18:2::/72
            preferred lifetime 300, valid lifetime 54333
            expires at Nov 08 2002 09:11 AM (54331 seconds)
    Prefix: 3FFE:C00:C18:3::/72
            preferred lifetime 280, valid lifetime 51111
            expires at Nov 08 2002 08:17 AM (51109 seconds)
  DNS server: 1001::1
  DNS server: 1001::2
  Domain name: domain1.net
  Domain name: domain2.net
  Domain name: domain3.net
Prefix name is cli-p1
Rapid-Commit is enabled
```

The table below describes the significant fields shown in the display.

Table 53: show ipv6 dhcp interface Field Descriptions

Field	Description
Ethernet2/1 is in server/client mode	Displays whether the specified interface is in server or client mode.
Preference value:	The advertised (or default of 0) preference value for the indicated server.
Prefix name is cli-p1	Displays the IPv6 general prefix pool name, in which prefixes successfully acquired on this interface are stored.
Using pool: svr-p1	The name of the pool that is being used by the interface.
State is OPEN	State of the DHCP for IPv6 client on this interface. "Open" indicates that configuration information has been received.
List of known servers	Lists the servers on the interface.
Address, DUID	Address and DHCP unique identifier (DUID) of a server heard on the specified interface.
Rapid commit is disabled	Displays whether the **rapid-commit** keyword has been enabled on the interface.

The following example shows the DHCP for IPv6 relay agent configuration on FastEthernet interface 0/0, and use of the **show ipv6 dhcp interface** command displays relay agent information on FastEthernet interface 0/0:

```
Router(config-if)# ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 FastEthernet0/1
Router# show ipv6 dhcp interface FastEthernet 0/0
FastEthernet0/0 is in relay mode
  Relay destinations:
    FE80::250:A2FF:FEBF:A056 via FastEthernet0/1
```

Related Commands

Command	Description
ipv6 dhcp client pd	Enables the DHCP for IPv6 client process and enables requests for prefix delegation through a specified interface.

Command	Description
ipv6 dhcp relay destination	Specifies a destination address to which client messages are forwarded and enables DHCP for IPv6 relay service on the interface.
ipv6 dhcp server	Enables DHCP for IPv6 service on an interface.

show ipv6 dhcp relay binding

To display DHCPv6 Internet Assigned Numbers Authority (IANA) and DHCPv6 Identity Association for Prefix Delegation (IAPD) bindings on a relay agent, use the **show ipv6 dhcp relay binding** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp relay binding [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.1(2)S	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(1)S	This command was modified. In addition to DHCPv6 IAPD bindings, DHCPv6 IANA bindings on a relay agent can be displayed.
Cisco IOS XE Release 3.5S	This command was modified. In addition to DHCPv6 IAPD bindings, DHCPv6 IANA bindings on a relay agent can be displayed.
12.2(33)SCF4	This command was implemented on Cisco uBR10012 and Cisco uBR7200 series universal broadband devices.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Usage Guidelines

If the **vrf** *vrf-name* keyword-argument pair is specified, all bindings belonging to the specified VRF are displayed.



Note Only the DHCPv6 IAPD bindings on a relay agent are displayed on the Cisco uBR10012 and Cisco uBR7200 series universal broadband devices.

Examples

The following is sample output from the **show ipv6 dhcp relay binding** command:

```
Device# show ipv6 dhcp relay binding
```

The following example shows output from the **show ipv6 dhcp relay binding** command with a specified VRF name on a Cisco uBR10012 universal broadband device:

```
Device# show ipv6 dhcp relay binding vrf vrf1

Prefix: 2001:DB8:0:1:/64 (Bundle100.600)
  DUID: 000300010023BED94D31
```

```
IAID: 3201912114
lifetime: 600
```

The table below describes the significant fields shown in the display.

Table 54: show ipv6 dhcp relay binding Field Descriptions

Field	Description
Prefix	IPv6 prefix for DHCP.
DUID	DHCP Unique Identifier (DUID) for the IPv6 relay binding.
IAID	Identity Association Identification (IAID) for DHCP.
lifetime	Lifetime of the prefix, in seconds.

Related Commands

Command	Description
clear ipv6 dhcp relay binding	Clears a specific IPv6 address or IPv6 prefix of a DHCP for IPv6 relay binding.

show ipv6 dhcp route

To display routes added by Dynamic Host Configuration Protocol for IPv6 (DHCPv6) on the DHCPv6 server for Internet Assigned Numbers Authority (IANA) and Identity Association for Prefix Delegation (IAPD), use the **show ipv6 dhcp route** command in privileged EXEC mode.

show ipv6 dhcp route {**vrf** *vrf-name*} {**ipv6-addressipv6-prefix*}

Syntax Description

vrf *vrf-name*	Specifies a virtual routing and forwarding (VRF) configuration.
*	Displays all the DHCPv6 relay bindings.
ipv6-address	DHCPv6 address.
ipv6-prefix	IPv6 prefix.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(1)S	This command was introduced.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.

Examples

The following is sample output from the **show ipv6 dhcp route** command:

```
Router# show ipv6 dhcp route vrf vrfname 2001:0DB8:3333:4::5/126
```

Related Commands

Command	Description
ipv6 dhcp iana-route-add	Adds routes for individually assigned IPv6 addresses on a relay or server.
ipv6 dhcp iapd-route-add	Enables route addition by the DHCPv6 relay and server for the delegated prefix.

show ip nat pool platform

To display results of **show platform software nat fp active pool** command, use the **show ip nat pool platform** command in user EXEC or privileged EXEC mode.

show ip nat pool platform

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

The following is sample output from the **show ip nat pool platform** command :

Examples

```
Device# show ip nat pool name natpool1 platform

Dump NAT pool config
ID: 1, Name: nat_pool1, Type: Generic, Mask: 255.255.0.0
Flags: Unknown, Acct name:
Address range blocks: 1
Start: 192.0.2.1, End: 192.0.2.254
Last stats update: 02/28 05:57:02.263
Last refcount value: 1
```

show ip nat pool name platform

To display combined results of **show platform hardware qfp active feature nat datapath pool** and **show platform software nat f0 pool-stats id** command, use the **show ip nat pool name platform** command in user EXEC or privileged EXEC mode.

show ip nat pool platform

Syntax Description

pool-name	Name of the NAT address pool for which information will be displayed.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

The following is sample output from the **show ip nat pool name platform** command :

Examples

```
Device# show ip nat pool name natpool1 platform

Total translations: 2 (0 static, 2 dynamic; 0 extended)
Outside interfaces: Serial0
Inside interfaces: Ethernet1
Hits: 135 Misses: 5
Expired translations: 2
Dynamic mappings:
-- Inside Source
access-list 1 pool net-208 refcount 2
pool net-208: netmask 255.255.255.240
start 172.16.233.208 end 172.16.233.221
type generic, total addresses 14, allocated 2 (14%), misses 0
```

show ipv6 nat statistics

To display Network Address Translation--Protocol Translation (NAT-PT) statistics, use the **show iv6 nat statistics**command in user EXEC or privileged EXEC mode.

show ipv6 nat statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Examples

The following is sample output from the **show ipv6 nat statistics**command:

```
Router# show ipv6 nat statistics
Total active translations: 4 (2 static, 2 dynamic; 2 extended)
NAT-PT interfaces:
  Ethernet3/1, Ethernet3/3
Hits: 1  Misses: 1
Expired translations: 0
```

The table below describes the significant fields shown in the display.

Table 55: show ipv6 nat statistics Field Descriptions

Field	Description
Total active translations	Number of translations active in the system. This number increments by one each time a translation is created and is decremented each time a translation is cleared or times out. Displays the numbers for each type of translation.
NAT-PT interfaces	The interfaces, by type and number, that are configured to run NAT-PT translations.
Hits	Number of times the software does a translations table lookup and finds an entry.
Misses	Number of times the software does a translations table lookup, fails to find an entry, and must try to create one.
Expired translations	Cumulative count of translations that have expired since the router was booted.

Related Commands

Command	Description
show ipv6 nat translations	Displays active NAT-PT translations.

show ipv6 nat translations

To display active Network Address Translation--Protocol Translation (NAT-PT) translations, use the **show ip nat translations** command in user EXEC or privileged EXEC mode.

show ipv6 nat translations [**icmp** | **tcp** | **udp**] [**verbose**]

Syntax Description

icmp	(Optional) Displays detailed information about NAT-PT ICMP translation events.
tcp	(Optional) Displays detailed information about NAT-PT TCP translation events.
udp	(Optional) Displays detailed information about NAT-PT User Datagram Protocol (UDP) translation events.
verbose	(Optional) Displays additional information for each translation table entry, including how long ago the entry was created and used.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Examples

The following is sample output from the **show ip nat translations** command. Two static translations have been configured between an IPv4 source address and an IPv6 destination, and vice versa.

```
Router# show ipv6 nat translations
Prot  IPv4 source              IPv6 source
      IPv4 destination         IPv6 destination
---   ---                      ---
      192.168.123.2            2001::2
---   ---                      ---
      192.168.122.10           2001::10
tcp   192.168.124.8,11047      3002::8,11047
      192.168.123.2,23         2001::2,23
udp   192.168.124.8,52922      3002::8,52922
      192.168.123.2,69         2001::2,69
udp   192.168.124.8,52922      3002::8,52922
      192.168.123.2,52922      2001::2,52922
---   192.168.124.8            3002::8
      192.168.123.2            2001::2
---   192.168.124.8            3002::8
      ---                      ---
---   192.168.121.4            5001::4
      ---                      ---
```

The following is sample output that includes the **verbose** keyword:

```
Router# show ipv6 nat translations verbose
Prot  IPv4 source              IPv6 source
      IPv4 destination         IPv6 destination
```

```
---   ---                       ---
      192.168.123.2             2001::2
      create 00:04:24, use 00:03:24,
---   ---                       ---
      192.168.122.10            2001::10
      create 00:04:24, use 00:04:24,
tcp   192.168.124.8,11047       3002::8,11047
      192.168.123.2,23          2001::2,23
      create 00:03:24, use 00:03:20, left 00:16:39,
udp   192.168.124.8,52922       3002::8,52922
      192.168.123.2,69          2001::2,69
      create 00:02:51, use 00:02:37, left 00:17:22,
udp   192.168.124.8,52922       3002::8,52922
      192.168.123.2,52922       2001::2,52922
      create 00:02:48, use 00:02:30, left 00:17:29,
---   192.168.124.8             3002::8
      192.168.123.2             2001::2
      create 00:03:24, use 00:02:34, left 00:17:25,
---   192.168.124.8             3002::8
      ---                       ---
      create 00:04:24, use 00:03:24,
---   192.168.121.4             5001::4
      ---                       ---
      create 00:04:25, use 00:04:25,
```

The table below describes the significant fields shown in the display.

Table 56: show ipv6 nat translations Field Descriptions

Field	Description
Prot	Protocol of the port identifying the address.
IPv4 source/IPv6 source	The IPv4 or IPv6 source address to be translated.
IPv4 destination/IPv6 destination	The IPv4 or IPv6 destination address.
create	How long ago the entry was created (in hours:minutes:seconds).
use	How long ago the entry was last used (in hours:minutes:seconds).
left	Time before the entry times out (in hours:minutes:seconds).

Related Commands

Command	Description
clear ipv6 nat translation	Clears dynamic NAT-PT translations from the translation state table.

show logging ip access-list

To display information about the logging IP access list, use the **show logging ip access-list** command in privileged EXEC mode.

show logging ip access-list {**cache** | **config**}

Syntax Description

cache	Displays information about all the entries in the Optimized ACL Logging (OAL) cache.
config	Displays information about the logging IP access-list configuration.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXE	This command was changed to include the **config** keyword on the Supervisor Engine 720 only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720 only.

OAL is supported on IPv4 unicast traffic only.

Examples

This example shows how to display all the entries in the OAL cache:

```
Router# show logging ip access-list cache
Matched flows:
id prot src_ip dst_ip sport dport status count
total lastlog
-------------------------------------------------------------------------------------
1 17 10.2.1.82 10.2.12.2 111 63 Permit 0
3906 2d02h
2 17 10.2.1.82 10.2.12.2 1135 63 Permit 0
3906 2d02h
3 17 10.2.1.82 10.2.12.2 2159 63 Permit 0
3906 2d02h
4 17 10.2.1.82 10.2.12.2 3183 63 Permit 0
3906 2d02h
5 17 10.2.1.82 10.2.12.2 4207 63 Permit 0
3906 2d02h
6 17 10.2.1.82 10.2.12.2 5231 63 Deny 0
3906 2d02h
7 17 10.2.1.82 10.2.12.2 6255 63 Deny 0
3906 2d02h
8 17 10.2.1.82 10.2.12.2 7279 63 Permit 0
3906 2d02h
9 17 10.2.1.82 10.2.12.2 8303 63 Permit 0
```

```
3906 2d02h
10 17 10.2.1.82 10.2.12.2 9327 63 Permit 0
3905 2d02h
11 17 10.2.1.82 10.2.12.2 10351 63 Permit 0
3905 2d02h
12 17 10.2.1.82 10.2.12.2 11375 63 Permit 0
3905 2d02h
13 17 10.2.1.82 10.2.12.2 12399 63 Deny 0
3905 2d02h
14 17 10.2.1.82 10.2.12.2 13423 63 Permit 0
3905 2d02h
15 17 10.2.1.82 10.2.12.2 14447 63 Deny 0
3905 2d02h
16 17 10.2.1.82 10.2.12.2 15471 63 Permit 0
3905 2d02h
17 17 10.2.1.82 10.2.12.2 16495 63 Permit 0
3905 2d02h
18 17 10.2.1.82 10.2.12.2 17519 63 Permit 0
3905 2d02h
19 17 10.2.1.82 10.2.12.2 18543 63 Permit 0
3905 2d02h
20 17 10.2.1.82 10.2.12.2 19567 63 Permit 0
3905 2d02h
Number of entries: 20
Number of messages logged: 112
Number of packets logged: 11200
Number of packets received for logging: 11200
```

This example shows how to display information about the logging IP access-list configuration:

```
Router# show logging ip access-list config
Logging ip access-list configuration
 Maximum number of cached entries: 8192
 Logging rate limiter: 0
 Log-update interval: 300
 Log-update threshold: 0
 Configured on input direction:
        Vlan2
        Vlan1
 Configured on output direction:
        Vlan2
```

Related Commands

Command	Description
clear logging ip access-list cache	Clears all the entries from the OAL cache and sends them to the syslog.
logging ip access-list cache (global configuration)	Configures the OAL parameters.
logging ip access-list cache (interface configuration)	Enables an OAL-logging cache on an interface that is based on direction.

show mdns cache

To display multicast Domain Name System (mDNS) cache information, use the **show mdns cache** command in user EXEC or privileged EXEC mode.

show mdns cache [**interface** *type number* [**detail**] | [**name** *record-name*] [**type** *record-type*] [**detail**]]

Syntax Description

interface *type number*	(Optional) Displays mDNS cache information for the specified interface.
detail	(Optional) Displays detailed mDNS cache information for the specified interface or record. **Note** You can use the **detail** keyword for a specific interface, record or type. You cannot use it independently with the **show mdns cache** command.
name *record-name*	(Optional) Displays mDNS cache information for the specified record.
type *record-type*	(Optional) Displays mDNS cache information for the specific record type.

Note You can view mDNS cache information for a specific record type and record name by using the keyword-argument pair combination **name** *record-name* **type** *record-type*.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.2(1)E	This command was introduced.
15.2(1)SY	This command was integrated into Cisco IOS Release 15.2(1)SY.
15.5(2)S	This command was integrated into Cisco IOS Release 15.5(2)S.

Examples

The following sample output displays mDNS cache information :

```
Device> enable
Device# show mdns cache


mDNS CACHE
==================================
 [<NAME>] [<TYPE>][<CLASS>] [<TTL>/Remaining] [Accessed] [If-index] [<RR
 Record Data>]
```

```
_services._dns-sd._udp.local PTR IN 4500/4496 0 3 _ipp._tcp.local

_ipp._tcp.local PTR IN 4500/4496 1 3 printer1._ipp._tcp.local

printer1._ipp._tcp.local TXT IN 4500/4496 1 3 (1)''
```

Related Commands

Command	Description
service-list mdns-sd	Creates a service-list and applies a filter on the service-list or associates a query for the service-list.
show mdns requests	Displays mDNS request information.
show mdns statistics	Displays mDNS statistics for the specified service-list.

show mdns cache mac

To display multicast Domain Name System (mDNS) cache information for a specific MAC address, use the **show mdns cache mac** command in user EXEC or privileged EXEC mode.

show mdns cache mac *mac-address* [**detail**]

Syntax Description

mac-address	Displays mDNS cache information for the specified MAC address.
detail	(Optional) Displays detailed mDNS cache information for the specified MAC address.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.2(2)E	This command was introduced.
Cisco IOS XE 3.6E	This command was integrated into the Cisco IOS XE 3.6E release.

Examples

The following is sample output from the **show mdns cache mac** command:

```
Device> enable
Device# show mdns cache mac aabb.cc01.2c10

mDNS CACHE
==================================

[<NAME>]                                                [<TYPE>][<CLASS>]
[<TTL>/Remaining] [Accessed] [If-name] [Mac Address] [<RR Record Data>]
_mdnsgateway._udp.local                                    PTR     IN
1200/1200         1          0
mdnsgateway-Et0/1._mdnsgateway._udp.local
```

The table below describes the significant fields in the display.

Table 57: show mdns cache mac Field Descriptions

Field	Description
[<NAME>]	Service instance. The service instance is of the specified service type.
[<TYPE>]	Service type.
[<CLASS>]	DNS class. IN refers to the internet class resource record.

Field	Description
[<TTL>/Remaining]	Time to Live (TTL) value of the service.
[If-name]	Interface name.
[Mac Address]	MAC address of the device.
[<RR Record Data>]	Resource record data. The data includes service instance information and the interface name.

Related Commands

Command	Description
service-list mdns-sd	Creates a service-list and applies a filter on the service-list or associates a query for the service-list.
show mdns cache	Displays mDNS cache information for the device.
show mdns cache static	Displays mDNS service instance records in cache that are statically registered.

show mdns cache static

To display multicast Domain Name System (mDNS) service instance records in cache that are statically registered, use the **show mdns cache static** command in user EXEC or privileged EXEC mode.

show mdns cache static

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.2(2)E	This command was introduced.
Cisco IOS XE 3.6E	This command was integrated into the Cisco IOS XE 3.6E release.

Examples

The following is sample output from the **show mdns cache static** command:

```
Device> enable
Device# show mdns cache static

mDNS CACHE
==================================

[<NAME>]                                                [<TYPE>][<CLASS>]
[<TTL>/Remaining] [Accessed] [If-name] [Mac Address] [<RR Record Data>]
_mdnsgateway._udp.local                                    PTR     IN
1200/1200       1       0
mdnsgateway-Et0/1._mdnsgateway._udp.local
_mdnsgateway._udp.local                                    PTR     IN
 600/600        1       0              mdnsgateway._mdnsgateway._udp.local
```

The table below describes the significant fields in the display.

Table 58: show mdns cache static Field Descriptions

Field	Description
[<NAME>]	Service instance. The service instance is of the specified service type.
[<TYPE>]	Service type.
[<CLASS>]	DNS class. IN refers to the internet class resource record.
[<TTL>/Remaining]	Time to Live (TTL) value of the service.

Field	Description
[If-name]	Interface name.
[Mac Address]	MAC address of the device.
[<RR Record Data>]	Resource record data. The data includes service instance information and the interface name.

Related Commands

Command	Description
service-list mdns-sd	Creates a service-list and applies a filter on the service-list or associates a query for the service-list.
show mdns cache	Displays mDNS cache information for the device.
show mdns cache mac	Displays mDNS cache information for a specific MAC address.

show mdns requests

To display multicast Domain Name System (mDNS) request information, use the **show mdns requests** command in privileged EXEC mode.

show mdns requests [**detail** | [**type** *record-type*] [**name** *record-name*]]

Syntax Description

detail	(Optional) Displays detailed mDNS request information, including record name, record type, and record class.
name *record-name*	(Optional) Displays mDNS request information for the specified record.
type *record-type*	(Optional) Displays mDNS request information for a specific record type. **Note** For the *record-type* argument, you must specify one of these record types - PTR, SRV, A, or AAAA.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(1)E	This command was introduced.
Cisco IOS XE Release 3.15S	This command was integrated into the Cisco IOS XE Release 3.13S
15.5(2)S	This command was integrated into Cisco IOS Release 15.5(2)S.

Examples

The following sample output displays detailed mDNS request information :

```
Device> enable
Device# show mdns requests detail


MDNS Outstanding Requests
================================
Request name  :   _ipp._tcp.local
Request type  :   PTR
Request class :   IN
```

Related Commands

Command	Description
service-list mdns-sd	Creates a service-list and applies a filter on the service-list or associates a query for the service-list.
show mdns cache	Displays mDNS cache information.

Command	Description
show mdns statistics	Displays mDNS statistics for the specified service-list.

show mdns service-types

To display multicast Domain Name System (mDNS) service type information for device interfaces, use the **show mdns service-types** command in user EXEC or privileged EXEC mode.

show mdns service-types [**all** | **interface** *type number*]

Syntax Description

all	(Optional) Displays mDNS service type information for all device interfaces.
interface *type number*	(Optional) Displays mDNS service type information for the specified interface.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.2(2)E	This command was introduced.
Cisco IOS XE 3.6E	This command was integrated into the Cisco IOS XE 3.6E release.

Examples

The following is sample output from the **show mdns service-types** command:

```
Device> enable
Device# show mdns service-types


mDNS SERVICES
================================
[<NAME>]            [<TTL>/Remaining] [If-name]

_ipp._tcp.local     4500/4496
```

The table below describes the significant fields in the display.

Table 59: show mdns service-types Field Descriptions

Field	Description
[<NAME>]	Service instance. The service instance is of the specified service type.
[<TTL>/Remaining]	Time to Live (TTL) value of the service.
[If-name]	Interface name.

Related Commands

Command	Description
service-list mdns-sd	Creates a service-list and applies a filter on the service-list or associates a query for the service-list.
show mdns requests	Displays mDNS request information.
show mdns statistics	Displays mDNS statistics for the specified service-list.

show mdns statistics

To display multicast Domain Name System (mDNS) statistics, use the **show mdns statistics** command in user EXEC or privileged EXEC mode.

show mdns statistics {**all** | **interface** *type number* | **service-list** *name* | [**cache** | **service-policy**] {**all** | **interface** *type number*} | **services orderby providers**}

Syntax Description

all	Displays mDNS statistics for the device or service-policy.
interface *type number*	Displays mDNS statistics or service-policy statistics for the specified interface.
service-list *name*	Displays mDNS statistics for the specified service-list.
cache	Displays mDNS cache statistics.
service-policy	Displays mDNS service-policy statistics.
services orderby providers	Displays the number of services learnt from each client. The services are displayed in the descending order; the client from which most number of services are learnt is displayed first on the list, and so on.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.2(1)E	This command was introduced.
15.2(2)E	This command was modified. The keyword-argument pair **service-list** *name* and the option to display mDNS statistics for an interface were added. The keywords **cache** and **services orderby providers** were added.
Cisco IOS XE 3.6E	This command was integrated into the Cisco IOS XE 3.6E release.
15.2(1)SY	This command was integrated into Cisco IOS Release 15.2(1)SY.
Cisco IOS XE Release 3.15S	This command was integrated into the Cisco IOS XE Release 3.15S
15.5(2)S	This command was integrated into Cisco IOS 15.5(2)S Release.

Usage Guidelines

The **all** keyword can be used in two forms of the **show mdns statistics** command. You can view mDNS statistics for the device using the **show mdns statistics all** command form. To view service-policy statistics, use the **show mdns statistics service-policy all** command form.

The keyword-argument pair **interface** *type number* can be used in two forms of the **show mdns statistics** command. To display mDNS statistics for a specific interface, use the **show mdns statistics interface** *type number* command form. To display service-policy statistics for a specific interface, use the **show mdns statistics service-policy interface** *type number* command form.

Examples

The following sample output displays detailed mDNS statistics:

```
Device> enable
Device# show mdns statistics all


 mDNS Statistics
================================
 mDNS packets sent : 0
 mDNS packets received : 31
 mDNS packets dropped : 8
 mDNS cache memory in use: 64264(bytes)
```

Related Commands

Command	Description
service-list mdns-sd	Creates a service-list and applies a filter on the service-list or associates a query for the service-list.
show mdns cache	Displays mDNS cache information.
show mdns requests	Displays mDNS request information.

show nat64

To display Network Address Translation 64 (NAT64) information, use the **show nat64** command in user EXEC or privileged EXEC mode.

show nat64 {**logging** | **services** | **timeouts** | **reconciliation** | **replications**}

Syntax Description

logging	Displays NAT64 logging information.
services	Displays NAT64 services information.
timeouts	Displays statistics for a NAT64 translation session timeout.
reconciliation	Displays NAT64 reconciliation information.
replications	Displays NAT64 replication information.

Command Modes

User EXEC (>)

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was modified. The **reconciliation** and **replications** keywords were added.
15.4(1)T	This command was integrated into Cisco IOS Release 15.4(1)T

Usage Guidelines

NAT64 supports logging of information about all NAT sessions that are created and deleted. All event entries that are logged have a time stamp. Use the output of this command verify your NAT64 configuration.

The output of the **show nat64 reconciliation** command displays information about Forwarding Processor (FP) switchovers. Whenever an FP does a switchover, the Route Processor (RP) and the newly active FP audit their own configuration and alias data to ensure that the RP and the newly active FP are synchronized.

Replication indicates whether the traffic to a port is replicated or not. The **show nat64 replications** command displays the state of any port that needs to be treated specially for replication. By default, HTTP (port 80) sessions are not synchronized.

Examples

The following is sample output from the **show nat64 logging** command:

```
Device# show nat64 logging

NAT64 Logging Type
   Method          Protocol Dst. Address    Dst. Port Src. Port

translation
   flow export     UDP      10.1.1.1         5000      60087
```

The table below describes the significant fields shown in the display.

Table 60: show nat64 logging Field Descriptions

Field	Description
Method	Method used for logging records. Depending on your release, only flow export is supported.
Protocol	Protocol used for translation.
Dst. Address	Destination IPv4 address of the external collector that is configured for logging records.
Dst. Port	Destination port of the external collector that is configured for logging records.
Src. Port	Source port from where logging records are sent out on the network.

The following is sample output from the **show nat64 services** command:

```
Device# show nat64 services

NAT64 Services

ftp
   UDP Enabled: TRUE
   TCP Enabled: TRUE
   Service Definition
   Protocol: 6 Port: 21
```

The table below describes the significant fields shown in the display.

Table 61: show nat64 services Field Descriptions

Field	Description
UDP Enabled	Indicates whether the service translation is enabled by default for UDP packets if the protocol is supported by the service definition.
TCP Enabled	Indicates whether the service translation is enabled by default for TCP packets if the protocol is supported by the service definition.
Service Definition	Definition of the service (the Protocol and Port fields for which packets are considered a match to the given service).

The following is sample output from the **show nat64 timeouts** command:

```
Device# show nat64 timeouts
```

```
NAT64 Timeout
   Seconds     CLI Cfg Uses 'All' all flows
   86400       FALSE   FALSE      udp
   300         FALSE   TRUE       tcp
   7200        FALSE   TRUE       tcp-transient
   240         FALSE   FALSE      icmp
   60          FALSE   TRUE
```

The table below describes the significant fields shown in the display.

Table 62: show nat64 timeouts Field Descriptions

Field	Description
Seconds	NAT64 timeout, in seconds.
CLI Cfg	Indicates whether the timeout is explicitly configured through the CLI. The timeout values configured through the CLI change the default timeout values.

The following is sample output from the **show nat64 reconciliation** command:

```
Device# show nat64 reconciliation

 Reconciliation Info

   Start updates received: 0
   End updates received: 0
   Last update received: --- (2)
```

The table below describes the significant fields shown in the display.

Table 63: show nat64 reconciliation Field Descriptions

Field	Description
Start updates received	Indicates the number of synchronization events that are started.
End updates received	Indicates the number of synchronization events that are completed.
Last updated received	Indicates which event was received last—the start or end event.

The following is sample output from the **show nat64 replications** command:

```
Device# show nat64 replications

 Replications configured for http: 1

 NAT64 Replications (ports not shown have replication enabled)
 Traffic Type     Port  Replication User-Configured

 http             80    disable     FALSE
```

The table below describes the significant fields shown in the display.

Table 64: show nat64 reconciliation Field Descriptions

Field	Description
Traffic type	Type of traffic.
Port	Layer 4 port of the traffic.
Replication	Indicates whether the traffic will be replicated or not. Valid values are enable (replicated) or disable (not replicated).
User-Configured	Indicates whether the replication is because of the default behavior (FALSE) of the traffic or user configuration (TRUE).

Related Commands

Command	Description
nat64 logging	Enables NAT64 logging.
nat64 service ftp	Enables NAT64 FTP service.
nat64 translation	Enables NAT64 translation.

show nat64 adjacency

To display information about the stateless Network Address Translation 64 (NAT64) managed adjacencies, use the **show nat64 adjacency** command in user EXEC or privileged EXEC mode.

show nat64 adjacency {**all** | **count** | **ipv4** | **ipv6**}

Syntax Description

all	Displays all adjacencies.
count	Displays the adjacency count.
ipv4	Displays IPv4 adjacencies.
ipv6	Displays IPv6 adjacencies.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.
15.4(1)T	This command was integrated into Cisco IOS Release 15.4(1)T.

Usage Guidelines

An adjacency is a node that can be reached by one Layer 2 hop. The stateless NAT64 adjacencies include adjacency addresses and the total number of adjacencies.

Examples

The following is sample output from the **show nat64 adjacency all** command:

```
Device# show nat64 adjacency all

Adjacency Counts
 IPv4 Adjacencies: 2
 IPv6 Adjacencies: 1
 Stateless Prefix Adjacency Ref Count: 1
Adjacencies
 IPv6 Adjacencies
    ::42
 IPv4 Adjacencies
    0.0.19.137 (5001)
    0.0.19.140 (5004)
```

The table below describes the significant fields shown in the display.

Table 65: show nat64 adjacency all Field Descriptions

Field	Description
Adjacency Counts	Count of all adjacencies.
Adjacencies	Types of adjacencies.

Related Commands

Command	Description
nat64 enable	Enables stateless NAT64 on an interface.

show nat64 aliases

To display the IP aliases created by Network Address Translation 64 (NAT64), use the **show nat64 aliases** command in user EXEC or privileged EXEC mode.

show nat64 aliases [**range** *lower-address-range upper-address-range*]

Syntax Description

range	(Optional) Displays information about the IP aliases in a given range.
lower-address-range	(Optional) IPv4 lower address range.
upper-address-range	(Optional) IPv4 upper address range.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.4(2)T	This command was integrated into Cisco IOS Release 15.4(2)T.

Usage Guidelines

An alias is an address (examples of an address are pool addresses and static mapping addresses) for which the router sends an Address Resolution Protocol (ARP) request even though the address is not configured on an interface. NAT64 maintains a database of all the addresses for which an ARP request is sent. These addresses are inserted in the database as IP aliases when they exist on the subnet of an interface address.

Examples

The following is sample output from the **show nat64 aliases** command:

```
Device# show nat64 aliases

Aliases configured: 1

Address   Table ID Inserted  Flags  Send ARP Reconcilable Stale Ref-Count

10.1.1.1    0        FALSE   0x0030 FALSE    TRUE         FALSE 1
```

The table below describes the significant fields shown in the display.

Table 66: show nat64 aliases Field Descriptions

Field	Description
Aliases configured	The number of NAT64 addresses for which an IP alias is configured.
Address	IPv4 address of the alias.

Field	Description
Table ID	VPN routing and forwarding (VRF) table ID that is associated with the alias.
Inserted	Indicates whether the alias is currently inserted as an IP alias.
Send ARP	Indicates whether an ARP request is sent. Valid values are TRUE or FALSE.

Related Commands

Command	Description
nat64 enable	Enables NAT64 on an interface.

show nat64 ha status

To display information about the stateless Network Address Translation 64 (NAT64) high availability (HA) status, use the **show nat64 ha status**command in user EXEC or privileged EXEC mode.

show nat64 ha status

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Examples

The following is sample output from the **show nat64 ha status** command:

```
Router# show nat64 ha status
NAT64 HA Status
 Role: active
 Peer is ready: TRUE
 Peer is compatible: TRUE
 Synchronization enabled: TRUE
 Is hot (standby): FALSE
 Bulk sync PID: NO_PROCESS
 ISSU negotiation status: IPC, CF
 ISSU context IDs: IPC(198), CF(197)
 Synchronization capabilities: 0x00000001
  Adjacency mappings: TRUE
 CF info: handle(0x0000011B), peer ready(TRUE),
  flow control(TRUE)(FALSE)(0x0)
 Initialized: HA(TRUE) ISSU(TRUE)
 Message stats:
  Adjacency mapping: rx(0) tx(5001) tx err(0)
  Bulk sync done: rx(0) tx(1) tx err(0)
 Errors:
  Bulk sync: 0
  CF tx: 0
```

The table below describes the significant fields shown in the display.

Table 67: show nat64 ha status Field Descriptions

Field	Description
NAT64 HA Status	Status of stateless NAT64 HA.
Message stats	Status of the messages.
Errors	Types of errors.

Related Commands

Command	Description
clear nat64 ha statistics	Clears stateless NAT64 HA statistics.
nat64 enable	Enables stateless NAT64 on an interface.

show nat64 limits

To display Network Address Translation 64 (NAT64) limits, use the **show nat64 limits** command in user EXEC or privileged EXEC mode.

show nat64 limits

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.4(2)T	This command was integrated into Cisco IOS Release 15.4(2)T.

Usage Guidelines

The **show nat64 limits** command displays the configured maximum limit for the number of entries that NAT64 translates.

Examples

The following is sample output from the **show nat64 limits** command:

```
Device# show nat64 limits

NAT64 Limit     Max Entries Is Configured

global          200         TRUE
```

The table below describes the fields shown in the display.

Table 68: show nat64 limits Field Descriptions

Field	Description
NAT64 Limit	Indicates whether the NAT64 translation limit is configured globally or on an interface.
Max Entries	The maximum number of entries that NAT64 translates.
Is Configured	Indicates whether the maximum limit is configured. Valid values are True or False.

Related Commands

Command	Description
nat64 enable	Enables NAT64 on an interface.

Command	Description
nat64 translation	Enables NAT64 translation.

show nat64 map-t

To display Network Address Translation 64 (NAT64) mapping of addresses and ports (MAP-T) information, use the **show nat64 map-t** command in privileged EXEC mode.

show nat64 map-t [**domain** *number*]

Syntax Description

domain *number*	Displays MAP-T information for a specific domain. Valid values for the *number* argument are from 1 to 128.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

MAP-T or Mapping of address and port (MAP) double stateless translation-based solution (MAP-T) provides IPv4 hosts connectivity to and across an IPv6 domain. MAP-T builds on existing stateless IPv4/IPv6 address translation techniques that are specified in RFC 6052, RFC 6144, and RFC 6145.

Examples

The following is sample output from the **show nat64 map-t domain**command:

```
Device# show nat64 map-t domain 89

MAP-T Domain 89
   Mode MAP-T
   Default-mapping-rule
      Ip-v6-prefix ::/0
   Basic-mapping-rule
      Ip-v6-prefix ::/0
      Ip-v4-prefix 10.1.1.1/32
      Port-parameters
         Share-ratio 34   Contiguous-ports 64   Start-port 3455
         Share-ratio-bits 6   Contiguous-ports-bits 6   Port-offset-bits 4
```

The

Related Commands

Command	Description
nat64 map-t	Configures NAT64 MAP-T settings

show nat64 mappings dynamic

To display the Network Address Translation 64 (NAT64) dynamic mappings, use the **show nat64 mappings dynamic** command in user EXEC or privileged EXEC mode.

show nat64 mappings dynamic [**list** *acl-name* | **pool** *pool-name*]

Syntax Description

list *acl-name*	(Optional) Displays the mappings of a specified access list.
pool *pool-name*	(Optional) Displays the mappings of a specified pool.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.4(2)T	This command was integrated into Cisco IOS Release 15.4(2)T.

Usage Guidelines

Dynamic one-to-one mapping is used to map IPv6 hosts from a pool of available IPv4 addresses on a first-come first-served basis. The dynamic one-to-one configuration is deployed when the number of IPv6 hosts is few and an equal or greater number of public IPv4 addresses are available. For dynamic binds, the mapping is always between an IPv4 address and an IPv6 address.

Examples

The following is sample output from the **show nat64 mappings dynamic** command:

```
Device# show nat64 mappings dynamic

Dynamic mappings configured: 1

Direction       ACL         Pool        Flags

v6v4            mylist      mypool      0x00000000 (none)
```

The table below describes the significant fields shown in the display.

Table 69: show nat64 mappings dynamic Field Descriptions

Field	Description
Dynamic mappings configured	The number of dynamic mappings configured.
Direction	The direction in which the dynamic mapping is configured.
ACL	Access list name.

Field	Description
Pool	Name of the pool.

Related Commands

Command	Description
nat64 v4v6	Translates an IPv4 source address to an IPv6 source address and an IPv6 destination address to an IPv4 destination address for NAT64.
nat64 v6v4	Translates an IPv6 source address to an IPv4 source address and an IPv4 destination address to an IPv6 destination address for NAT64.

show nat64 pools

To display the IPv4 address pools for dynamic Network Address Translation 64 (NAT64) mapping, use the **show nat64 pools** command in user EXEC or privileged EXEC mode.

show nat64 pools [**name** *pool-name* | **range** *lower-address-range upper-address-range*] [**routes**]

Syntax Description

name *pool-name*	(Optional) Displays information about the configured address pools listed by the pool name.
range	(Optional) Displays information about address pools within a provided address range.
lower-address-range	(Optional) IPv4 lower address range.
upper-address-range	(Optional) IPv4 upper address range.
routes	(Optional) Displays static routes for a given pool.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.4(2)T	This command was integrated into Cisco IOS Release 15.4(2)T.

Usage Guidelines

Pools allow you to specify an IPv4 address range that is used for dynamic mapping of objects. Only IPv4 address pools and one contiguous address range per pool object is supported in Cisco IOS XE Release 3.4S. When a pool is created, a static route is installed for all addresses in the pool range.

Examples

The following is sample output from the **show nat64 pools** command:

```
Device# show nat64 pools

Pools configured: 1

Protocol Name    Is Single    Range                    Ranges

IPv4     mypool   TRUE        (10.1.1.1 - 10.1.1.10)  10.1.1.1 - 10.1.1.10
```

The table below describes the fields shown in the display.

Table 70: show nat64 pools Field Descriptions

Field	Description
Protocol	Name of the protocol.

Field	Description
Name	Name of the configured pool.
Is Single	Indicates whether the pool contains a single address range or multiple address ranges. The value of the range is displayed. In Cisco IOS XE Release 3.4S only a single address range is supported.
Range	IPv4 address range.
Ranges	All address ranges for the pool. In Cisco IOS XE Release 3.4S only a single address range is supported.

Related Commands

Command	Description
nat64 enable	Enables NAT64 on an interface.
nat64 v4	Enables NAT64 IPv4 configuration.

show nat64 prefix stateful

To display information about Network Address Translation 64 N(AT64) stateful prefixes, use the **show nat64 prefix stateful** command in user EXEC or privileged EXEC mode.

show nat64 prefix stateful {**global** | {**interfaces** | **static-routes**} [**prefix** *ipv6-address*/*prefix-length*]}

Syntax Description

global	Displays information about global prefixes.
interfaces	Displays information about the configured interfaces.
prefix	(Optional) Displays information about interfaces that use a prefix.
ipv6-address	(Optional) IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/prefix-length	(Optional) Length of the IPv6 prefix. Prefix length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. Valid values are from 0 to 128.
static-routes	Displays information about prefix static routes.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.4(2)T	This command was integrated into Cisco IOS Release 15.4(2)T.

Usage Guidelines

A maximum of one global stateful prefix and one stateful prefix per interface is supported. NAT64 uses the configured stateful prefix to algorithmically translate the IPv4 addresses of the IPv4 hosts to and from IPv6 addresses. If a global stateful prefix or an interface stateful prefix is not configured, the Well Known Prefix (WKP) of 64:ff9b::/96 is used to translate the IPv4 address of the IPv4 host.

Examples

The following is sample output from the **show nat64 prefix stateful global** command:

```
Device# show nat64 prefix stateful global

Global Stateful Prefix: is valid, 2001:DB8::/96
IFs Using Global Prefix    Gi0/1/0
```

The following is sample output from the **show nat64 prefix stateful interfaces** command:

```
Device# show nat64 prefix stateful interfaces
```

```
Stateful Prefixes


Interface               NAT64        Enabled    Global Prefix

GigabitEthernet0/1/0    TRUE          TRUE      2001:DB8:1:1/96
GigabitEthernet0/1/3    TRUE          FALSE     2001:DB8:2:2/96
```

The following is sample output from the **show nat64 prefix stateful static-routes** command:

```
Device# show nat64 prefix stateful static-routes

Stateful Prefixes


NAT64 Prefix    Static Route  Ref-Count

2001:DB8:1:1/96   1
2001:DB8:2:1/96   1
```

The table below describes the significant fields shown in the display.

Table 71: show nat6 prefix stateful Field Descriptions

Field	Description
IFs Using Global Prefix	Lists the interfaces that are using the specified global prefix.
Enabled	Information on whether NAT64 is enabled on a route. TRUE if enabled and FALSE if not enabled.
Static Route	IPv6 static route that is configured to route packets.

Related Commands

Command	Description
nat64 prefix stateful	Configures a prefix and prefix length for stateful NAT64.

show nat64 prefix stateless

To display information about the configured Network Address Translation 64 (NAT64) stateless prefixes, use the **show nat64 prefix stateless**command in user EXEC or privileged EXEC mode.

show nat64 prefix stateless {**global** | {**interfaces** | **static-routes**} [**prefix** *ipv6-prefix*/*prefix-length*]}

Syntax Description

global	Displays the global stateless prefixes.
interfaces	Displays the interfaces and the stateless prefixes used by the interfaces.
prefix	(Optional) Displays the interfaces that are using a specific stateless prefix.
static-routes	Displays the static routes that are using the stateless prefix.
ipv6-prefix	(Optional) IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/ *prefix-length*	(Optional) Length of the IPv6 prefix. Prefix length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. Valid values are from 0 to 128.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.
15.4(1)T	This command was integrated into Cisco IOS Release 15.4(1)T.

Usage Guidelines

The output of the **show nat64 prefix stateless** command displays the interfaces that use a specific prefix and the number of prefixes that use a static route.

Examples

The following is sample output from the **show nat64 prefix stateless global**command:

```
Device# show nat64 prefix stateless global
Global Prefix: is valid, 2001::/96
IFs Using Global Prefix
   Fa0/3/4
   Fa0/3/5
```

The table below describes the significant fields shown in the display.

Table 72: show nat64 prefix stateless global Field Descriptions

Field	Description
Global Prefix	IPv6 stateless prefix configured at the global level.
IFs Using Global Prefix	Lists the interfaces that are using the specified global prefix.

The following is sample output from the **show nat64 prefix stateless interfaces**command.

```
Device# show nat64 prefix stateless interfaces

Interface           NAT64 Enabled    Global    Stateless Prefix
FastEthernet0/3/4   TRUE             FALSE     2001::/96
```

The table below describes the significant fields shown in the display.

Table 73: show nat64 prefix stateless interfaces Field Descriptions

Field	Description
Interface	Interface name and number.
NAT64 Enabled	Information on whether NAT64 is enabled on a route. TRUE if enabled and FALSE if not enabled.
Global	Information on whether a global prefix is used. TRUE if the global prefix is used and FALSE if the interface prefix is used.
Stateless Prefix	Stateless prefix used for NAT64 translation.

The following is sample output from the **show nat64 prefix stateless static-routes**command. The output fields are self-explanatory.

```
Device# show nat64 prefix stateless static-routes

Stateless            Prefix Static Route Ref Count
2001::/96               1
```

Related Commands

Command	Description
nat64 prefix	Assigns a global or interface-specific NAT64 stateless prefix.

show nat64 routes

To display information about the configured Network Address Translation 64 (NAT64) routes, use the **show nat64 routes**command in privileged EXEC mode.

show nat64 routes [**adjacency** *address* | **interface** *type number* | **prefix** *prefix-length*]

Syntax Description

adjacency	(Optional) Displays the route for an adjacency address.
address	(Optional) Adjacency address for lookup.
interface	(Optional) Displays routes pointing to an interface.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
prefix	(Optional) Displays the route of an IPv4 prefix.
prefix-length	(Optional) Length of the IPv4 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.
15.4(1)T	This command was integrated into Cisco IOS Release 154(1)T.

Usage Guidelines

The output of the **show nat64 routes** command displays the stateless prefix and adjacency used by the routes and information on whether the routes are enabled.

Examples

The following is sample output from the **show nat64 routes** command:

```
Device# show nat64 routes
IPv4 Prefix           Adj. Address    Enabled   Output IF    Global    IPv6 Prefix
192.0.2.1/24          0.0.19.137      FALSE     Fa0/3/4
198.51.100.253/24     0.0.19.140      TRUE      Fa0/3/0      FALSE     3001::/96
```

The table below describes the significant fields shown in the display.

Table 74: show nat64 routes Field Descriptions

Field	Description
IPv4 Prefix	Prefix used by the IPv4 address.
Adj. Address	Adjacency address.
Enabled	Information about whether NAT64 is enabled on a route. TRUE if enabled and FALSE if not enabled.
Output IF	Output interfaces.
Global	Information about whether a global prefix is used. TRUE if the global prefix is used and FALSE if the interface prefix is used.

Related Commands

Command	Description
nat64 route	Specifies the NAT64 stateless prefix to which an IPv4 prefix should be translated.

show nat64 services

To display the Network Address Translation (NAT64) services, use the **show nat64 services** command in user EXEC or privileged EXEC mode.

show nat64 services

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.4(2)T	This command was integrated into Cisco IOS Release 15.4(2)T.

Usage Guidelines

Cisco IOS XE Release 3.4S supports only FTP service.

Examples

The following is sample output from the **show nat64 services** command:

```
Device# show nat64 services

NAT64 Services

ftp
   UDP Enabled: TRUE
   TCP Enabled: TRUE
   Service Definition
   Protocol: 6 Port: 21
```

The table below describes the significant fields shown in the display.

Table 75: show nat64 services Field Descriptions

Field	Description
UDP Enabled	Indicates whether service translation is enabled by default for UDP packets, if the protocol is supported by the service definition.
TCP Enabled	Indicates whether the service translation is enabled by default for TCP packets, if the protocol is supported by the service definition.

Field	Description
Service Definition	The definition of the service (the protocol and port fields for which packets are considered a match to the given service).

Related Commands

Command	Description
nat64 service ftp	Enables NAT64 FTP service.

show nat64 statistics

To display Network Address Translation 64 (NAT64) packet count statistics, use the **show nat64 statistics**command in user EXEC or privileged EXEC mode.

show nat64 statistics [**global** | **interface** *type number* | **limit** | **mapping dynamic**[**acl** *acl-name* **pool** *pool-name* | **pool***pool-name*] | **prefixstateful** *ipv6-prefix/prefix-length* | **stateless**]

Syntax Description

global	(Optional) Displays global NAT64 statistics.
interface	(Optional) Displays statistics for an interface.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
limit	(Optional) Clears the statistics for a specific limit. <what is the limit?>
prefix	(Optional) Displays statistics for a specified prefix.
ipv6-prefix	(Optional) IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/ *prefix-length*	(Optional) Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. The valid values are from 0 to 128.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.
15.4(1)T	This command was integrated into Cisco IOS Release 15.4(1)T.

Usage Guidelines

The output of the **show nat64 statistics** command displays the interfaces configured for stateless NAT64 and the packets that were translated or dropped.

Examples

The following is sample output from the **show nat64 statistics** command:

```
Device# show nat64 statistics

NAT64 Statistics
```

```
Total active translations: 3 (1 static, 2 dynamic; 1 extended)
Sessions found: 518938
Sessions created: 2
Expired translations: 1
Global Stats:
   Packets translated (IPv4 -> IPv6)
      Stateless: 30
      Stateful: 259469
   Packets translated (IPv6 -> IPv4)
      Stateless: 30
      Stateful: 259471

Interface Statistics
   GigabitEthernet0/1/0 (IPv4 configured, IPv6 not configured):
      Packets translated (IPv4 -> IPv6)
         Stateless: 15
         Stateful: 259469
      Packets translated (IPv6 -> IPv4)
         Stateless: 0
         Stateful: 0
      Packets dropped: 0
   GigabitEthernet0/1/3 (IPv4 not configured, IPv6 configured):
      Packets translated (IPv4 -> IPv6)
         Stateless: 0
         Stateful: 0
      Packets translated (IPv6 -> IPv4)
         Stateless: 0
         Stateful: 259471
      Packets dropped: 0
Dynamic Mapping Statistics
   v6v4
      access-list mylist pool mypool refcount 2
         pool mypool:
            start 34.1.1.1 end 34.1.1.1
            total addresses 1, allocated 1 (100%)
            address exhaustion packet count 0
Limit Statistics
   max entry: max allowed 200, used 2, packets exceeded 0
```

The table below describes the significant fields shown in the display.

Table 76: show nat64 statistics Field Descriptions

Field	Description
Global Stats	Statistics of all the NAT64 interfaces.
Packets translated	Number of packets translated from IPv4 to IPv6 and vice versa.
Packets dropped	Number of packets dropped. The packets that are not translated are dropped.

Related Commands

Command	Description
nat64 enable	Enables stateless NAT64 on an interface.

show nat64 timeouts

To display the Network Address Translation 64 (NAT64) translation session timeout, use the **show nat64 timeouts** command in user EXEC or privileged EXEC mode.

show nat64 timeouts

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.4(2)T	This command was integrated into Cisco IOS Release 15.4(2)T.

Examples

The following is sample output from the **show nat64 timeouts** command:

```
Device# show nat64 timeouts

NAT64 Timeout
   Seconds     CLI Cfg Uses 'All' all flows
   86400       FALSE   FALSE      udp
   300         FALSE   TRUE       tcp
   7200        FALSE   TRUE       tcp-transient
   240         FALSE   FALSE      icmp
   60          FALSE   TRUE
```

The table below describes the significant fields shown in the display.

Table 77: show nat64 timeouts Field Descriptions

Field	Description
Seconds	NAT64 timeout, in seconds.
CLI Cfg	Indicates whether the timeout is explicitly configured through the CLI. The timeout values configured through the CLI changes the default timeout values.

Related Commands

Command	Description
nat64 translation	Enables NAT64 translation.

show nat64 translations

To display information about Network Address Translation 64 (NAT64) translations, use the **show nat64 translations port** command in user EXEC or privileged EXEC mode.

show nat64 translations {**port** *number* | **protocol** {**icmp** | **tcp** | **udp**} | **v4** {**original** *ipv4-address* | **translated** *ipv6-address*} | **v6** {**original** *ipv6-address* | **translated** *ipv4-address*}} [**total** | **verbose**]

Syntax Description

port	Displays information about NAT64 translations filtered by port numbers.
number	Port number. Valid values are from 1 to 65535.
protocol	Displays information about NAT64 translations, filtered by the protocols configured.
icmp	Displays Internet Control Message Protocol (ICMP) entries.
tcp	Displays TCP entries.
udp	Displays UDP entries.
v4	Displays information about NAT64 translations based on an IPv4 address.
original	Displays translations for the original address.
ipv4-address	IPv4 address.
translated	Displays information about translations for the translated IPv4 or IPv6 address.
ipv6-address	IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
v6	Displays information about NAT64 translations based on an IPv6 address.
total	(Optional) Displays the total NAT64 translation count.
verbose	(Optional) Displays detailed NAT64 translation information.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.4(2)T	This command was integrated into Cisco IOS Release 15.4(2)T.

Examples

The following is sample output from the **show nat64 translations port** command:

```
Device# show nat64 translations port 23

Proto  Original IPv4         Translated IPv4
       Translated IPv6       Original IPv6
------------------------------------------------------------------------------

tcp    192.0.2.1:23          [3001::c000:201]:23
       56.1.1.1:20822        [2001:db8::1]:20822

Total number of translations: 1
```

The following is sample output from the **show nat64 translations v4 original** command:

```
Device# show nat64 translations v4 original 192.0.2.1

Proto  Original IPv4         Translated IPv4
       Translated IPv6       Original IPv6
------------------------------------------------------------------------------

tcp    192.0.2.1:23          [3001::c000:201]:23
       56.1.1.1:20822        [2001:db8::1]:20822
icmp   192.0.2.1:2816        [3001::c000:201]:2816
       56.1.1.1:2816         [2001:db8::1]:2816

Total number of translations: 2
```

The table below describes the significant fields shown in the display.

Table 78: show nat64 translations Field Descriptions

Field	Description
Proto	Protocol type.
Original IPv4 Translated IPv6	IPv4 address that was translated as an IPv6 address. **Note** This field displays the IPv4 addresses that were translated into IPv6 addresses and the IPv4 addresses that were translated from IPv6 addresses.
Translated IPv4 Original IPv6	IPv6 address that was translated as an IPv4 address. **Note** This field displays the IPv6 addresses that were translated into IPv4 addresses and the IPv6 addresses that were translated from IPv4 addresses.

Related Commands

Command	Description
show nat64 translations entry-type	Displays information about NAT64 translations filtered by entry type.
show nat64 translations time	Displays information about NAT64 translations filtered by time.
show nat64 translations total	Displays information about the total NAT64 translation count.
show nat64 translations verbose	Displays detailed NAT64 translation information.

show nat64 translations entry-type

To display information about Network Address Translation 64 (NAT64) translations filtered by entry type, use the **show nat64 translations entry-type** command in user EXEC or privileged EXEC mode.

show nat64 translations entry-type {**bind** {**all** | **dynamic** | **static**} | **session**} [**total** | **verbose**]

Syntax Description

bind	Displays information about NAT64 translation mapping entries.
all	Displays information about all NAT64 translation mapping entries.
dynamic	Displays information about dynamic mapping entries.
static	Displays information about static mapping entries.
session	Displays information about NAT64 translation session entries.
total	(Optional) Displays information about the total NAT64 translation entry count.
verbose	(Optional) Displays detailed NAT64 translation information.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Examples

The following is sample output from the **show nat64 translations entry-type session** command:

```
Router# show nat64 translations entry-type session

Proto  Original IPv4         Translated IPv4
       Translated IPv6       Original IPv6
------------------------------------------------------------------------------

---    ---                   ---
       56.1.1.1              2001:db8::1

Total number of translations: 1
```

The table below describes the significant fields shown in the display.

Table 79: show nat64 translations entry-type session Field Descriptions

Field	Description
Proto	Protocol type.

Field	Description
Original IPv4 Translated IPv6	IPv4 address that was translated as an IPv6 address. **Note** This field displays the IPv4 addresses that were translated into IPv6 addresses and the IPv4 addresses that were translated from IPv6 addresses.
Translated IPv4 Original IPv6	IPv6 address that was translated as an IPv4 address. **Note** This field displays the IPv6 addresses that were translated into IPv4 addresses and the IPv6 addresses that were translated from IPv4 addresses.

Related Commands

Command	Description
show nat64 translations	Displays information about NAT64 translations.
show nat64 translations time	Displays information about NAT64 translations filtered by time.
show nat64 translations total	Displays information about the total NAT64 translation count.
show nat64 translations verbose	Displays detailed NAT64 translation information.

show nat64 translations redundancy

To display the Network Address Translation 64 (NAT64) translations filtered by redundancy groups (RGs), use the **show nat64 translations redundancy** command in user EXEC or privileged EXEC mode.

show nat64 translations redundancy *group-id* [**total** | **verbose**]

Syntax Description

group-id	Redundancy group ID. Valid values are from 1 and 2.
total	(Optional) Displays information about the total NAT64 redundancy translations.
verbose	(Optional) Displays detailed NAT64 redundancy translation information.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced.

Usage Guidelines

Use the output of the verify the redundancy groups that you have configured.

Examples

The following is sample output from the **show nat64 translations redundancy** command:

```
Device# show nat64 translations redundancy 1

  Proto  Original IPv4         Translated IPv4
         Translated IPv6       Original IPv6
 ------------------------------------------------------------------------------

         209.165.201.2:21      [2001:DB8:1::103]:32847

 tcp     10.2.1.11:32863       [2001::3201:10b]:32863
         10.1.1.1:80           [2001::11]:80
 tcp     209.165.201.2:21      [2001:DB8:1::104]:32848
         10.1.1.1:80           [2001::11]:80

 Total number of translations: 3
```

The table below describes the significant fields shown in the display.

Table 80: show nat64 translations redundancy Field Descriptions

Field	Description
Proto	Protocol type.
Original IPv4 Translated IPv6	IPv4 address that was translated as an IPv6 address. **Note** This field displays IPv4 addresses that were translated into IPv6 addresses and IPv4 addresses that were translated from IPv6 addresses.

Field	Description
Translated IPv4 Original IPv6	IPv6 address that was translated as an IPv4 address. **Note** This field displays IPv6 addresses that were translated into IPv4 addresses and IPv6 addresses that were translated from IPv4 addresses.

Related Commands

Command	Description
show nat64 translations	Displays information about NAT64 translations.

show nat64 translations time

To display information about Network Address Translation 64 (NAT64) translations filtered by time, use the **show nat64 translations time** command in user EXEC or privileged EXEC mode.

show nat64 translations time {**created** | **last-used**} {**newer-than** | **older-than**} *day month year hh*:*mm*:*ss* [**total** | **verbose**]

Syntax Description

created	Displays translation entries that were created at the specified time.
last-used	Displays the translation entries that were last used at the specified time.
newer-than	Displays translation entries that are newer than the time stamp.
older-than	Displays translation entries that are older than the time stamp.
day	Day of the month. Valid values are from 1 to 31.
month	Month of the year. Valid values are from January to December.
year	Year. Valid values are from 1993 to 2035.
hh:*mm*:*ss*	Time in hh:mm:ss format.
total	(Optional) Displays the total NAT64 translation count.
verbose	(Optional) Displays detailed NAT64 translation information.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Examples

The following is sample output from the **show nat64 translations time created newer-than** command:

```
Router# show nat64 translations time created newer-than 20 June 2011 20:00:00

Proto  Original IPv4         Translated IPv4
       Translated IPv6       Original IPv6
------------------------------------------------------------------------------

       56.1.1.1              2001:db8::1
tcp    192.0.2.1:23          [3001::c000:201]:23
       56.1.1.1:20822        [2001:db8::1]:20822
icmp   192.0.2.1:2816        [3001::c000:201]:2816
       56.1.1.1:2816         [2001:db8::1]:2816

Total number of translations: 3
```

The table below describes the significant fields shown in the display.

Table 81: show nat64 translations time created newer-than Field Descriptions

Field	Description
Proto	Protocol type.
Original IPv4 Translated IPv6	IPv4 address that was translated as an IPv6 address. **Note** This field displays the IPv4 addresses that were translated into IPv6 addresses and the IPv4 addresses that were translated from IPv6 addresses.
Translated IPv4 Original IPv6	IPv6 address that was translated as an IPv4 address. **Note** This field displays the IPv6 addresses that were translated into IPv4 addresses and the IPv6 addresses that were translated from IPv4 addresses.

Related Commands

Command	Description
show nat64 translations	Displays information about NAT64 translations.
show nat64 translations entry-type	Displays information about NAT64 translations filtered by entry type.
show nat64 translations total	Displays information about the total NAT64 translation count.
show nat64 translations verbose	Displays the detailed NAT64 translation information.

show nat64 translations total

To display the total Network Address Translation 64 (NAT64) translation count, use the **show nat64 translations total** command in user EXEC or privileged EXEC mode.

show nat64 translations total [**entry-type** {**bind** {**all** | **dynamic** | **static**} | **session**} | **port** *number* | **protocol** {**icmp** | **tcp** | **udp**} | **time** {**created** | **last-used**} {**newer-than** | **older-than**} *day month year hh*:*mm*:*ss* | **v4** {**original** *ipv4-address* | **translated** *ipv6-address*} | **v6** {**original** *ipv6-address* | **translated** *ipv4-address*}]

Syntax Description

entry-type	(Optional) Displays information about NAT64 translations filtered by entry type.
bind	(Optional) Displays information about NAT64 translation mapping entries.
all	(Optional) Displays information about all NAT64 translation mapping entries.
dynamic	(Optional) Displays information about dynamic mapping entries.
static	(Optional) Displays information about static mapping entries.
session	(Optional) Displays information about NAT64 translation session entries.
port *number*	(Optional) Displays information about NAT64 translations filtered by port number. Valid values are from 1 to 65535.
protocol	(Optional) Displays information about NAT64 translations filtered by protocol.
icmp	(Optional) Displays information about Internet Control Message Protocol (ICMP) entries.
tcp	(Optional) Displays information about TCP entries.
udp	(Optional) Displays information about UDP entries.
time	(Optional) Displays information about NAT64 translations filtered by time.
created	(Optional) Displays translation entries created at the specified time.
last-used	(Optional) Displays the translation entries that were last used at the specified time.
newer-than	(Optional) Displays translation entries that are newer than the time stamp.
older-than	(Optional) Displays translation entries that are older than the time stamp.
day	(Optional) Day of the month. Valid values are from 1 to 31.
month	(Optional) Month of the year. Valid values are from January to December.
year	(Optional) Year. Valid values are from 1993 to 2035.
hh:*mm*:*ss*	(Optional) Time in hh:mm:ss format.
v4	(Optional) Displays information about NAT64 translations based on an IPv4 address.
original	(Optional) Displays information about translations for the original IPv4 or IPv6 address.

ipv4-address	(Optional) IPv4 address.
translated	(Optional) Displays information about translations for the translated IPv4 or IPv6 address.
ipv6-address	(Optional) IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
v6	(Optional) Displays information about NAT64 translations based on an IPv6 address.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Examples

The following is sample output from the **show nat64 translations total** command:

```
Router# show nat64 translations total

Total number of translations: 3
```

The output fields are self-explanatory.

Related Commands

Command	Description
show nat64 translations	Displays information about NAT64 translations.
show nat64 translations entry-type	Displays information about NAT64 translations filtered by entry type.
show nat64 translations time	Displays information about NAT64 translations filtered by time.
show nat64 translations verbose	Displays detailed NAT64 translation information.

show nat64 translations v4

To display Network Address Translation 64 (NAT64) translations based on an IPv4 address, use the **show nat64 translations v4** command in user EXEC or privileged EXEC mode.

show nat64 translation v4 {**original** *ipv4-address* | **translated** *ipv6-address*} **total** | **verbose**

Syntax Description

original	Displays translations for the original IPv4 address.
ipv4-address	IPv4-address.
translated	Displays translations for the translated address.
ipv6-address	IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
total	(Optional) Displays the total NAT64 translation count.
verbose	(Optional) Displays detailed NAT64 translation information.

Command Default

This command has no default settings.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Examples

The following is sample output from the**show nat64 translation v4 original** command:

```
Router# show nat64 translation v4 original 112.1.1.10

Proto  Original IPv4         Translated IPv4
       Translated IPv6       Original IPv6
------------------------------------------------------------------------

tcp    112.1.1.10:23         [3001::7001:10a]:23
       56.1.1.2:12656        [2001::2]:12656

Total number of translations: 1
```

The following is sample output from the **show nat64 translations v4 translated**command:

```
Router# show nat64 translations v4 translated 3001::7001:10a

Proto  Original IPv4         Translated IPv4
       Translated IPv6       Original IPv6
------------------------------------------------------------------------
```

```
icmp   112.1.1.10:677        [3001::7001:10a]:677
       56.1.1.2:677          [2001::1b01:10a]:677

Total number of translations: 1
```

The table below describes the significant fields shown in the display.

Table 82: show nat64 translations v4 Field Descriptions

Field	Description
Proto	Protocol type.
Original IPv4 Translated IPv6	IPv4 address that was translated as an IPv6 address.
Translated IPv4 Original IPv6	IPv6 address that was translated as an IPv4 address.

Related Commands

Command	Description
show nat64 translations entry-type	Displays NAT64 translations filtered by entry type.
show nat64 translations port	Displays NAT64 translations filtered by port numbers.
show nat64 translations protocol	Displays NAT64 translations filtered by protocols.
show nat64 translations time	Displays NAT64 translations filtered by time.
show nat64 translations total	Displays the total NAT64 translation count.
show nat64 translations v6	Displays NAT64 translations based on an IPv6 address.
show nat64 translations verbose	Displays detailed NAT64 translation information.

show nat64 translations v6

To display Network Address Translation 64 (NAT64) translations based on an IPv6 address, use the **show nat64 translations v4** command in user EXEC or privileged EXEC mode.

show nat64 translations v6 {**original** *ipv6-address* | **translated** *ipv4-address*}[**total** | **verbose**]

Syntax Description

original	Displays translations for the original IPv6 address.
ipv6-address	IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
translated	Displays translations for the translated address.
ipv4-address	IPv4-address.
total	Displays the total NAT64 translation count.
verbose	Displays detailed NAT64 translation information.

Command Default

This command has no default settings.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Examples

The following is sample output from the **show nat64 translation v6 original** command:

```
Router# show nat64 translations v6 original 2001::2

Proto  Original IPv4         Translated IPv4
       Translated IPv6       Original IPv6
------------------------------------------------------------------------------

---    ---                   ---
       56.1.1.1              2001::2
tcp    112.1.1.10:23         [3001::7001:10a]:23
       56.1.1.1:38924        [2001::2]:38924

Total number of translations: 2
```

The following is sample output from the **show nat64 translations v6 translated** command:

```
Router# show nat64 translations v6 translated 56.1.1.2

Proto  Original IPv4         Translated IPv4
       Translated IPv6       Original IPv6
```

```
--------------------------------------------------------------------------------

---     ---                     ---
        56.1.1.2                2001::1b01:10a
icmp    112.1.1.10:2370         [3001::7001:10a]:2370
        56.1.1.2:2370           [2001::1b01:10a]:2370

Total number of translations: 2
```

The table below describes the significant fields shown in the display.

Table 83: show nat64 translations v6 Field Descriptions

Field	Description
Proto	Protocol type.
Original IPv4 Translated IPv6	IPv4 address that was translated as an IPv6 address.
Translated IPv4 Original IPv6	IPv6 address that was translated as an IPv4 address.

Related Commands

Command	Description
nat64 translation	Enables NAT64 translation.
show nat64 translations entry-type	Displays NAT64 translations filtered by entry type.
show nat64 translations port	Displays NAT64 translations filtered by port numbers.
show nat64 translations protocol	Displays NAT64 translations filtered by protocols.
show nat64 translations time	Displays NAT64 translations filtered by time.
show nat64 translation total	Displays the total NAT64 translation count.
show nat64 translations v4	Displays NAT64 translations based on an IPv4 address.
show nat64 translations verbose	Displays detailed NAT64 translation information.

show nat64 translations verbose

To display the detailed Network Address Translation 64 (NAT64) translation information, use the **show nat64 translations verbose** command in user EXEC or privileged EXEC mode.

show nat64 translations verbose [**entry-type** {**bind** {**all** | **dynamic** | **static**} | **session**} | **port** *number* | **protocol** {**icmp** | **tcp** | **udp**} | **time** {**created** | **last-used**} {**newer-than** | **older-than**} *day month year hh*:*mm*:*ss* | **v4** {**original** *ipv4-address* | **translated** *ipv6-address*} | **v6** {**original** *ipv6-address* | **translated** *ipv4-address*}]

Syntax Description

entry-type	(Optional) Displays information about NAT64 translations filtered by entry type.
bind	(Optional) Displays information about NAT64 translation mapping entries.
all	(Optional) Displays information about all NAT64 translation mapping entries.
dynamic	(Optional) Displays information about dynamic mapping entries.
static	(Optional) Displays information about static mapping entries.
session	(Optional) Displays information about NAT64 translation session entries.
port *number*	(Optional) Displays information about NAT64 translations filtered by port number. Valid values are from 1 to 65535.
protocol	(Optional) Displays information about NAT64 translations filtered by protocol.
icmp	(Optional) Displays information about Internet Control Message Protocol (ICMP) entries.
tcp	(Optional) Displays information about TCP entries.
udp	(Optional) Displays information about UDP entries.
time	(Optional) Displays information about NAT64 translations filtered by time.
created	(Optional) Displays translation entries created at the specified time.
last-used	(Optional) Displays the translation entries that were last used at the specified time.
newer-than	(Optional) Displays translation entries that are newer than the time stamp.
older-than	(Optional) Displays translation entries that are older than the time stamp.
day	(Optional) Day of the month. Valid values are from 1 to 31.
month	(Optional) Month of the year. Valid values are from January to December.
year	(Optional) Year. Valid values are from 1993 to 2035.
hh:*mm*:*ss*	(Optional) Time in hh:mm:ss format.
v4	(Optional) Displays information about NAT64 translations based on an IPv4 address.
original	(Optional) Displays information about translations for the original IPv4 or IPv6 address.

ipv4-address	(Optional) IPv4 address.
translated	(Optional) Displays information about translations for the translated IPv4 or IPv6 address.
ipv6-address	(Optional) IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
v6	(Optional) Displays information about NAT64 translations based on an IPv6 address.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Examples

The following is sample output from the **show nat64 translations verbose** command:

```
Router# show nat64 translations verbose

Proto  Original IPv4         Translated IPv4
       Translated IPv6       Original IPv6
------------------------------------------------------------------------------

       56.1.1.1              2001:db8::1
         created: 01 Jul 2011 15:27:06, last-used:   ---,
           inactivity-time:     ---
         flags: none
         entry-id: 0000000000, use-count: 3
tcp    192.0.2.1:23          [3001::c000:201]:23
       56.1.1.1:42485        [2001:db8::1]:42485
         created: 01 Jul 2011 15:32:01, last-used:   01 Jul 2011 15:32:04,
           inactivity-time:     00:03:53
         flags: timing-out, syn-in
         entry-id: 0x8ca82cd0, use-count: 1
icmp   192.0.2.1:8552        [3001::c000:201]:8552
       56.1.1.1:8552         [2001:db8::1]:8552
         created: 01 Jul 2011 15:31:23, last-used:   01 Jul 2011 15:31:23,
           inactivity-time:     00:00:11
         flags: none
         entry-id: 0x8ca82c30, use-count: 1
icmp   192.0.2.1:983         [3001::c000:201]:983
       56.1.1.1:983          [2001:db8::1]:983
         created: 01 Jul 2011 15:32:06, last-used:   01 Jul 2011 15:32:06,
           inactivity-time:     00:00:54
         flags: none
         entry-id: 0x8ca82d70, use-count: 1

Total number of translations: 4
```

The table below describes the significant fields shown in the display.

Table 84: show nat64 translations verbose Field Descriptions

Field	Description
Proto	Protocol type.
Original IPv4 Translated IPv6	IPv4 address that was translated as an IPv6 address. **Note** This field displays the IPv4 addresses that were translated into IPv6 addresses and the IPv4 addresses that were translated from IPv6 addresses.
Translated IPv4 Original IPv6	IPv6 address that was translated as an IPv4 address. **Note** This field displays the IPv6 addresses that were translated into IPv4 addresses and the IPv6 addresses that were translated from IPv4 addresses.
created	The date and time when the entry was created.
last-used	The date and time when the entry was last used.

Related Commands

Command	Description
show nat64 translations	Displays information about NAT64 translations.
show nat64 translations entry-type	Displays NAT64 translations filtered by entry type.
show nat64 translations time	Displays NAT64 translations filtered by time.
show nat64 translations total	Displays the total NAT64 translation count.

show nhrp debug-condition

To display the Next Hop Resolution Protocol (NHRP) conditional debugging information, use the **show nhrp debug-condition**command in privileged EXEC mode.

show nhrp debug-condition

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Examples

The following is sample output from the **show nhrp debug-condition** command:

```
Router# show nhrp debug-condition
Peer NBMA addresses under debug are:
1.1.1.1,
Interfaces under debug are:
Tunnel1, Peer Tunnel addresses under debug are:
2.2.2.2,
```

The output if self-explanatory. It displays the conditional debugging information for NHRP.

Related Commands

Command	Description
debug nhrp condition	Enables the NHRP conditional debugging.

show nhrp group-map

To display the details of NHRP group mappings, use the **show nhrp group-map** command in user EXEC or privileged EXEC mode.

show nhrp group-map [*group-name*]

Syntax Description

group-name	(Optional) Name of an NHRP group mapping for which information will be displayed.

Command Default

Information is displayed for all NHRP group mappings.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.4(1)T	This command was introduced.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

This command displays the details on NHRP group mappings on the hub along with the list of tunnels using each of the NHRP groups defined in the mappings. In combination with the **show ip nhrp** command, this command lets you easily determine which QoS policy map is applied to a specific tunnel endpoint.

This command displays the details of the specified NHRP group mapping. The details include the associated QoS policy name and the list of tunnel endpoints using the QoS policy. If no option is specified, it displays the details of all NHRP group mappings.

Note This command will replace the **show ip nhrp group-map** command in a future release.

Examples

The following is sample output from the **show nhrp group-map** command:

```
Device# show nhrp group-map

Interface: Tunnel0
 NHRP group: spoke_group1
  QoS policy: group1_parent
  Transport endpoints using the qos policy: None

 NHRP group: spoke_group2
  QoS policy: group2_parent
  Transport endpoints using the qos policy: None

 NHRP group: spoke_group3
  QoS policy: group3_parent
  Transport endpoints using the qos policy: None
```

The following is sample output from the **show nhrp group-map** command for an NHRP group named test-group-0:

```
Device# show nhrp group-map test-group-0

Interface: Tunnel0
 NHRP group: tes-group-0
  QoS policy: group3_parent
  Transport endpoints using the qos policy:
  6001::1000:1
```

The table below describes the significant fields shown in the displays.

Table 85: show nhrp group-map Field Descriptions

Field	Description
Interface	Interface on which the policy is configured.
NHRP group	NHRP group associated with the QoS policy on the interface.
QoS policy	QoS policy configured on the interface.
Transport endpoints using the qos policy	List of transport endpoints using the QoS policy.

Related Commands

Command	Description
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
nhrp group	Configures an NHRP group on a spoke.
nhrp map group	Adds NHRP groups to QoS policy mappings on a hub.
show dmvpn	Displays DMVPN-specific session information.
show ip nhrp	Displays NHRP mapping information.
show policy-map mgre	Displays statistics about a specific QoS policy as it is applied to a tunnel endpoint.

show platform hardware qfp feature

To display feature-specific information in the Cisco Quantum Flow Processor (QFP), use the **show platform hardware qfp feature**command in privileged EXEC mode.

show platform hardware qfp {**active** | **standby**} **feature alg** {**memory** | **statistics** [*protocol* | **clear** [**clear**]]}

Syntax Description

active	Displays the active instance of the processor.
standby	Displays the standby instance of the processor.
alg	Displays the Application Level Gateway (ALG) information of the processor.
memory	Displays ALG memory usage information of the processor.
statistics	Displays ALG common statistics information of the processor.
protocol	Protocol name. It can be one of the following values: • **dns** --Displays Domain Name System (DNS) ALG information in the QFP datapath. • **exec** --Displays exec ALG information in the QFP datapath. • **ftp** --Displays FTP ALG information in the QFP datapath. • **h323** --Displays H.323 ALG information in the QFP datapath. • **http** --Displays HTTP ALG information in the QFP datapath. • **imap** --Displays Internet Message Access Protocol (IMAP) ALG information in the QFP datapath. • **ldap** --Displays Lightweight Directory Access Protocol (LDAP) ALG information in the QFP datapath. • **login** --Displays login ALG information in the QFP datapath. • **netbios** --Displays Network Basic Input Output System (NetBIOS) ALG information in the QFP datapath. • **pop3** --Displays pop3 ALG information in the QFP datapath. • **rtsp** --Displays Rapid Spanning Tree Protocol (RSTP) ALG information in the QFP datapath. • **shell** --Displays shell ALG information in the QFP datapath. • **sip** --Displays Session Initiation Protocol (SIP) ALG information in the QFP datapath. • **skinny** --Displays skinny ALG information in the QFP datapath. • **smtp** --Displays Simple Mail Transfer Protocol (SMTP) ALG information in the QFP datapath. • **sunrpc** --Displays Sun RPC ALG information in the QFP datapath. • **tftp** --Displays TFTP ALG information in the QFP datapath.

clear	(Optional) Clears ALG common counters after display.
clear	(Optional) Clears the ALG counters.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.2	This command was introduced.
Cisco IOS XE Release 3.1S	This command was modified. Support for the NetBIOS protocol was added.
Cisco IOS XE Release 3.2S	This command was modified. The show output was modified to display SIP statistics information.

Usage Guidelines

The **show platform hardware qfp feature** command when used withthe **netbios** keyworddisplays the NetBIOS ALG memory usage and statistics information of the processor.

Examples

The following example displays the NetBIOS ALG statistics information of the processor:

```
Router# show platform hardware qfp active feature alg statistics netbios
NetBIOS ALG Statistics:
  No. of allocated chunk elements in L7 data pool:0
  No. of times L7 data is allocated:0  No. of times L7 data is freed:0
  Datagram Service statistics
    Total packets            :0
    Direct unique packets    :0
    Direct group packets     :0
    Broadcast packets        :0
    DGM Error packets        :0
    Query request packets    :0
    Positive Qry response packets :0
    Netgative Qry response packets:0
    Unknown packets          :0
    Total error packets      :0
  Name Service statistics
    Total packets            :0
    Query request packets    :0
    Query response packets   :0
    Registration req packets :0
    Registration resp packets:0
    Release request packets  :0
    Release response packets :0
    WACK packets             :0
    Refresh packets          :0
    Unknown packets          :0
    Total error packets      :0
  Session Service statistics
    Total packets            :0
    Message packets          :0
    Request packets          :0
    Positive response packets:0
    Negative response packets:0
    Retarget response packets:0
    Keepalive packets        :0
    Unknown packets          :0
    Total error packets      :0
```

The table below describes the significant fields shown in the display.

Table 86: show platform hardware qfp feature Field Descriptions

Field	Description
No. of allocated chunk elements in L7 data pool	Number of memory chunks allocated for processing NetBIOS packets.
No. of times L7 data is allocated:0 No. of times L7 data is freed	Number of times memory is allocated and freed for processing NetBIOS packets.
Direct unique packets	Number of direct unique NetBIOS packets processed.
Direct group packets	Number of direct group NetBIOS packets processed.
Broadcast packets	Number of broadcast NetBIOS packets processed.
DGM Error packets	Number of Datagram Error NetBIOS packets processed.
Query request packets	Number of query request NetBIOS packets processed.
Positive Qry response packets	Number of positive query response NetBIOS packets processed.
Negative Qry response packets	Number of negative query response NetBIOS packets processed.
Unknown packets	Number of unknown packets.
Total error packets	Counter tracking number of error packets.

The following example displays SIP statistics information of the processor. The field descriptions are self-explanatory.

```
Router# show platform hardware qfp active feature alg statistics sip
SIP info pool used chunk entries number: 0
RECEIVE
Register: 0 -> 200-OK: 0
Invite: 0 -> 200-OK: 0 Re-invite 0
Update: 0 -> 200-OK: 0
Bye: 0 -> 200-OK: 0
Trying: 0 Ringing: 0 Ack: 0
Info: 0 Cancel: 0 Sess Prog: 0
Message: 0 Notify: 0 Prack: 0
OtherReq: 0 OtherOk: 0
Events
Null dport: 0 Media Port Zero: 0
Malform Media: 0 No Content Length: 0
Cr Trunk Chnls: 0 Del Trunk Chnls: 0
Cr Normal Chnls: 0 Del Normal Chnls: 0
Media Addr Zero: 0 Need More Data: 0
Errors
Create Token Err: 0 Add portlist Err: 0
Invalid Offset: 0 Invalid Pktlen: 0
Free Magic: 0 Double Free: 0
Retmem Failed: 0 Malloc Failed: 0
```

```
Bad Format: 0 Invalid Proto: 0
Add ALG state Fail: 0 No Call-id: 0
Parse SIP Hdr Fail: 0 Parse SDP Fail: 0
Error New Chnl: 0 Huge Size: 0
Create Failed: 0
Writeback Errors
Offset Err: 0 PA Err: 0
No Info: 0
```

Related Commands

Command	Description
debug platform hardware qfp feature	Debugs feature-specific information in the QFP.

show platform hardware qfp feature alg statistics sip

To display Session Initiation Protocol (SIP) application layer gateway (ALG)-specific statistics information in the Cisco Quantum Flow Processor (QFP), use the **show platform hardware qfp feature alg statistics sip** command in privileged EXEC mode.

show platform hardware qfp feature alg statistics sip [**clear** | **dbl** [**all** | **clear** | **entry** *entry-string* [**clear**]] | **dblcfg** | **l7data** {**callid** *call-id* | **clear**} | **processor** | **timer**]

Syntax Description

clear	(Optional) Clears ALG counters after display.
dbl	(Optional) Displays brief information about all SIP blocked list data.
all	(Optional) Displays all dynamic blocked list entries: blocked list and non blocked list entries.
entry *entry-string*	(Optional) Clears the specified blocked list entry.
dblcfg	(Optional) Displays all SIP blocked list settings.
l7data	(Optional) Displays brief information about all SIP Layer 7 data.
callid *call-id*	(Optional) Displays information about the specified SIP call ID.
processor	(Optional) Displays SIP processor settings.
timer	(Optional) Displays SIP timer settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.11S	This command was introduced.

Usage Guidelines

This command displays the following error details:

- Session write lock exceeded
- Global write lock exceeded
- Blocked list

This command also displays the following event details:

- Blocked list triggered
- Blocked list timeout

A blocked list is a list of entities that are denied a particular privilege, service, or access.

Examples

The following is sample output from the **show platform hardware qfp active feature alg statistics sip** command:

```
Device#  show platform hardware qfp active feature alg statistics sip
```

```
Events
...
Cr dbl entry:                10   Del dbl entry:                 10
Cr dbl cfg entry:             8   Del dbl cfg entry:              4
start dbl trig tmr:          10   restart dbl trig tmr:        1014
stop dbl trig tmr:           10   dbl trig timeout:            1014
start dbl blk tmr:            0   restart dbl blk tmr:            0
stop dbl blk tmr:             0   dbl blk tmr timeout:            0
start dbl idle tmr:          10   restart dbl idle tmr:         361
stop dbl idle tmr:            1   dbl idle tmr timeout:           9

DoS Errors
Dbl Retmem Failed:            0    Dbl Malloc Failed:             0
DblCfg Retm Failed:           0    DblCfg Malloc Failed:          0
Session wlock ovflw:          0    Global wlock ovflw:            0
Blacklisted:                561
```

The table below describes the significant fields shown in the display.

Table 87: show platform hardware qfp active feature alg statistics sip Field Descriptions

Field	Description
CR dbl entry	Number of dynamic blocked list entries.
start dbl blk tmr	Number of events that have started the dynamic blocked list timer.
stop dbl idle tmr	Number of events that have stopped the dynamic blocked list idle timer.
Del dbl entry	Number of dynamic blocked list entries deleted.
restart dbl trig tmr	Number of dynamic blocked list trigger timers restarted.
dbl trig timeout	Number of dynamic blocked list trigger timers timed out.
restart dbl blk tmr	Number of dynamic blocked list timers to be restarted.
dbl idle tmr timeout	Number of dynamic blocked list idle timers timed out.
DoS Errors	Denial of service (DoS) related errors.
Dbl Retmem Failed	Number of dynamic blocked list return memory failures.
DblCfg Retm Failed	Number of dynamic blocked list configuration return memory failures.
Session wlock ovflw	Number of packets that are dropped because the session-level write lock number is exceeded.
Blocked list	Number of packets dropped by dynamic blocked list.
Dbl Malloc Failed	Number of dynamic blocked list memory allocation failures.
DblCfg Malloc Failed	Number of dynamic blocked list configuration memory allocation failures.

Field	Description
Global wlock ovflw	Number of packets dropped because the global-level write-lock number is exceeded.

The following is sample output from the **show platform hardware qfp active feature alg statistics sip dbl entry** command:

```
Device# show platform hardware qfp active feature alg statistics sip dbl entry a4a051e0a4a1ebd

req_src_addr: 10.74.30.189              req_dst_addr: 10.74.5.30
trigger_period:     1000(ms)            block_timeout:       30(sec)
idle_timeout:       60(sec)             dbl_flags: 0x        1
cfg_trig_cnt:        5                  cur_trig_cnt:        0
```

The table below describes the significant fields shown in the display.

Table 88: show platform hardware qfp active feature alg statistics sip Field Descriptions

Field	Description
req_src_addr	Source IP address of a SIP request message.
trigger_period	Dynamic blocked list trigger period.
idle_timeout	Dynamic blocked list idle timeout entry.
cfg_trig_cnt	Configured trigger counter.
req_dst_addr	Destination IP address of a SIP request message.
block_timeout	Dynamic blocked list block timeout.
dbl_flags	Dynamic blocked list entry flags.
cur_trig_cnt	Current trigger counter.

Related Commands

alg sip blacklist	Configures a dynamic SIP ALG blocked list for destinations.
alg sip processor	Configures the maximum number of backlog messages that wait for shared resources.
alg sip timer	Configures a timer that SIP ALG uses to manage SIP calls.

show platform software trace message

To display trace messages for a module, enter the **show platform software trace message** command in privileged EXEC mode or diagnostic mode.

show platform software trace message *process hardware-module slot*

Syntax Description

process	The process in which the tracing level is being set. The following keywords are available: • **chassis-manager** --The Chassis Manager process. • **cpp-control-process** --The Cisco packet processor (CPP) Control process. • **cpp-driver** --The CPP driver process. • **cpp-ha-server** --The CPP high availability (HA) server process. • **cpp-service-process** --The CPP service process. • **forwarding-manager** --The Forwarding Manager process. • **host-manager** --The Host Manager process. • **interface-manager** --The Interface Manager process. • **ios** --The Cisco IOS process. • **logger** --The logging manager process. • **pluggable-services** --The pluggable services process. • **shell-manager** --The Shell Manager process.
hardware-module	Tthe hardware module where the process whose trace level is being set is running. The following keywords are available: • **carrier-card** --The process is on an SPA Interface Processor (SIP). • **forwarding-processor** --The process is on an embedded services processor (ESP). • **route-processor** --The process is on an route processor (RP).

slot	The slot of the hardware module. Options are as follows: • *number* --The number of the SIP slot of the hardware module where the trace level is being set. For instance, if you want to specify the SIP in SIP slot 2 of the router, enter 2. • *SIP-slot* / *SPA-bay* --The number of the SIP router slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in router slot 3, enter 3/2. • **cpp active** --The CPP in the active ESP. • **cpp standby** --The CPP in the standby ESP. • **f0** --The ESP in ESP slot 0. • **f1** --The ESP in ESP slot 1 • **fp active** --The active ESP. • **fp standby** --The standby ESP.
	• **r0** --The RP in RP slot 0. • **r1** --The RP in RP slot 1. • **rp active** --The active RP. • **rp standby** --The standby RP. • **qfp active** --The active Quantum Flow Processor (QFP)

Command Modes

Privileged EXEC (#) Diagnostic (diag)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
12.2(33)XND	This command was modified. The command output displays the truncated traceback message also.
Cisco IOS XE Release XE 3.1S	The **qfp active** keywords were added.

Usage Guidelines

The **show platform software trace message** command is used to display trace messages from an in-memory message ring of a module's process that keeps a condensed historical record of all messages. Although all messages are saved in a trace log file unmodified, only the first 128 bytes of a message are saved in the message ring. The size limitation does not apply to the traceback portion of a message.

Examples

The following example shows how to display the trace messages for the Host Manager process in RP slot 0 using the **show platform software trace message** command:

```
Router# show platform software trace message host-manager R0
08/23 12:09:14.408 [uipeer]: (info): Looking for a ui_req msg
08/23 12:09:14.408 [uipeer]: (info): Start of request handling for con 0x100a61c8
```

```
08/23 12:09:14.399 [uipeer]: (info): Accepted connection for 14 as 0x100a61c8
08/23 12:09:14.399 [uipeer]: (info): Received new connection 0x100a61c8 on descriptor 14
08/23 12:09:14.398 [uipeer]: (info): Accepting command connection on listen fd 7
08/23 11:53:57.440 [uipeer]: (info): Going to send a status update to the shell manager in
 slot 0
08/23 11:53:47.417 [uipeer]: (info): Going to send a status update to the shell manager in
 slot 0
```

The following example shows a truncated message that has a traceback. The truncated portion of the message is indicated by an ellipsis (...):

```
03/02 15:47:44.002 [errmsg]: (ERR): %EVENTLIB-3-TIMEHOG: read asyncon 0x100a9260: 60618ms,
 Traceback=1#862f8780825f93a618ecd9 ...Traceback=1#862f8780825f93a618ecd9dd48b3be96
evlib:FCAF000+CC00 evlib:FCAF000+A6A8 evutil:FFCA000+ADD0 evutil:FFCA000+5A80
evutil:FFCA000+A68C uipeer:FF49000+10AFC evlib:FCAF000+D28C evlib:FCAF000+F4C4 :10000000+1B24C
 c:EF44000+1D078 c:EF44000+1D220
```

Related Commands

Command	Description
set platform software trace	Sets the trace level for a specific module.
show platform software trace levels	Displays trace levels for a module.

show redundancy application control-interface group

To display control interface information for a redundancy group, use the **show redundancy application control-interface group** command in privileged EXEC mode.

show redundancy application control-interface group [*group-id*]

Syntax Description

group-id	(Optional) Redundancy group ID. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show redundancy application control-interface**command shows information for the redundancy group control interfaces.

Examples

The following is sample output from the **show redundancy application control-interface** command:

```
Router# show redundancy application control-interface group 2
The control interface for rg[2] is GigabitEthernet0/1/0
Interface is Control interface associated with the following protocols: 2 1
BFD Enabled
Interface Neighbors:
```

Related Commands

Command	Description
show redundancy application faults	Displays fault-specific information for a redundancy group.
show redundancy application group	Displays redundancy group information.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.
show redundancy application protocol	Displays protocol-specific information for a redundancy group.

show redundancy application data-interface

To display data interface-specific information, use the **show redundancy application data-interface**command in privileged EXEC mode.

show redundancy application data-interface group [*group-id*]

Syntax Description

group	Specifies the redundancy group.
group-id	(Optional) Redundancy group ID. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show redundancy application data-interface** command displays information about the redundancy group data interfaces.

Examples

The following is sample output from the **show redundancy application data-interface** command:

```
Router# show redundancy application data-interface group 1
The data interface for rg[1] is GigabitEthernet0/1/1
```

Related Commands

Command	Description
show redundancy application control-interface	Displays control interface information for a redundancy group.
show redundancy application faults	Displays fault-specific information for a redundancy group.
show redundancy application group	Displays redundancy group information.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.
show redundancy application protocol	Displays protocol-specific information for a redundancy group.

show redundancy application faults group

To display fault-specific information for a redundancy group, use the **show redundancy application faults group**command in privileged EXEC mode.

show redundancy application faults group [*group-id*]

Syntax Description

group-id	(Optional) Redundancy group ID. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show redundancy application faults**command shows information returned by redundancy group faults.

Examples

The following is sample output from the **show redundancy application faults** command:

```
Router# show redundancy application faults group 2
Faults states Group 2 info:
        Runtime priority: [150]
                RG Faults RG State: Up.
                        Total # of switchovers due to faults:           2
                        Total # of down/up state changes due to faults: 2
```

Related Commands

Command	Description
show redundancy application control-interface	Displays control interface information for a redundancy group.
show redundancy application group	Displays redundancy group information.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.
show redundancy application protocol	Displays protocol-specific information for a redundancy group.

show redundancy application group

To display the redundancy group information, use the **show redundancy application group** command in privileged EXEC mode.

show redundancy application group [*group-id* | **all**]

Syntax Description

group-id	(Optional) Redundancy group ID. Valid values are 1 and 2.
all	(Optional) Display information about all redundancy groups.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
15.3(2)T	This command was integrated into Cisco IOS Release 15.3(2)T.

Usage Guidelines

Use the **show redundancy application group** command to display the current state of each interbox redundancy group on the device and the peer device.

Examples

The following is sample output from the **show redundancy application group all** command:

```
Device# show redundancy application group all

Faults states Group 1 info:
        Runtime priority: [200]
                RG Faults RG State: Up.
                        Total # of switchovers due to faults:           3
                        Total # of down/up state changes due to faults: 2
Group ID:1
Group Name:grp2
Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: UNKNOWN
Peer Presence: No
Peer Comm: No
Peer Progression Started: No
RF Domain: btob-one
         RF state: ACTIVE
         Peer RF state: DISABLED
RG Protocol RG 1
------------------
        Role: Active
        Negotiation: Enabled
        Priority: 200
        Protocol state: Active
        Ctrl Intf(s) state: Down
        Active Peer: Local
        Standby Peer: Not exist
        Log counters:
```

```
                role change to active: 2
                role change to standby: 0
                disable events: rg down state 1, rg shut 0
                ctrl intf events: up 0, down 2, admin_down 1
                reload events: local request 3, peer request 0
RG Media Context for RG 1
--------------------------
        Ctx State: Active
        Protocol ID: 1
        Media type: Default
        Control Interface: GigabitEthernet0/1/0
        Hello timer: 5000
        Effective Hello timer: 5000, Effective Hold timer: 15000
         LAPT values: 0, 0
        Stats:
                Pkts 0, Bytes 0, HA Seq 0, Seq Number 0, Pkt Loss 0
                Authentication not configured
                Authentication Failure: 0
                Reload Peer: TX 0, RX 0
                Resign: TX 1, RX 0
        Standby Peer: Not Present.
Faults states Group 2 info:
        Runtime priority: [150]
                RG Faults RG State: Up.
                        Total # of switchovers due to faults:           2
                        Total # of down/up state changes due to faults: 2
Group ID:2
Group Name:name1
Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: UNKNOWN
Peer Presence: No
Peer Comm: No
Peer Progression Started: No
RF Domain: btob-two
         RF state: ACTIVE
         Peer RF state: DISABLED
RG Protocol RG 2
------------------
        Role: Active
        Negotiation: Enabled
        Priority: 150
        Protocol state: Active
        Ctrl Intf(s) state: Down
        Active Peer: Local
        Standby Peer: Not exist
        Log counters:
                role change to active: 1
                role change to standby: 0
                disable events: rg down state 1, rg shut 0
                ctrl intf events: up 0, down 2, admin_down 1
                reload events: local request 2, peer request 0
RG Media Context for RG 2
--------------------------
        Ctx State: Active
        Protocol ID: 2
        Media type: Default
        Control Interface: GigabitEthernet0/1/0
        Hello timer: 5000
        Effective Hello timer: 5000, Effective Hold timer: 15000
         LAPT values: 0, 0
        Stats:
                Pkts 0, Bytes 0, HA Seq 0, Seq Number 0, Pkt Loss 0
```

```
        Authentication not configured
        Authentication Failure: 0
        Reload Peer: TX 0, RX 0
        Resign: TX 0, RX 0
Standby Peer: Not Present.
```

The table below describes the significant fields shown in the display.

Table 89: show redundancy application group all Field Descriptions

Field	Description
Faults states Group 1 info	Redundancy group faults information for Group 1.
Runtime priority	Current priority of the redundancy group.
RG Faults RG State	Redundancy group state returned by redundancy group faults.
Total # of switchovers due to faults	Number of switchovers triggered by redundancy group fault events.
Total # of down/up state changes due to faults	Number of down and up state changes triggered by redundancy group fault events.
Group ID	Redundancy group ID.
Group Name	Redundancy group name.
Administrative State	Redundancy group state configured by users.
Aggregate operational state	Current redundancy group state.
My Role	Current role of the device.
Peer Role	Current role of the peer device.
Peer Presence	Indicates if the peer device is detected or not.
Peer Comm	Indicates the communication state with the peer device.
Peer Progression Started	Indicates if the peer device has started Redundancy Framework (RF) progression.
RF Domain	Name of the RF domain for the redundancy group.

Related Commands

Command	Description
show redundancy application control-interface	Displays control interface information for a redundancy group.
show redundancy application faults	Displays fault-specific information for a redundancy group.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.

Command	Description
show redundancy application protocol	Displays protocol-specific information for a redundancy group.

show redundancy application if-mgr

To display interface manager information for a redundancy group, use the **show redundancy application if-mgr** command in privileged EXEC mode.

show redundancy application if-mgr group [*group-id*]

Syntax Description

group	Specifies the redundancy group.
group-id	(Optional) Redundancy group ID. Valid values are 1 to 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show redundancy application if-mgr** command shows information of traffic interfaces protected by redundancy groups. When a traffic interface is functioning with the redundancy group, the state is no shut on the active device, and shut on the standby device. On the other hand, it is always shut on the standby device.

Examples

The following is sample output from the **show redundancy application if-mgr** command:

```
Router# show redundancy application if-mgr group 2
RG ID: 2
 Interface       VIP         VMAC        Shut   Decrement
 ============================================================
 GigabitEthernet0/1/7 10.1.1.3 0007.b422.0016  no shut    50
 GigabitEthernet0/3/1 11.1.1.3 0007.b422.0017  no shut    50
```

The table below describes the significant fields shown in the display.

Table 90: show redundancy application if-mgr Field Descriptions

Field	Description
RG ID	Redundancy group ID.
Interface	Interface name.
VIP	Virtual IP address for this traffic interface.
VMAC	Virtual MAC address for this traffic interface.
Shut	The state of this interface. **Note** It is always “shut” on the standby box.
Decrement	The decrement value for this interface. When this interface goes down, the runtime priority of its redundancy group decreases.

Related Commands

Command	Description
show redundancy application control-interface	Displays control interface information for a redundancy group.
show redundancy application faults	Displays fault-specific information for a redundancy group.
show redundancy application group	Displays redundancy group information.
show redundancy application protocol	Displays protocol-specific information for a redundancy group

show redundancy application protocol

To display protocol-specific information for a redundancy group, use the **show redundancy application protocol**command in privileged EXEC mode.

show redundancy application protocol {*protocol-id* | **group** [*group-id*] }

Syntax Description

protocol-id	Protocol ID. The range is from 1 to 8.
group	Specifies the redundancy group.
group-id	(Optional) Redundancy group ID. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show redundancy application protocol**command shows information returned by redundancy group protocol.

Examples

The following is sample output from the **show redundancy application protocol** command:

```
Router# show redundancy application protocol 3

Protocol id: 3, name:
 BFD: ENABLE
 Hello timer in msecs: 0
 Hold timer in msecs: 0
```

The table below describes the significant fields shown in the display.

Table 91: show redundancy application protocol Field Descriptions

Field	Description
Protocol id	Redundancy group protocol ID.
BFD	Indicates whether the BFD protocol is enabled for the redundancy group protocol.
Hello timer in msecs	Redundancy group hello timer, in milliseconds, for the redundancy group protocol. The default is 3000 msecs.
Hold timer in msecs	Redundancy group hold timer, in milliseconds, for the redundancy group protocol. The default is 10000 msecs.

Related Commands

Command	Description
show redundancy application group	Displays redundancy group information.
show redundancy application control-interface	Displays control interface information for a redundancy group.
show redundancy application faults	Displays fault-specific information for a redundancy group.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.

show redundancy application transport

To display transport-specific information for a redundancy group, use the **show redundancy application transport**command in privileged EXEC mode.

show redundancy application transport {**client** | **group** [*group-id*]}

Syntax Description

client	Displays transport client-specific information.
group	Displays the redundancy group name.
group-id	(Optional) Redundancy group ID. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show redundancy application transport** command shows information for redundancy group transport.

Examples

The following is sample output from the **show redundancy application transport group** command:

```
Router# show redundancy application transport group 1
Transport Information for RG (1)
```

Related Commands

Command	Description
show redundancy application control-interface	Displays control interface information for a redundancy group.
show redundancy application faults	Displays fault-specific information for a redundancy group.
show redundancy application group	Displays redundancy group information.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.
show redundancy application protocol	Displays protocol-specific information for a redundancy group.

show running-config mdns-sd policy

To display current running multicast Domain Name System (mDNS) service-policy configuration details for the device or interface, use the **show running-config mdns-sd policy** command in privileged EXEC mode.

show running-config mdns-sd policy {**global** | **interface** *type number*}

Syntax Description

global	Displays current running mDNS service-policy configuration details for the device.
interface *type number*	Displays current running mDNS service-policy configuration details for the specified interface.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(2)E	This command was introduced.
Cisco IOS XE 3.6E	This command was integrated into the Cisco IOS XE 3.6E release.

Usage Guidelines

To view current running mDNS service-policy configuration details for the device, use the **show running-config mdns-sd policy global** command form.

To view current running mDNS service-policy configuration details for a specific interface, use the **show running-config mdns-sd policy interface** *type number* command form

Examples

The following is sample output for the **show running-config mdns-sd policy** command.

The current running configuration details for the device is displayed below. The output signifies that the mDNS gateway functionality is enabled on the device, and the designated gateway status is enabled without a Time to Live (TTL) value.

```
Device> enable
Device# show running-config mdns-sd policy global


service-routing mdns-sd
  designated-gateway enable
  service-type-enumeration period 16
```

The current running configuration details for the interface is displayed below. The output given below signifies that the mDNS gateway functionality is enabled on the interface, and the designated gateway status is enabled with a TTL value of 20 minutes.

Examples

Current running configuration details for a device interface

The output given below signifies that the mDNS gateway functionality is enabled on the interface, and the designated gateway status is enabled with a TTL value of 20 minutes.

```
Device> enable
Device# show running-config mdns-sd policy interface ethernet 0/1


service-routing mdns-sd
  designated-gateway enable ttl 20
```

Related Commands

Command	Description
show running-config mdns-sd service-instance	Displays current running mDNS service-instance configuration details.
show running-config mdns-sd service-list	Displays current running mDNS service-list configuration details.

show running-config mdns-sd service-instance

To display current running multicast Domain Name System (mDNS) service-instance configuration details, use the **show running-config mdns-sd service-instance** command in privileged EXEC mode.

show running-config mdns-sd service-instance {**all** | **name** *service-instance-name* **regtype** *service-type* **domain** *name*}

Syntax Description

all	Displays all current running mDNS service-instance configuration details.
name *service-instance-name*	Displays current running mDNS service-instance configuration details for the specified service instance.
regtype *service-type*	Specifies that the service instance is of the specified service type.
domain *name*	Specifies the domain with which the service-instance is being associated.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(2)E	This command was introduced.
Cisco IOS XE 3.6E	This command was integrated into the Cisco IOS XE 3.6E release.

Usage Guidelines

To view current running mDNS service-instance configuration details for all services, use the **show running-config mdns-sd service-instance all** command form.

To view current running mDNS service-policy configuration details for a specific service-instance, use the **show running-config mdns-sd service-instance name** *service-instance-name* command form. To view specific service-instance configuration details, you need to specify the service type and domain name too.

Examples

The following is a sample output for the **show running-config mdns-sd service-instance** command.

The current running mDNS service-instance configuration information for all services is displayed below. The service instance names, the service type and the domain names are displayed in the output.

```
Device> enable
Device# show running-config mdns-sd service-instance all


service-instance mdns-sd service serv2 regtype _tcp._123 domain tcp
 port 55
service-instance mdns-sd service serv1 regtype _tcp._12 domain tcp
```

Examples

Current running mDNS service-instance configuration information for a service instance.

```
Device> enable
Device# show running-config mdns-sd service-instance name serv1 regtype _tcp._12 domain tcp

service-instance mdns-sd service serv1 regtype _tcp._12 domain tcp
```

Related Commands

Command	Description
show running-config mdns-sd policy	Displays current running mDNS service-policy configuration details for the device or interface.
show running-config mdns-sd service-list	Displays current running mDNS service-list configuration details.

show running-config mdns-sd service-list

To display current running multicast Domain Name System (mDNS) service-list configuration details, use the **show running-config mdns-sd service-list** command in privileged EXEC mode.

show running-config mdns-sd service-list {**all** | **name** *service-list-name* [**sequence-number** *sequence-number*] | **query**}

Syntax Description

all	Displays all current running mDNS service-list configuration details. The details include the service-list name, sequence number, the option that is applied, and associated match statements, if any.
name *service-list-name*	Displays current running mDNS service-list configuration details for the specified service list.
sequence-number *sequence-number*	(Optional) Specifies that the service-list configuration details must be displayed for the specified sequence number. **Note** You must specify the sequence number since more than one sequence number can be associated with the same service-list.
query	Displays current running mDNS service-list query details.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(2)E	This command was introduced.
Cisco IOS XE 3.6E	This command was integrated into the Cisco IOS XE 3.6E release.

Usage Guidelines

To view current running mDNS service-list configuration details for all service-lists, use the **show running-config mdns-sd service-list all** command form.

To view current running mDNS service-list configuration details for a specific service-list, use the **show running-config mdns-sd service-list name** *service-list-name* [**sequence-number** *sequence-number*] command form. The keyword-argument pair **sequence-number** *sequence-number* enables you to view the match statements associated with the service-list. The match statements are associated with service-lists for filtering types of service, types of service instances and associated queries, and types of messages such as announcements and queries.

To view queries that are associated with various service-lists, use the **show running-config mdns-sd service-list query** command form.

Examples

The following is a sample output for the **show running-config mdns-sd service-list** command.

The current running mDNS service-list configuration information is displayed below. The service list names, match statements, and the permit or deny option details are displayed in the output.

```
Device> enable
Device# show running-config mdns-sd service-list all
```

```
service-list mdns-sd sl1 permit 2
service-list mdns-sd sl3 deny 10
 match message-type announcement
 match service-type _ipp._tcp
service-list mdns-sd srvc-lst permit 6
```

Examples

Current running mDNS service-list configuration for an active query.

```
Device> enable
Device# show running-config mdns-sd service-list query
```

```
service-list mdns-sd sl2 query
service-list mdns-sd sl-qry query
 service-type ser-type
 service-type _tcp._dom1
service-list mdns-sd sd2 query
```

Related Commands

Command	Description
show running-config mdns-sd policy	Displays current running mDNS service-policy configuration details for the device or interface.
show running-config mdns-sd service-instance	Displays current running mDNS service-instance configuration details.

show running-config vrf

To display the subset of the running configuration of a router that is linked to a specific VPN routing and forwarding (VRF) instance or linked to all VRFs configured on the router, use the **show running-config vrf** command in privileged EXEC mode.

show running-config vrf [*vrf-name*]

Syntax Description

vrf-name	(Optional) Name of the VRF configuration that you want to display.

Command Default

If you do not specify the name of a VRF configuration, the running configurations of all VRFs on the router are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.5S	This command was modified. The output of the command was modified to display the Network Address Translation (NAT) configuration.

Usage Guidelines

Use the **show running-config vrf** command to display a specific VRF configuration or to display all VRF configurations on the router. To display the configuration of a specific VRF, specify the name of the VRF.

This command displays the following elements of the VRF configuration:

- The VRF submode configuration.
- The routing protocol and static routing configurations associated with the VRF.
- The configuration of interfaces in the VRF, which includes the configuration of any owning controller and physical interface for a subinterface.

Examples

The following is sample output from the **show running-config vrf** command. It includes a base VRF configuration for VRF vpn3 and Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF) configurations associated with VRF vpn3.

```
Router# show running-config vrf vpn3

Building configuration...

Current configuration : 720 bytes
```

```
ip vrf vpn3
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
!
interface GigabitEthernet0/0/1
 description connected to nat44-1ru-ce1 g0/0/0
 ip vrf forwarding vpn3
 ip address 172.17.0.1 255.0.0.0
 ip nat inside
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/3
 no ip address
 negotiation auto
!
interface GigabitEthernet0/0/3.2
 encapsulation dot1Q 2
 ip vrf forwarding vpn3
 ip address 10.0.0.1 255.255.255.0
 ip nat inside
!
router bgp 100
 !
 address-family ipv4 vrf vpn3
  redistribute connected
  redistribute static
 exit-address-family
ip nat inside source route-map rm-vpn3 pool shared-pool vrf vpn3 match-in-vrf overload
ip nat pool shared-pool 10.0.0.2 10.0.0.254 prefix-length 24
!
router ospf 101 vrf vpn3
 log-adjacency-changes
 area 1 sham-link 10.43.43.43 10.23.23.23 cost 10
 network 172.17.0.0 0.255.255.255 area 1
.
.
.
end
```

The table below describes the significant fields shown in the display.

Table 92: show running-config vrf Field Descriptions

Field	Description
Current configuration: 720 bytes	Indicates the number of bytes (720) in the VRF vpn3 configuration.
ip vrf vpn3	Indicates the name of the VRF (vpn3) for which the configuration is displayed.
rd 100:1	Identifies the route distinguisher (100:1) for VRF vpn3.
route-target export 100:1 route-target import 100:1	Specifies the route-target extended community for VRF vpn3. • Routes tagged with route-target export 100:1 are exported from VRF vpn3. • Routes tagged with the route-target import 100:1 are imported into VRF vpn3.

Field	Description
interface GigabitEthernet0/0/1	Specifies the interface associated with VRF vpn3.
ip vrf forwarding vpn3	Associates VRF vpn3 with the named interface.
ip address 172.17.0.1 255.0.0.0	Configures the IP address of the Gigabit Ethernet interface.
ip nat inside	Enables NAT of inside addresses.
router bgp 100	Sets up a BGP routing process for the router with the autonomous system number as 100.
address-family ipv4 vrf vpn3	Sets up a routing session for VRF vpn3 using the standard IPv4 address prefixes.
redistribute connected	Redistributes routes that are automatically established by the IP on an interface into the BGP routing domain.
ip nat pool	Defines a pool of IP addresses for NAT.
router ospf 101 vrf vpn3	Sets up an OSPF routing process and associates VRF vpn3 with OSPF VRF processes.
area 1 sham-link 10.43.43.43 10.23.23.23 cost 10	Configures a sham-link interface on a provider edge (PE) router in a Multiprotocol Label Switching (MPLS) VPN backbone. • 1 is the ID number of the OSPF area assigned to the sham-link. • 10.43.43.43 is the IP address of the source PE router. • 10.23.23.23 is the IP address of the destination PE router. • 10 is the OSPF cost to send IP packets over the sham-link interface.
network 172.17.0.0 0.255.255.255 area 1	Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.

Related Commands

Command	Description
ip vrf	Configures a VRF routing table.
show ip interface	Displays the usability status of interfaces configured for IP.
show ip vrf	Displays the set of defined VRFs and associated interfaces.
show running-config interface	Displays the configuration for a specific interface.

show tech nat

To display NAT data that is useful for troubleshooting. The outpout of **show tech nat** command includes output for the following commands:

- **show clock**
- **show version**
- **show running-config**
- **show ip nat translations total**
- **show ip nat stat**
- **show platform hardware qfp active statistics drop**
- **show platform hardware qfp active feature nat datapath stats**
- **show platform hardware qfp active feature nat datapath basecfg**
- **show platform hardware qfp active feature nat datapath map**
- **show platform hardware qfp active feature nat datapath pool**
- **show platform hardware qfp active feature nat datapath port**
- **show platform hardware qfp active feature nat datapath time**
- **show platform hardware qfp active feature nat datapath hsl**
- **show platform hardware qfp active feature nat datapath rmap**
- **show platform hardware qfp active feature nat datapath limit**
- **show platform hardware qfp active feature nat datapath esp**
- **show platform hardware qfp active feature nat datapath gatein**
- **show platform hardware qfp active feature nat datapath gateout**
- **show platform hardware qfp active feature nat datapath ha**
- **show platform hardware qfp active feature nat datapath nonpat**
- **show platform hardware qfp active feature alg statistics**
- **show platform hardware qfp active datapath utilization**
- **show platform hardware qfp active tcam resource-manager usage**

- **show platform software nat counters**
- **show platform software nat rp active msg-stats**
- **show platform software nat rp active db-stats**

```
show tech nat
```

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS XE Release 16.3	This command was introduced.

sip address

To configure a Session Initiation Protocol (SIP) server IPv6 address to be returned in the SIP server's IPv6 address list option to clients, use the **sip address**command in DHCP for IPv6 pool configuration mode. To disable this feature, use the **no** form of this command.

sip address *ipv6-address*
no sip address *ipv6-address*

Syntax Description

ipv6-address	An IPv6 address. The *ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

No default behavior or values

Command Modes

DHCP for IPv6 pool configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

For the Dynamic Host Configuration Protocol (DHCP) for IPv6 server to obtain prefixes from RADIUS servers, the user must also configure the authorization, authentication, and accounting (AAA) client and PPP on the router. For information on how to configure the AAA client and PPP, see the "Implementing ADSL and Deploying Dial Access for IPv6" module.

The **sip address** command configures a SIP server IPv6 address to be returned in the SIP server's IPv6 address list option to clients. To configure multiple SIP server addresses, issue this command multiple times. The new addresses will not overwrite old ones.

Examples

In the following example, the SIP server IPv6 address 2001:0db8::2 is configured to be returned in the SIP server's IPv6 address list option to clients:

```
sip address 2001:0DB8::2
```

Related Commands

Command	Description
prefix-delegation aaa	Specifies that prefixes are to be acquired from AAA servers.
sip domain-name	Configures an SIP server domain name to be returned in the SIP server's domain name list option to clients.

sip domain-name

To configure a Session Initiation Protocol (SIP) server domain name to be returned in the SIP server's domain name list option to clients, use the **sip domain-name**command in DHCP for IPv6 pool configuration mode. To disable this feature, use the **no** form of this command.

sip domain-name *domain-name*
no sip domain-name *domain-name*

Syntax Description

domain-name	A domain name for a DHCP for IPv6 client.

Command Default

No default behavior or values.

Command Modes

DHCP for IPv6 pool configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

In order for the Dynamic Host Configuration Protocol (DHCP) for IPv6 server to obtain prefixes from RADIUS servers, the user must also configure the authorization, authentication, and accounting (AAA) client and PPP on the router. For information on how to configure the AAA client and PPP, see the "Implementing ADSL and Deploying Dial Access for IPv6" module.

The **sip domain-name** command configures a SIP server domain name to be returned in the SIP server's domain name list option to clients. To configure multiple SIP server domain names, issue this command multiple times. The new domain names will not overwrite old ones.

Examples

The following example configures the SIP server domain name sip1.cisco.com to be returned in the SIP server's domain name list option to clients:

```
sip domain-name sip1.cisco.com
```

Related Commands

Command	Description
prefix-delegation aaa	Specifies that prefixes are to be acquired from AAA servers.
sip address	Configures a SIP server IPv6 address to be returned in the SIP server's IPv6 address list option to clients.

snmp-server enable traps dhcp

To enable DHCP Simple Network Management Protocol (SNMP) trap notifications, use the **snmp-server enable traps dhcp** command in global configuration mode. To disable DHCP trap notifications, use the **no** form of this command.

snmp-server enable traps dhcp [**duplicate**] [**interface**] [**pool**] [**subnet**] [**time**]
no snmp-server enable traps dhcp [**duplicate**] [**interface**] [**pool**] [**subnet**] [**time**]

Syntax Description

duplicate	(Optional) Sends notification about duplicate IP addresses.
interface	(Optional) Sends notification that a per interface lease limit is exceeded.
pool	(Optional) Sends notification when address utilization for an address pool has risen above or fallen below a configurable threshold.
subnet	(Optional) Sends notification when address utilization for a subnet has risen above or fallen below a configurable threshold.
time	(Optional) Sends notification that the DHCP server has started or stopped.

Command Default

DHCP trap notifications are not sent.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.

Usage Guidelines

If you do not specify any of the optional keywords, all DHCP trap notifications are enabled.

Examples

The following example shows how to send SNMP trap notifications to the SNMP manager when the secondary subnet utilization falls below or exceeds the configured threshold:

```
Router(config)# ip dhcp pool pool2
Router(dhcp-config)# utilization mark high 80 log
Router(dhcp-config)# utilization mark low 70 log
Router(dhcp-config)# network 192.0.2.0 255.255.255.0
Router(dhcp-config)# network 192.0.4.0 255.255.255.252 secondary
Router(config-dhcp-subnet-secondary)# override utilization high 40
Router(config-dhcp-subnet-secondary)# override utilization low 30
!
Router(config)# snmp-server enable traps dhcp subnet
```

In the following example, all DHCP trap notifications will be sent to the SNMP manager in response to DHCP server events:

```
Router(config)# snmp-server enable traps dhcp
```

source-interface (mDNS)

To specify an alternate source interface for outgoing multicast Domain Name System (mDNS) packets on a device, use the **source-interface** command in mDNS configuration mode. To disable the alternate source interface for outgoing mDNS packets on a device, use the **no** form of this command.

source-interface *type number*
no source-interface *type number*

Syntax Description

type	Interface type. Specify the interface that you want to configure as the alternate source interface for outgoing mDNS packets on the device. For more information, use the question mark (?) online help function.
number	Interface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Default

An alternate source interface for outgoing mDNS packets is not configured on a device.

Command Modes

Multicast DNS configuration (config-mdns)

Command History

Release	Modification
15.2(2)E	This command was introduced.
Cisco IOS XE 3.6E	This command was integrated into the Cisco IOS XE 3.6E release.
15.2(1)SY	This command was integrated into Cisco IOS Release 15.2(1)SY.
Cisco IOS XE Release 3.15S	This command was integrated into the Cisco IOS XE Release 3.15S
15.5(2)S	This command was integrated into Cisco IOS 15.5(2)S Release.

Usage Guidelines

Some devices have interfaces for which no IP address is assigned. If you configure the **source-interface** command on such a device, then the IP address of the source-interface is used when outgoing mDNS service information is transported through the interface with no IP address.

Note Before configuring the alternate mDNS source interface for a device, ensure that the source interface has a valid IP address assigned to it.

Examples

The following example shows you how to specify an interface as an alternate source interface for outgoing mDNS packets on a device:

```
Device> enable
Device# configure terminal
Device(config)# service-routing mdns-sd
Device(config-mdns)# source-interface ethernet 0/1
Device(config-mdns)# exit
```

Related Commands

Command	Description
service-routing mdns-sd	Enables mDNS gateway functionality for a device.
show mdns statistics	Displays mDNS statistics for the specified service-list.
show running-config mdns-sd policy	Displays current running mDNS service-policy configuration details for the device or interface.

subnet prefix-length

To configure a subnet allocation pool and determine the size of subnets that are allocated from the pool, use the **subnet prefix-length** command in DHCP pool configuration mode. To unconfigure subnet pool allocation, use the **no** form of this command.

subnet prefix-length *prefix-length*
no subnet prefix-length *prefix-length*

Syntax Description

prefix-length	Configures the IP subnet prefix length in classless interdomain routing (CIDR) bit count notation. The range is from 1 to 31.

Command Default

No default behavior or values.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

This command is used to configure a Cisco IOS router as a subnet allocation server for a centralized or remote Virtual Private Network (VPN) on-demand address pool (ODAP) manager. This command is configured under a DHCP pool. The *prefix-length* argument is used to determine the size of the subnets that are allocated from the subnet allocation pool. The values that can be configured for the *prefix-length* argument follow CIDR bit count notation format.

Configuring Global Subnet Pools

Global subnet pools are created in a centralized network. The ODAP server allocates subnets from the subnet allocation server based on subnet availability. When the ODAP manager allocates a subnet, the subnet allocation server creates a subnet binding. This binding is stored in the DHCP database for as long as the ODAP server requires the address space. The binding is destroyed and the subnet is returned to the subnet pool only when the ODAP server releases the subnet as address space utilization decreases.

Configuring VPN Subnet Pools

A subnet allocation server can be configured to assign subnets from VPN subnet allocation pools for Multiprotocol Label Switching (MPLS) VPN clients. VPN routes between the ODAP manager and the subnet allocation server are configured based on VRF name or VPN ID configuration. The VRF and VPN ID are configured to maintain routing information that defines customer VPN sites. This customer site is attached to a provider edge (PE) router. A VRF consists of an IP routing table, a derived Cisco Express Forwarding (CEF) table, a set of interfaces that use the forwarding table, and a set of rules and routing protocol parameters that control the information that is included in the routing table.

Configuring VPN Subnet Pools for VPN clients with VPN IDs

A subnet allocation server can also be configured to assign subnets from VPN subnet allocation pools based on the VPN ID of a client. The VPN ID (or Organizational Unique Identifier [OUI]) is a unique identifier

assigned by the IEEE. VPN routes between the ODAP manager and the subnet allocation server are enabled by configuring the DHCP pool with a VPN ID that matches the VPN ID that is configured for the VPN client.

Examples

Global Configuration Example

The following example configures a router to be a subnet allocation server and creates a global subnet allocation pool named GLOBAL-POOL from the 10.0.0.0 network. The configuration of the **subnet prefix-length** command in this example configures each subnet that is allocated from the subnet pool to support 254 host IP addresses.

```
ip dhcp pool GLOBAL-POOL
 network 10.0.0.0 255.255.255.0
 subnet prefix-length 24
```

VPN Configuration Example

The following example configures a router to be a subnet allocation server and creates a VPN routing and forwarding (VRF) subnet allocation pool named VRF-POOL from the 172.16.0.0 network and configures the VPN to match the VRF named pool1. The configuration of the **subnet prefix-length** command in this example configures each subnet that is allocated from the subnet pool to support 62 host IP addresses.

```
ip dhcp pool VRF-POOL
 vrf pool1
 network 172.16.0.0 /16
 subnet prefix-length 26
```

VPN ID Configuration Example

The following example configures a router to be a subnet allocation server and creates a VRF subnet allocation pool named VPN-POOL from the 192.168.0.0 network and configures the VRF named abc. The VPN ID must match the unique identifier that is assigned to the client site. The route target and route distinguisher are configured in the as-number:network number format. The route target and route distinguisher must match. The configuration of the **subnet prefix-length** command in this example configures each subnet that is allocated from the subnet pool to support 30 host IP addresses.

```
ip vrf abc
 rd 100:1
 route-target both 100:1
 vpn id 1234:123456
!
ip dhcp pool VPN-POOL
 vrf abc
 network 192.168.0.0 /24
 subnet prefix-length /27
```

Related Commands

Command	Description
ip dhcp database	Configures a Cisco IOS DHCP server to save automatic bindings on a remote host called a database agent.

Command	Description
ip dhcp pool	Enables the IP address of an interface to be automatically configured when a DHCP pool is populated with a subnet from IPCP negotiation.
network (DHCP)	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.
show ip dhcp pool	Displays information about the DHCP pools.

term ip netmask-format

To specify the format in which netmasks are displayed in **show** command output, use the **term ip netmask-format**command inEXEC configuration mode. To restore the default display format, use the **no** form of this command.

term ip netmask-format {**bitcount** | **decimal** | **hexadecimal**}
no term ip netmask-format [**bitcount** | **decimal** | **hexadecimal**]

Syntax Description

bitcount	Number of bits in the netmask.
decimal	Netmask dotted decimal notation.
hexadecimal	Netmask hexadecimal format.

Command Default

Netmasks are displayed in dotted decimal format.

Command Modes

EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

IP uses a 32-bit mask that indicates which address bits belong to the network and subnetwork fields, and which bits belong to the host field. This range of IP addresses is called a *netmask*. By default, **show** commands display an IP address and then its netmask in dotted decimal notation. For example, a subnet would be displayed as 131.108.11.55 255.255.255.0.

However, you can specify that the display of the network mask appear in hexadecimal format or bit count format instead. The hexadecimal format is commonly used on UNIX systems. The previous example would be displayed as 131.108.11.55 0XFFFFFF00.

The bitcount format for displaying network masks is to append a slash (/) and the total number of bits in the netmask to the address itself. The previous example would be displayed as 131.108.11.55/24.

Examples

The following example specifies that network masks for the session be displayed in bitcount notation in the output of **show** commands:

```
term ip netmask-format bitcount
```

timers hellotime

To configure timers for hellotime and holdtime messages for a redundancy group, use the **timers hellotime**command in redundancy application protocol configuration mode. To disable the timers in the redundancy group, use the **no** form of this command.

timers hellotime [**msec**] *seconds* **holdtime** [**msec**] *seconds*
no timers hellotime [**msec**] *seconds* **holdtime** [**msec**] *seconds*

Syntax Description

msec	(Optional) Specifies the interval, in milliseconds, for hello messages.
seconds	Interval time, in seconds, for hello messages. The range is from 1 to 254.
holdtime	Specifies the hold timer.
msec	Specifies the interval, in milliseconds, for hold time messages.
seconds	Interval time, in milliseconds, for hold time messages. The range is from 6 to 255.

Command Default

The default value for the hellotime interval is 3 seconds and for the holdtime interval is 10 seconds.

Command Modes

Redundancy application protocol configuration (config-red-app-prtc)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The hello time is an interval in which hello messages are sent. The holdtime is the time before the active or the standby device is declared to be in down state. Use the **msec** keyword to configure the timers in milliseconds.

Note If you allocate a large amount of memory to the log buffer (e.g. 1 GB), then the CPU and memory utilization of the router increases. This issue is compounded if small intervals are set for the hellotime and the holdtime. If you want to allocate a large amount of memory to the log buffer, we recommend that you accept the default values for the hellotime and holdtime. For the same reason, we also recommend that you do not use the **preempt** command.

Examples

The following example shows how to configure the hellotime and holdtime messages:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# protocol 1
Router(config-red-app-prtcl)# timers hellotime 100 holdtime 100
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
group(firewall)	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.
protocol	Defines a protocol instance in a redundancy group.

trusted-port (DHCPv6 Guard)

To configure a port to become a trusted port, use the **trusted-port** command in Dynamic Host Configuration Protocol version 6 (DHCPv6) guard configuration mode. To disable this function, use the **no** form of this command.

trusted-port
no trusted-port

Syntax Description

This command has no arguments or keywords.

Command Default

No ports are trusted.

Command Modes

DHCPv6 guard configuration (config-dhcp-guard)

Command History

Release	Modification
15.2(4)S	This command was introduced.

Usage Guidelines

When the **trusted-port** command is enabled, messages received on ports that have this policy are not verified.

Examples

The following example defines a DHCPv6 guard policy name as policy1, places the router in DHCPv6 guard configuration mode, and sets the port to trusted:

```
Router(config)# ipv6 dhcp guard policy policy1
Router(config-dhcp-guard)# trusted-port
```

Related Commands

Command	Description
ipv6 dhcp guard policy	Defines the DHCPv6 guard policy name.

update arp

To secure dynamic Address Resolution Protocol (ARP) entries in the ARP table to their corresponding DHCP bindings, use the **update arp**command in DHCP pool configuration mode. To disable this command and change secure ARP entries to dynamic ARP entries, use the **no** form of this command.

update arp
no update arp

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

The **update arp** DHCP pool configuration command is used to secure ARP table entries and their corresponding DHCP leases. However, existing active leases are not secured. These leases will remain insecure until they are renewed. When the lease is renewed, it is treated as a new lease and will be secured automatically. If this feature is disabled on the DHCP server, all existing secured ARP table entries will automatically change to dynamic ARP entries.

This command can be configured only under the following conditions:

- DHCP network pools in which bindings are created automatically and destroyed upon lease termination or when the client sends a DHCPRELEASE message.
- Directly connected clients on LAN interfaces and wireless LAN interfaces.

The configuration of this command is not visible to the client. When this command is configured, secured ARP table entries that are created by a DHCP server cannot be removed from the ARP table by the **clear arp-cache** command. This is designed behavior. If a secure ARP entry created by the DHCP server must be removed, the **clear ip dhcp binding** command can be used. This command will clear the DHCP binding and secured ARP table entry.



Note This command does not secure ARP table entries for BOOTP clients.

Examples

The following example configures the Cisco IOS DHCP server to secure ARP table entries to their corresponding DHCP leases within the DHCP pool named WIRELESS-POOL:

```
ip dhcp pool WIRELESS-POOL
 update arp
```

Related Commands

Command	Description
clear arp-cache	Deletes all dynamic entries from the ARP cache.
clear ip dhcp binding	Deletes an automatic address binding from the Cisco IOS DHCP Server database.

update dns

To dynamically update the Domain Name System (DNS) with address (A) and pointer (PTR) Resource Records (RRs) for some address pools, use the **update dns** command in global configuration mode. To disable dynamic updates, use the **no** form of this command.

update dns [**both** | **never**] [**override**] [**before**]
no update dns [**both** | **never**] [**override**] [**before**]

Syntax Description

both	(Optional) Dynamic Host Configuration Protocol (DHCP) server will perform Dynamic DNS (DDNS) updates for both PTR (reverse) and A (forward) RRs associated with addresses assigned from an address pool.
never	(Optional) DHCP server will not perform DDNS updates for any addresses assigned from an address pool.
override	(Optional) DHCP server will perform DDNS updates for PTR RRs associated with addresses assigned from an address pool, even if the DHCP client has specified in the fully qualified domain name (FQDN) option that the server should not perform updates.
before	(Optional) DHCP server will perform DDNS updates before sending the DHCP ACK back to the client. The default is to perform updates after sending the DHCP ACK.

Command Default

No updates are performed.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.3(8)YA	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Usage Guidelines

If you configure the **update dns both override** command, the DHCP server will perform DDNS updates for both PTR and A RRs associated with addresses assigned from an address pool, even if the DHCP client specified in the FQDN that the server should not.

If the server is configured using this command with or without any of the other keywords, and if the server does not see an FQDN option in the DHCP interaction, then it will assume that the client does not understand DDNS and act as though it were configured to update both A and PTR records on behalf of the client.

Examples

The following example shows how to configure the DHCP to never update the A and PTR RRs:

```
update dns never
```

Related Commands

Command	Description
ip ddns update method	Specifies a method of DDNS updates of A and PTR RRs and the maximum interval between the updates.

utilization mark high

To configure the high utilization mark of the current address pool size, use the **utilization mark high** command in DHCP pool configuration mode. To remove the high utilization mark, use the **no** form of this command.

utilization mark high *percentage-number* [**log**]
no utilization mark high *percentage-number* [**log**]

Syntax Description

percentage-number	Percentage of the current pool size.
log	(Optional) Enables the logging of a system message.

Command Default

The default high utilization mark is 100 percent of the current pool size.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.4(4)T	The **log** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The current pool size is the sum of all addresses in all the subnets in the pool. If the utilization level exceeds the configured high utilization mark, the pool will schedule a subnet request.

This command can be used with both network and on-demand pools. However, in the case of a network pool, only the **log** option of this command can be used. In the case of an on-demand pool, the **autogrow** *size*option of the **origin** command must be configured.

In certain network deployments, it is important for the network administrator to receive asynchronous notification when the DHCP pools are nearly exhausted so that preventive action can be taken. One common method for such notification is the generation of a system message.

If you use the **log** option, a system message can be generated for a DHCP pool when the pool utilization exceeds the configured high utilization threshold. A system message can also be generated when the pool's utilization is detected to be below the configured low utilization threshold.

Examples

The following example sets the high utilization mark to 80 percent of the current pool size:

```
utilization mark high 80
```

The following pool configuration using the **log** keyword option generates a system message:

```
! ip dhcp pool abc
utilization mark high 30 log
utilization mark low 25 log
network 10.1.1.0 255.255.255.248
!
```

The following system message is generated when the second IP address is allocated from the pool:

```
00:02:01: %DHCPD-6-HIGH_UTIL: Pool "abc" is in high utilization state (2 addresses used out
 of 6). Threshold set at 30%.
```

The following system message is generated when one of the two allocated IP addresses is returned to the pool:

```
00:02:58: %DHCPD-6-LOW_UTIL: Pool "abc" is in low utilization state (1 addresses used out
of 6). Threshold set at 25%.
```

Related Commands

Command	Description
origin	Configures an address pool as an on-demand address pool.
utilization mark low	Configures the low utilization mark of the current address pool size.

utilization mark low

To configure the low utilization mark of the current address pool size, use the **utilization mark low** command in DHCP pool configuration mode. To remove the low utilization mark, use the **no** form of this command.

utilization mark low *percentage-number*
no utilization mark low *percentage-number*

Syntax Description

percentage-number	Percentage of the current pool size.

Command Default

The default low utilization mark is 0 percent of the current pool size.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The current pool size is the sum of all addresses in all the subnets in the pool. If the utilization level drops below the configured low utilization mark, a subnet release is scheduled from the address pool.

This command can be used with both network and on-demand pools. However, in the case of a network pool, only the **log** option of this command can be used. In the case of an on-demand pool, the **autogrow** *size*option of the **origin** command must be configured.

In certain network deployments, it is important for the network administrator to receive asynchronous notification when the DHCP pools are nearly exhausted so that preventive action can be taken. One common method for such notification is the generation of a system message.

If you use the **log** option, a system message can be generated for a DHCP pool when the pool utilization exceeds the configured high utilization threshold. A system message can also be generated when the pool's utilization is detected to be below the configured low utilization threshold.

Examples

The following example sets the low utilization mark to 20 percent of the current pool size:

```
utilization mark low 20
```

Related Commands

Command	Description
origin	Configures an address pool as an on-demand address pool.
utilization mark high	Configures the high utilization mark of the current address pool size.

view (DNS)

To access or create the specified Domain Name System (DNS) view list member in the DNS view list and then enter DNS view list member configuration mode, use the **view** command in DNS view list configuration mode. To remove the specified DNS view list member from the DNS view list, use the **no** form of this command.

view [**vrf** *vrf-name*] {**default***view-name*} *order-number*
no view [**vrf** *vrf-name*] {**default***view-name*} *order-number*

Syntax Description

vrf *vrf-name*	(Optional) The *vrf-name* argument specifies the name of the Virtual Private Network (VPN) routing and forwarding (VRF) instance associated with the DNS view. Default is the global VRF (that is, the VRF whose name is a NULL string). **Note** If the named VRF does not exist, a warning is displayed but the view is added to the view list anyway. The specified VRF can be defined after the view is added as a member of the view list (and after the view itself is defined). **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name (or the **default** keyword) and the VRF with which it is associated.
default	Specifies that the DNS view is unnamed. **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name (or the **default** keyword) and the VRF with which it is associated.
view-name	String (not to exceed 64 characters) that identifies the name of an existing DNS view. **Note** If the specified view does not exist, a warning is displayed but the default view list member is added anyway. The specified view can be defined after it is added as a member of DNS view list. **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name (or the **default** keyword) and the VRF with which it is associated.
order-number	Integer from 1 to 2147483647 that specifies the order in which the DNS view is checked, with respect to other DNS views in the same DNS view list. **Tip** If the *order-number* values for the DNS views within a DNS view list are configured with large intervals between them (for example, by specifying *order-number* values such as 10, 20, and 30), additional DNS views can be inserted into the view list quickly without affecting the existing ordering or views in the view list. That is, adding a new view to the view list--or changing the ordering of existing views within the view list--does not require that existing views in the view list be removed from the view list and then added back to the list with new *order-number* values.

Command Default No DNS view is accessed or created.

Command Modes DNS view list configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines This command enters DNS view list member configuration mode--for the specified view list member--so that usage restrictions can be configured for that view list member. If the DNS view list member does not exist yet, the specified DNS view is added to the DNS view list along with the value that indicates the order in which the view list member is to be checked (relative to the other DNS views in the view list) whenever the router needs to determine which DNS view list member to use to address a DNS query.

Note The maximum number of DNS views and view lists supported is not specifically limited but is dependent on the amount of memory on the Cisco router. Configuring a larger number of DNS views and view lists uses more router memory, and configuring a larger number of views in the view lists uses more router processor time. For optimum performance, configure no more views and view list members than needed to support your Split DNS query forwarding or query resolution needs.

Note The parameters {**default** | *view-name*} and [**vrf** *vrf-name*] identify an existing DNS view, as defined by using the **ip dns view** command. More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.

The **view** command can be entered multiple times to specify more than one DNS view in the DNS view list.

To display information about a DNS view list, use the **show ip dns view-list** command.

Subsequent Operations on a DNS View List Member

After you use the **view** command to define a DNS view list member and enter DNS view list member configuration mode, you can use any of the following commands to configure usage restrictions for the DNS view list member:

- **restrict authenticated**
- **restrict name-group**
- **restrict source access-group**

These optional, additional restrictions are based on query source authentication, the query hostname, and the query source host IP address, respectively. If none of these optional restrictions are configured for the view list member, the only usage restriction on the view list member is the usage restriction based on its association with a VRF.

Reordering of DNS View List Members

To provide for efficient management of the order of the members in a view list, each view list member definition includes the specification of the position of that member within the list. That is, the order of the members within a view list is defined by explicit specification of position values rather than by the order in

which the individual members are added to the list. This enables you to add members to an existing view list or reorder the members within an existing view list without having to remove all the view list members and then redefine the view list membership in the desired order:

Examples

The following example shows how to add the view user3 to the DNS view list userlist5 and assign this view member the order number 40 within the view list. Next, the view user2, associated with the VRF vpn102 and assigned the order number 20 within the view list, is removed from the view list.

```
Router(config)# ip dns view-list userlist5

Router(cfg-dns-view-list)# view user3 40
Router(cfg-dns-view-list-member)# exit

Router(cfg-dns-view-list)# no view vrf vpn102 user2 20
```

Related Commands

Command	Description
ip dns view-list	Enters DNS view list configuration mode so that DNS views can be added to or removed from the ordered list of DNS views.
restrict authenticated	Restricts the use of the DNS view list member to DNS queries for which the DNS query host can be authenticated.
restrict name-group	Restricts the use of the DNS view list member to DNS queries for which the query hostname matches a particular DNS name list.
restrict source access-group	Restricts the use of the DNS view list member to DNS queries for which the query source IP address matches a particular standard ACL.
show ip dns view-list	Displays information about a particular DNS view list or about all configured DNS view lists.

vrf (DHCP pool)

To associate the on-demand address pool with a VPN routing and forwarding instance (VRF) name, use the **vrf** command in DHCP pool configuration mode. To remove the VRF name, use the **no** form of this command.

vrf *name*
no vrf *name*

Syntax Description

name	Name of the VRF to which the address pool is associated.

Command Default

No default behavior or values

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Associating a pool with a VRF allows overlapping addresses with other pools that are not on the same VRF. Only one pool can be associated with each VRF. If the pool is configured with the **origin dhcp** command or **origin aaa** command, the VRF information is sent in the subnet request. If the VRF is configured with an RFC 2685 VPN ID, the VPN ID will be sent instead of the VRF name.

Examples

The following example associates the on-demand address pool with a VRF named pool1:

```
ip dhcp pool pool1
  origin dhcp subnet size initial 24 autogrow 24
  utilization mark high 85
  utilization mark low 15
  vrf pool1
```

Related Commands

Command	Description
origin	Configures an address pool as an on-demand address pool.

vrf (DHCPv6 pool)

To associate a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) address pool with a virtual private network (VPN) routing and forwarding (VRF) instance, use the **vrf** command in DHCPv6 pool configuration mode. To remove the VRF name, use the **no** form of this command.

vrf *name*
no vrf *name*

Syntax Description

name	Name of the VRF with which the address pool is associated.

Command Default

No VRF is associated with the DHCPv6 address pool.

Command Modes

DHCPv6 pool configuration (config-dhcp)

Command History

Release	Modification
15.1(2)S	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Examples

The following example shows how to configure an IPv6 pool named pool1, and associate pool1 with a VRF instance named vrf1:

```
Router(config)# ipv6 dhcp pool pool1
# vrf vrf1
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCPv6 configuration information pool and enters DHCPv6 pool configuration mode.