

IP Addresses and Services Command Reference for Cisco NCS 5000 Series Routers

First Published: 2016-11-01

Last Modified: 2023-08-18

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)

© 2016–2023 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

Preface xiii

Changes to This Document xiii

Communications, Services, and Additional Information xiii

CHAPTER 1

Access List Commands 1

atomic-disable 3

clear access-list ipv4 4

clear access-list ipv6 6

copy access-list ipv4 8

copy access-list ipv6 10

deny (IPv4) 12

deny (IPv6) 23

interface ipv4/ipv6 access-group 27

ipv4 access-group 29

ipv6 access-group 30

ipv4 access-list 31

ipv6 access-list 32

ipv4 access-list log-update rate 35

ipv6 access-list log-update rate 36

ipv4 access-list log-update threshold 37

ipv6 access-list log-update threshold 38

ipv6 access-list maximum ace threshold 39

object-group network 40

object-group port 42

permit (IPv4) 43

permit (IPv6) 61

remark (IPv4) 68
remark (IPv6) 70
resequence access-list ipv4 72
resequence access-list ipv6 74
set qos-group 76
show access-lists afi-all 78
show access-lists ipv4 79
show access-lists ipv6 83
show object-group network 88
show object-group port 90

CHAPTER 2 ARP Commands 91
arp 92
arp dagr 94
arp gratuitous ignore 95
arp learning 96
arp purge-delay 97
arp timeout 98
clear arp-cache 99
local-proxy-arp 101
peer (DAGR) 102
priority-timeout 103
proxy-arp 104
route distance 105
route metric 106
show arp 107
show arp idb 111
show arp dagr 113
show arp traffic 114
timers (DAGR) 117

CHAPTER 3 Cisco Express Forwarding Commands 119
bgp policy accounting 121
cef adjacency route override rib 123

clear cef ipv4 drops 125
clear cef ipv4 exceptions 127
clear cef ipv6 drops 129
clear cef ipv6 exceptions 131
show adjacency 133
show cef 135
show cef ipv4 137
show cef ipv4 adjacency 140
show cef ipv4 drops 142
show cef ipv4 hardware 144
show cef ipv4 exact-route 147
show cef ipv4 exceptions 149
show cef ipv4 resource 151
show cef ipv4 summary 153
show cef ipv4 unresolved 155
show cef ipv6 157
show cef ipv6 adjacency 161
show cef ipv6 adjacency hardware 165
show cef ipv6 drops 168
show cef ipv6 exact-route 170
show cef ipv6 exceptions 172
show cef ipv6 hardware 174
show cef ipv6 interface 176
show cef ipv6 resource 179
show cef ipv6 summary 181
show cef ipv6 unresolved 183
show cef mpls adjacency 185
show cef mpls adjacency hardware 187
show cef mpls interface 189
show cef mpls unresolved 191
show cef summary 192

CHAPTER 4 **DHCP Commands** 195

clear dhcp ipv4 client 197

clear dhcp ipv4 server binding 198
clear dhcp ipv4 server statistics 199
clear dhcp ipv6 proxy binding 200
clear dhcp ipv6 relay binding 201
clear dhcp ipv6 relay statistics 203
client-mac-mismatch 204
database (DHCPv6 Binding) 205
default-router 207
dhcp ipv4 208
dhcp ipv6 209
dns-server 210
domain-name 211
duplicate-mac-allowed 212
giaddr policy 214
helper-address 216
helper-address (ipv6) 218
interface (DHCP) 220
lease (DHCPv4 Server) 222
limit lease 223
netbios-name-server 224
netbios-node-type 225
pool 226
profile (DHCP) 228
relay information check 230
relay information option 232
relay information option allow-untrusted 234
subnet-mask 236
show dhcp ipv4 client 237
show dhcp ipv4 relay profile 239
show dhcp ipv4 relay profile name 240
show dhcp ipv4 relay statistics 241
show dhcp ipv4 server binding 243
show dhcp ipv4 server profile 245
show dhcp ipv4 server statistics 246

show dhcp ipv6 relay binding 248
show dhcp ipv6 relay statistics 250
show tech support dhcp ipv4 client 252
show dhcp vrf ipv4 server statistics 254
trust relay-reply 256

CHAPTER 5 Host Services and Applications Commands 257
cinetd rate-limit 258
clear host 259
destination address(ipsla) 260
domain ipv4 host 261
domain ipv6 host 262
domain list 263
domain lookup disable 264
domain name (IPAddr) 265
domain name-server 266
ftp client anonymous-password 267
ftp client passive 268
ftp client password 269
ftp client source-interface 270
ftp client username 271
logging source-interface 272
ping (network) 273
ping bulk (network) 276
scp 278
show cinetd services 280
show hosts 282
telnet 284
telnet client source-interface 287
telnet dscp 288
telnet server 289
telnet transparent 291
tftp client source-interface 292
tftp server 293

traceroute 294

CHAPTER 6 HSRP Commands 297

address (hsrp) 299

address global (HSRP) 301

address global subordinate (HSRP) 303

address linklocal(HSRP) 305

address secondary (hsrp) 307

authentication (hsrp) 309

clear hsrp statistics 311

hsrp authentication 312

hsrp delay 314

hsrp ipv4 316

mac-address (hsrp) 318

hsrp priority 320

hsrp redirects 322

hsrp timers 323

hsrp track 325

hsrp use-bia 327

interface (HSRP) 328

preempt (hsrp) 330

priority (hsrp) 332

router hsrp 334

session name 335

show hsrp 337

show hsrp mgo 340

show hsrp statistics 342

show hsrp summary 344

hsrp slave follow 346

subordinate primary virtual IPv4 address 347

subordinate secondary virtual IPv4 address 348

subordinate virtual mac address 349

timers (hsrp) 350

track (hsrp) 352

track(object) 354

CHAPTER 7 LPTS Commands 357

clear lpts ifib statistics 358

clear lpts pifib statistics 359

show lpts bindings 360

show lpts clients 364

show lpts flows 366

show lpts ifib 369

show lpts ifib slices 372

show lpts ifib statistics 375

show lpts ifib times 377

show lpts pifib 379

show lpts pifib hardware police 384

show lpts pifib hardware usage 387

show lpts pifib statistics 389

show lpts port-arbitrator statistics 390

CHAPTER 8 Network Stack IPv4 and IPv6 Commands 391

clear ipv6 neighbors 393

icmp ipv4 rate-limit unreachable 394

ipv4 address (network) 395

ipv4 assembler max-packets 397

ipv4 assembler timeout 398

ipv4 mask-reply 399

ipv4 conflict-policy 400

ipv4 mtu 401

ipv4 unnumbered (point-to-point) 403

ipv6 address 405

ipv6 assembler 407

ipv6 conflict-policy 408

ipv6 address link-local 409

ipv6 enable 411

ipv6 hop-limit 413

ipv6 icmp error-interval 414
ipv6 mtu 416
ipv6 nd dad attempts 418
ipv6 nd managed-config-flag 421
ipv6 nd ns-interval 423
ipv6 nd other-config-flag 425
ipv6 nd prefix 427
ipv6 nd ra-interval 429
ipv6 nd ra-lifetime 431
ipv6 nd reachable-time 432
ipv6 nd redirects 434
ipv6 nd scavenge-timeout 435
ipv6 nd suppress-ra 436
ipv6 neighbor 437
ipv6 path-mtu enable 439
ipv6 path-mtu timeout 440
ipv6 source-route 441
ipv6 tcp-mss-adjust 442
ipv6 virtual address 443
show arm conflicts 445
show arm registrations producers 447
show arm router-ids 449
show arm summary 450
show ipv4 interface 451
show ipv4 traffic 454
show ipv6 interface 456
show ipv6 neighbors 460
show ipv6 neighbors summary 463
show ipv6 path-mtu 464
show ipv6 traffic 465

CHAPTER 9 **Prefix List Commands** 469

clear prefix-list ipv4 470
copy prefix-list ipv4 472

deny (prefix-list) 474
ipv4 prefix-list 476
ipv6 prefix-list 478
permit (prefix-list) 479
remark (prefix-list) 481
resequence prefix-list ipv4 483
resequence prefix-list ipv6 485
show prefix-list afi-all 487
show prefix-list 488
show prefix-list ipv4 489
show prefix-list ipv6 491
show prefix-list ipv4 standby 493

CHAPTER 10 **Transport Stack Commands** 495
clear raw statistics pcb 496
clear tcp pcb 498
clear tcp statistics 499
clear udp statistics 500
forward-protocol udp 501
service tcp-small-servers 503
service udp-small-servers 504
show raw brief 505
show raw detail pcb 507
show raw extended-filters 509
show raw statistics pcb 511
show tcp brief 513
show tcp detail 515
show tcp extended-filters 516
show tcp statistics 518
show udp brief 520
show udp detail pcb 522
show udp extended-filters 524
show udp statistics 525
tcp mss 527

tcp path-mtu-discovery 528
tcp selective-ack 529
tcp synwait-time 530
tcp timestamp 531
tcp window-size 532

CHAPTER 11 VRRP Commands 533
accept-mode 534
accept-mode (subordinate) 536
address-family 537
address (VRRP) 538
address global 540
address linklocal 542
address secondary 544
clear vrrp statistics 546
delay (VRRP) 548
interface (VRRP) 549
message state disable 551
router vrrp 552
session name(vrrp) 553
show vrrp 554
vrrp slave follow 560
subordinate primary virtual IPv4 address(vrrp) 561
subordinate secondary virtual IPv4 address(vrrp) 562
snmp-server traps vrrp events 563
track object(vrrp) 564
unicast-peer 565
vrrp 566
vrrp preempt 568
vrrp priority 570
vrrp text-authentication 571
vrrp timer 572
vrrp track interface 573



Preface

This preface contains these sections:

- Changes to This Document, on page xiii
- Communications, Services, and Additional Information, on page xiii

Changes to This Document

This table lists the technical changes made to this document since it was first published.

Table 1: Changes to this Document

Date	Change Summary
August 2023	Republished for Release 7.10.1.
July 2021	Republished with documentation updates for Cisco IOS XR Release 7.4.1 features.
July 2018	Republished with documentation updates for Cisco IOS XR Release 6.5.1 features.
March 2018	Republished with documentation updates for Cisco IOS XR Release 6.3.2 and 6.4.1 features.
September 2017	Republished with documentation updates for Cisco IOS XR Release 6.3.1 features.
July 2017	Republished with documentation updates for Cisco IOS XR Release 6.2.2 features.
November 2016	Initial release of this document.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results you're looking for with the technologies that matter, visit Cisco Services.

- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



Access List Commands

This module describes the Cisco IOS XR software commands used to configure IP Version 4 (IPv4) and IP Version 6 (IPv6) access lists.

For detailed information about ACL concepts, configuration tasks, and examples, refer to the *IP Addresses and Services Configuration Guide for Cisco NCS 5000 Series Routers*.

- atomic-disable, on page 3
- clear access-list ipv4, on page 4
- clear access-list ipv6, on page 6
- copy access-list ipv4 , on page 8
- copy access-list ipv6, on page 10
- deny (IPv4) , on page 12
- deny (IPv6) , on page 23
- interface ipv4/ipv6 access-group, on page 27
- ipv4 access-group, on page 29
- ipv6 access-group, on page 30
- ipv4 access-list, on page 31
- ipv6 access-list, on page 32
- ipv4 access-list log-update rate , on page 35
- ipv6 access-list log-update rate, on page 36
- ipv4 access-list log-update threshold , on page 37
- ipv6 access-list log-update threshold , on page 38
- ipv6 access-list maximum ace threshold, on page 39
- object-group network, on page 40
- object-group port, on page 42
- permit (IPv4) , on page 43
- permit (IPv6) , on page 61
- remark (IPv4) , on page 68
- remark (IPv6) , on page 70
- resequence access-list ipv4 , on page 72
- resequence access-list ipv6 , on page 74
- set qos-group, on page 76
- show access-lists afi-all, on page 78
- show access-lists ipv4 , on page 79
- show access-lists ipv6, on page 83

- show object-group network, on page 88
- show object-group port , on page 90

atomic-disable

Allows all traffic that matches the ACL rule, or denies all traffic on the interface, while the ACL is being modified.

hardware access-list atomic-disable [**default-action permit**]

Syntax Description

default-action permit	Allows all traffic on the interface that matches the ACL rule, while the ACL is being modified.
<none>	Denies all traffic on the interface while the ACL is being modified.

Command Default

None

Command Modes

Privileged Executive mode

Command History

Release	Modification
Release 6.2.1	This command was introduced.

Usage Guidelines

When atomic ACL updates are disabled, the ACL is detached, and the ACL rules are not applied during the ACE modification process. Hence, it is recommended to configure to either permit or deny all traffic until the modification is complete.

For more information, see the Atomic ACL Updates By Using the Disable Option section in the *IP Addresses and Services Configuration Guide for Cisco NCS 5000 Series Routers*.

Example

To disable atomic updates on the hardware, by permitting packets that match the ACE rule, use the following configuration.

```
RP/0/RP0/CPU0:router# hardware access-list atomic-disable default-action permit
```

To disable atomic updates on the hardware, by denying all packets until the modification is complete, use the following configuration.

```
RP/0/RP0/CPU0:router# hardware access-list atomic-disable
```

clear access-list ipv4

To clear IPv4 access list counters, use the **clear access-list ipv4** command in XR EXEC mode.

clear access-list ipv4 *access-list name* [*sequence-number* | **ingress**] [**location** *node-id* | **sequence** *number*]

Syntax Description

access-list-name	Name of a particular IPv4 access list. The name cannot contain a spaces or quotation marks, but can include numbers.
sequence-number	(Optional) Specific sequence number with which counters are cleared for an access list. Range is 1 to 2147483644.
ingress	Specifies an inbound direction.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
location *node-id*	(Optional) Clears hardware resource counters from the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
sequence *number*	(Optional) Clears counters for an access list with a specific sequence number. Range is 1 to 2147483644.

Command Default

The default clears the specified IPv4 access list.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **clear access-list ipv4** command to clear counters for a specified configured access list. Use a sequence number to clear counters for an access list with a specific sequence number.

Use an asterisk (***)** in place of the *access-list-name* argument to clear all access lists.

Task ID

Task ID	Operations
basic-services	read, write
acl	read, write

Task ID	Operations
bgp	read, write, execute

Examples

In the following example, counters for an access list named *marketing* are cleared:

```
RP/0/RP0/CPU0:router# show access-lists ipv4 marketing

ipv4 access-list marketing
  10 permit ip 192.168.34.0 0.0.0.255
  20 permit ip 172.16.0.0 0.0.255.255
  30 deny tcp host 172.16.0.0 eq bgp host 192.168.202.203 30

RP/0/RP0/CPU0:router# clear access-list ipv4 marketing

RP/0/RP0/CPU0:router# show access-lists ipv4 marketing

ipv4 access-list marketing
  10 permit ip 192.168.34.0 0.0.0.255 any
  20 permit ip 172.16.0.0 0.0.255.255 any
  30 deny tcp host 172.16.0.0 eq bgp host 192.168.202.203 30
```

clear access-list ipv6

To clear IPv6 access list counters, use the **clear access-list ipv6** command in .

clear access-list ipv6 *access-list-name* [*sequence-number* | **ingress**] [**location** *node-id* | **sequence** *number*]

Syntax Description

access-list-name	Name of a particular IPv6 access list. The name cannot contain a spaces or quotation marks, but can include numbers.
sequence-number	(Optional) Specific sequence number for a particular access control entry (ACE) with which counters are cleared for an access list. Range is 1 to 2147483644.
ingress	(Optional) Specifies an inbound direction.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
instance *interface-path-id*	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
location *node-id*	(Optional) Clears counters for an access list enabled on a card interface. The *node-id* argument is entered in the rack/slot/module notation.
sequence *number*	(Optional) Specifies a specific sequence number that clears access list counters. Range is 1 to 2147483644.

Command Default

The default clears the specified IPv6 access list.

Command Modes

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

The **clear access-list ipv6** command is similar to the **clear access-list ipv4** command, except that it is IPv6-specific.

Use the **clear access-list ipv6** command to clear counters for a specified configured access list. Use a sequence number to clear counters for an access list with a specific sequence number

Use an asterisk **(*)** in place of the *access-list-name* argument to clear all access lists.

Task ID

Task ID	Operations
basic-services	read, write
acl	read, write
network	read, write

Examples

In the following example, counters for an access list named *marketing* are cleared:

```
RP/0/# show access-lists ipv6 marketing
ipv6 access-list marketing
  10 permit ipv6 3333:1:2:3::/64 any
  20 permit ipv6 4444:1:2:3::/64 any
  30 permit ipv6 5555:1:2:3::/64 any
RP/0/# clear access-list ipv6 marketing
RP/0/# show access-lists ipv6 marketing
ipv6 access-list marketing
  10 permit ipv6 3333:1:2:3::/64 any
  20 permit ipv6 4444:1:2:3::/64 any
  30 permit ipv6 5555:1:2:3::/64 any
```

copy access-list ipv4

To create a copy of an existing IPv4 access list, use the **copy access-list ipv4** command in XR EXEC mode.

copy access-list ipv4 *source-acl destination-acl*

Syntax Description

source-acl	Name of the access list to be copied.
destination-acl	Name of the destination access list where the contents of the *source-acl* argument is copied.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **copy access-list ipv4** command to copy a configured access list. Use the *source-acl* argument to specify the access list to be copied and the *destination-acl* argument to specify where to copy the contents of the source access list. The *destination-acl* argument must be a unique name; if the *destination-acl* argument name exists for an access list or prefix list, the access list is not copied. The **copy access-list ipv4** command checks that the source access list exists then checks the existing list names to prevent overwriting existing access lists or prefix lists.

Task ID

Task ID	Operations
acl	read, write
filesystem	execute

Examples

In the following example, a copy of access list list-1 is created:

```
RP/0/RP0/CPU0:router# show access-lists ipv4 list-1

ipv4 access-list list-1
  10 permit tcp any any log
  20 permit ip any any
RP/0/RP0/CPU0:router# copy access-list ipv4 list-1 list-2
RP/0/RP0/CPU0:router# show access-lists ipv4 list-2
ipv4 access-list list-2
  10 permit tcp any any log
  20 permit ip any any
```

In the following example, copying the access list list-1 to list-3 is denied because a list-3 access list already exists:

```
RP/0/RP0/CPU0:router# copy access-list ipv4 list-1 list-3

list-3 exists in access-list

RP/0/RP0/CPU0:router# show access-lists ipv4 list-3

ipv4 access-list list-3
  10 permit ip any any
  20 deny tcp any any log
```

copy access-list ipv6

To create a copy of an existing IPv6 access list, use the **copy access-list ipv6** command in .

copy access-list ipv6 *source-acl destination-acl*

Syntax Description

source-acl	Name of the access list to be copied.
destination-acl	Destination access list where the contents of the *source-acl* argument is copied.

Command Default

No default behavior or value

Command Modes

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

Use the **copy access-list ipv6** command to copy a configured access list. Use the *source-acl* argument to specify the access list to be copied and the *destination-acl* argument to specify where to copy the contents of the source access list. The *destination-acl* argument must be a unique name; if the *destination-acl* argument name exists for an access list or prefix list, the access list is not copied. The **copy access-list ipv6** command checks that the source access list exists then checks the existing list names to prevent overwriting existing access lists or prefix lists.

Task ID

Task ID	Operations
acl	read, write
filesystem	execute

Examples

In this example, a copy of access list list-1 is created:

```
RP/0/# show access-lists ipv6 list-1

ipv6 access-list list-1
  10 permit tcp any any log
  20 permit ipv6 any any

RP/0/# copy access-list ipv6 list-1 list-2

RP/0/# show access-lists ipv6 list-2

ipv6 access-list list-2
  10 permit tcp any any log
  20 permit ipv6 any any
```

In this example, copying access list list-1 to list-3 is denied because a list-3 access list already exists:

```
RP/0/# copy access-list ipv6 list-1 list-3

list-3 exists in access-list

RP/0/# show access-lists ipv6 list-3
ipv6 access-list list-3
  10 permit ipv6 any any
  20 deny tcp any any log
```

deny (IPv4)

To set conditions for an IPv4 access list, use the **deny** command in access list configuration mode. There are two versions of the **deny** command: **deny** (source), and **deny** (protocol). To remove a condition from an access list, use the **no** form of this command.

[*sequence-number*] **deny** *source* [*source-wildcard*] **counter** *counter-name* [**log** | **log-input**]
[*sequence-number*] **deny** *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**dscp** *dscp*] [**fragments**] [*packet-length operator packet-length value*] [**log** | **log-input**] [**ttl** *ttl value* [*value1....value2*]] [**counter** *counter-name*]
no *sequence-number*

Internet Control Message Protocol (ICMP)
[*sequence-number*] **deny icmp** *source source-wildcard destination destination-wildcard* [*icmp-type*] [*icmp-code*] [**precedence** *precedence*] [**dscp** *dscp*] [**fragments**] [**log** | **log-input**] [**counter** *counter-name*] [**icmp-off**]

Internet Group Management Protocol (IGMP)
[*sequence-number*] **deny igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**dscp** *value*] [**fragments**] [**log** | **log-input**] [**counter** *counter-name*]

User Datagram Protocol (UDP)
[*sequence-number*] **deny udp** *source source-wildcard* [*operator* { *port protocol-port* }] *destination destination-wildcard* [*operator* { *port protocol-port* }] [**precedence** *precedence*] [**dscp** *dscp*] [**fragments**] [**log** | **log-input**] [**counter** *counter-name*]

Syntax Description

sequence-number	(Optional) Number of the **deny** statement in the access list. This number determines the order of the statements in the access list. The number can be from 1 to 2147483644. (By default, the first statement is number 10, and the subsequent statements are incremented by 10.)
source	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part dotted-decimal format. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use the **host** *source* combination as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.

source-wildcard	Wildcard bits to be applied to the source. There are three alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use the **host** *source* combination as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
protocol	Name or number of an IP protocol. It can be one of the keywords , **esp** , **gre** , **icmp** , **igmp** , **igrp** , **ip** , **ipinip** , **nos** , **ospf** , **pim** , **pcp** , **tcp** , or **udp** , or an integer from 0 to 255 representing an IP protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the **ip** keyword. ICMP, and TCP allow further qualifiers, which are described later in this table.
destination	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part dotted-decimal format. • Use the **any** keyword as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use the **host** *destination* combination as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
destination-wildcard	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: • Use a 32-bit quantity in four-part dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use the **host** *destination* combination as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.

precedence *precedence*	(Optional) Packets can be filtered by precedence level (as specified by a number from 0 to 7) or by the following names: • **routine** —Match packets with routine precedence (0) • **priority** —Match packets with priority precedence (1) • **immediate** —Match packets with immediate precedence (2) • **flash** —Match packets with flash precedence (3) • **flash-override** —Match packets with flash override precedence (4) • **critical** —Match packets with critical precedence (5) • **internet** —Match packets with internetwork control precedence (6) • **network** —Match packets with network control precedence (7)

dscp *dscp*	(Optional) Differentiated services code point (DSCP) provides quality of service control. The values for *dscp* are as follows: • **0**–**63**–Differentiated services codepoint value • **af11**—Match packets with AF11 dscp (001010) • **af12**—Match packets with AF12 dscp (001100) • **af13**—Match packets with AF13 dscp (001110) • **af21**—Match packets with AF21 dscp (010010) • **af22**—Match packets with AF22 dscp (010100) • **af23**—Match packets with AF23 dscp (010110) • **af31**—Match packets with AF31 dscp (011010) • **af32**—Match packets with AF32 dscp (011100) • **af33**—Match packets with AF33 dscp (011110) • **af41**—Match packets with AF41 dscp (100010) • **af42**—Match packets with AF42 dscp (100100) • **af43**—Match packets with AF43 dscp (100110) • **cs1**—Match packets with CS1 (precedence 1) dscp (001000) • **cs2**—Match packets with CS2 (precedence 2) dscp (010000) • **cs3**—Match packets with CS3 (precedence 3) dscp (011000) • **cs4**—Match packets with CS4 (precedence 4) dscp (100000) • **cs5**—Match packets with CS5 (precedence 5) dscp (101000) • **cs6**—Match packets with CS6 (precedence 6) dscp (110000) • **cs7**—Match packets with CS7 (precedence 7) dscp (111000) • **default**—Default DSCP (000000) • **ef**—Match packets with EF dscp (101110)
fragments	(Optional) Causes the software to examine fragments of IPv4 packets when applying this access list entry. When this keyword is specified, fragments are subject to the access list entry.

log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the access list number, whether the packet was permitted or denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches a flow, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval.
log-input	(Optional) Provides the same function as the **log** keyword, except that the log-message also includes the input interface.
ttl value [*value1*. . *value2*[	(Optional) TTL value used for filtering. Range is 1 to 255. If only *value* is specified, the match is against this value. If both *value1* and *value2* are specified, the packet TTL is matched against the range of TTLs between *value1* and *value2* .
icmp-off	(Optional) Turns off ICMP generation for denied packets.
icmp-type	(Optional) ICMP message type for filtering ICMP packets. Range is from 0 to 255.
icmp-code	(Optional) ICMP message code for filtering ICMP packets. Range is from 0 to 255.
igmp-type	(Optional) IGMP message type (0 to 15) or message name for filtering IGMP packets, as follows: • dvmrp • host-query • host-report • mtrace • mtrace-response • pim • precedence • trace • v2-leave • v2-report • v3-report

operator	(Optional) Operator is used to compare source or destination ports. Possible operands are **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source* and *source-wildcard* values, it must match the source port. If the operator is positioned after the *destination* and *destination-wildcard* values, it must match the destination port. If the operator is positioned after the **ttl** keyword, it matches the TTL value. The **range** operator requires two port numbers. All other operators require one port number.
port	Decimal number of a TCP or UDP port. A port number is a number from 0 to 65535. TCP ports can be used only when filtering TCP. UDP ports can be used only when filtering UDP.
protocol-port	Name of a TCP or UDP port. TCP and UDP port names are listed in the "Usage Guidelines" section. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.
established	(Optional) For the TCP protocol only: Indicates an established connection.
match-any	(Optional) For the TCP protocol only: Filters on any combination of TCP flags.
match-all	(Optional) For the TCP protocol only: Filters on all TCP flags.
+ | -	(Required) For the TCP protocol **match-any** , **match-all** : Prefix *flag-name* with **+** or **-** . Use the + *flag-name* argument to match packets with the TCP flag set. Use the - *flag-name* argument to match packets when the TCP flag is not set.
flag-name	(Optional) For the TCP protocol **match-any** , **match-all** . Flag names are: **ack** , **fin** , **psh** , **rst** , **syn** , **urg**.
counter	(Optional) Enables accessing ACL counters using SNMP query.
counter-name	Defines an ACL counter name.

Command Default

There is no specific condition under which a packet is denied passing the IPv4 access list.

ICMP message generation is enabled by default.

Command Modes

IPv4 access list configuration

Command History

Release	Modification
Release 7.6.1	The **log-input** option was introduced.
Release 6.0	This command was introduced.

Usage Guidelines

Use the **deny** command following the **ipv4 access-list** command to specify conditions under which a packet cannot pass the access list.

By default, the first statement in an access list is number 10, and the subsequent statements are incremented by 10.

You can add **permit**, **deny**, or **remark** statements to an existing access list without retyping the entire list. To add a new statement anywhere other than at the end of the list, create a new statement with an appropriate entry number that falls between two existing entry numbers to indicate where it belongs.

The following is a list of precedence names:

- critical
- flash
- flash-override
- immediate
- internet
- network
- priority
- routine

The following is a list of ICMP message type names:

- administratively-prohibited
- alternate-address
- conversion-error
- dod-host-prohibited
- dod-net-prohibited
- echo
- echo-reply
- general-parameter-problem
- host-isolated
- host-precedence-unreachable
- host-redirect
- host-tos-redirect
- host-tos-unreachable
- host-unknown
- host-unreachable
- information-reply

- information-request
- mask-reply
- mask-request
- mobile-redirect
- net-redirect
- net-tos-redirect
- net-tos-unreachable
- net-unreachable
- network-unknown
- no-room-for-option
- option-missing
- packet-too-big
- parameter-problem
- port-unreachable
- precedence-unreachable
- protocol-unreachable
- reassembly-timeout
- redirect
- router-advertisement
- router-solicitation
- source-quench
- source-route-failed
- time-exceeded
- timestamp-reply
- timestamp-request
- traceroute
- ttl-exceeded
- unreachable

The following is a list of TCP port names that can be used instead of port numbers. Refer to the current *Assigned Numbers* RFC to find a reference to these protocols. You can find port numbers corresponding to these protocols by typing a ? in the place of a port number.

- bgp

- chargen
- cmd
- daytime
- discard
- domain
- echo
- exec
- finger
- ftp
- ftp-data
- gopher
- hostname
- ident
- irc
- klogin
- kshell
- login
- lpd
- nntp
- pim-auto-rp
- pop2
- pop3
- smtp
- sunrpc
- tacacs
- talk
- telnet
- time
- uucp
- whois
- www

The following UDP port names can be used instead of port numbers. Refer to the current *Assigned Numbers* RFC to find a reference to these protocols. You can find port numbers corresponding to these protocols by typing a ? in the place of a port number.

- biff
- bootpc
- bootps
- discard
- dnsix
- domain
- echo
- isakmp
- mobile-ip
- nameserver
- netbios-dgm
- netbios-ns
- netbios-ss
- ntp
- pim-auto-rp
- rip
- snmp
- snmptrap
- sunrpc
- syslog
- tacacs
- talk
- tftp
- time
- who
- xdmcp

Use the following flags in conjunction with the **match-any** and **match-all** keywords and the + and - signs to select the flags to display:

- ack
- fin

- psh
- rst
- syn

For example, **match-all** + *ack* + *syn* displays TCP packets with both the ack *and* syn flags set, or **match-any** + *ack* - *syn* displays the TCP packets with the ack set *or* the syn not set.



Note If any ACE in an ACL contains ABF clause, this ACL cannot be applied at any non-zero compression level.

Task ID

Task ID	Operations
ipv4	read, write
acl	read, write

Examples

This example shows how to set a deny condition for an access list named Internet filter:

```
Router(config)# ipv4 access-list Internetfilter
Router(config-ipv4-acl)# 10 deny 192.168.34.0 0.0.0.255
Router(config-ipv4-acl)# 20 deny 172.16.0.0 0.0.255.255
Router(config-ipv4-acl)# 25 deny tcp host 172.16.0.0 eq bgp host 192.168.202.203 range 1300
 1400
Router(config-ipv4-acl)# permit 10.0.0.0 0.255.255.255
```

deny (IPv6)

To set deny conditions for an IPv6 access list, use the **deny** command in IPv6 access list configuration mode. To remove the deny conditions, use the **no** form of this command.

no *sequence-number*

Internet Control Message Protocol (ICMP)

Transmission Control Protocol (TCP)

User Datagram Protocol (UDP)

Syntax Description

sequence-number	(Optional) Number of the **deny** statement in the access list. This number determines the order of the statements in the access list. Range is 1 to 2147483644. (By default, the first statement is number 10, and the subsequent statements are incremented by 10.)
protocol	Name or number of an Internet protocol. It can be one of the keywords **ahp** , **esp** , **gre**, **icmp** , **igmp**, **igrp**, **ipinip**, **ipv6** , **nos**, **ospf**, **pcp** , **tcp** , or **udp** , or an integer in the range from 0 to 255 representing an IPv6 protocol number.
source-ipv6-prefix / prefix-length	The source IPv6 network or class of networks about which to set deny conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
any	An abbreviation for the IPv6 prefix ::/0.
host *source-ipv6-address*	Source IPv6 host address about which to set deny conditions. This *source-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.
ipv6-wildcard-mask	IPv6 wildcard mask. The IPv6 wildcard mask can take any IPv6 address value which is used instead of prefix length.
operator {*port* | *protocol-port*}	(Optional) Operand that compares the source or destination ports of the specified protocol. Operands are **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source-ipv6-prefix / prefix-length* argument, it must match the source port. If the operator is positioned after the *destination-ipv6-prefix / prefix-length* argument, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number. The *port* argument is the decimal number of a TCP or UDP port. Range is 0 to 65535. The *protocol-port* argument is the name of a TCP or UDP port. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.

destination-ipv6-prefix / prefix-length	Destination IPv6 network or class of networks about which to set deny conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
host *destination-ipv6-address*	Destination IPv6 host address about which to set deny conditions. This *destination-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.
dscp *value*	(Optional) Matches a differentiated services code point DSCP value against the traffic class value in the Traffic Class field of each IPv6 packet header. Range is 0 to 63.
routing	(Optional) Matches source-routed packets against the routing extension header within each IPv6 packet header.
authen	(Optional) Matches if the IPv6 authentication header is present.
destopts	(Optional) Matches if the IPv6 destination options header is present.
fragments	(Optional) Matches noninitial fragmented packets where the fragment extension header contains a nonzero fragment offset. The **fragments** keyword is an option only if the *operator* [*port-number*] arguments are not specified.
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the access list name and sequence number, whether the packet was denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets denied in the prior 5-minute interval.
log-input	(Optional) Provides the same function as the **log** keyword, except that the log-message also includes the input interface.
ttl	(Optional) Turns on matching against time-to-life (TTL) value.
operator	(Optional) Operand that compares the source or destination ports of the specified protocol. Operands are **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range).
ttl value [*value1 ... value2*]	(Optional) TTL value used for filtering. Range is 1 to 255. If only *value* is specified, the match is against this value. If both *value1* and *value2* are specified, the packet TTL is matched against the range of TTLs between *value1* and *value2* .
icmp-off	(Optional) Turns off ICMP generation for denied packets.

icmp-type	(Optional) ICMP message type for filtering ICMP packets. ICMP packets can be filtered by ICMP message type. Range is 0 to 255.
icmp-code	(Optional) ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. Range is 0 to 255.
established	(Optional) For the TCP protocol only: Indicates an established connection.
match-any	(Optional) For the TCP protocol only: Filters on any combination of TCP flags.
match-all	(Optional) For the TCP protocol only: Filters on all TCP flags.
+ | -	(Required) For the TCP protocol **match-any** , **match-all** : Prefix *flag-name* with + or - . Use the + *flag-name* argument to match packets with the TCP flag set. Use the - *flag-name* argument to match packets when the TCP flag is not set.
flag-name	(Optional) For the TCP protocol **match-any** , **match-all** . Flag names are: **ack**, **fin**, **psh**, **rst**, **syn**, **urg**.

Command Default

No IPv6 access list is defined.

ICMP message generation is enabled by default.

Command Modes

IPv6 access list configuration

Command History

Release	Modification
Release 6.5.1	Added the hop-by-hop option.
Release 6.0.1	This command was introduced.

Usage Guidelines

The **deny** (IPv6) command is similar to the **deny** (IPv4) command, except that it is IPv6-specific.

Use the **deny** (IPv6) command following the **ipv6 access-list** command to define the conditions under which a packet passes the access list.



Note If any ACE in an ACL contains ABF clause, this ACL cannot be applied at any non-zero compression level.

Specifying **ipv6** for the *protocol* argument matches against the IPv6 header of the packet.

By default, the first statement in an access list is number 10, and the subsequent statements are numbered in increments of 10.

You can add permit, deny, or remark statements to an existing access list without retyping the entire list. To add a new statement anywhere other than at the end of the list, create a new statement with an appropriate entry number that falls between two existing entry numbers to indicate where it belongs.

Both the *source-ipv6-prefix/prefix-length* and *destination-ipv6-prefix/prefix-length* arguments are used for traffic filtering (the source prefix filters traffic based upon the traffic source; the destination prefix filters traffic based upon the traffic destination).



Note IPv6 prefix lists, not access lists, should be used for filtering routing protocol prefixes.

The **fragments** keyword is an option only if the *operator* [*port* | *protocol-port*] arguments are not specified.

Task ID

Task ID	Operations
acl	read, write

Examples

The following example shows how to configure the IPv6 access list named toCISCO and apply the access list to the traffic entering the HundredGigE interface 0/2/0/2. Specifically, the deny entry in the list keeps all packets that have a destination TCP port number greater than 5000 from entering the HundredGigE interface 0/2/0/2. The permit entry in the list permits all ICMP packets to enter the HundredGigE interface 0/2/0/2.

```
Router(config)# ipv6 access-list toCISCO
Router(config-ipv6-acl)# deny tcp any any gt 5000
Router(config-ipv6-acl)# permit icmp any any
Router(config)#  interface HundredGigE 0/2/0/2
Router(config-if)# ipv6 access-group tOCISCO ingress
```

interface ipv4/ipv6 access-group

To configure an interface to accept multiple IPv4 or IPv6 ACLs, use the **interface ipv4/ipv6 access-group** command in XR Config mode.

interface *type interface-path-id* [**ipv4 | ipv6**] **access-group common** *acl-c1* **common** *acl-c2 acl-i2 acl-i4 acl-i5* **ingress**

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface -path-id	Physical interface or virtual interface. Use the **show interfaces** command to see a list of all interfaces currently configured on the router.
common *acl-c1* **common** *acl-c2*	Common ACLs, each preceded by the keyword **common**. Common ACLs are only supported in the ingress direction.
acl-i2 acl-i4 acl-i5	Interface ACLs.
ingress	Specifies an inbound direction.

Command Default

The interface does not have an IPv4/IPv6 access list applied to it.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

Use the **interface ipv4/ipv6 access-group** command to configure an interface on Cisco ASR 9000 High Density 100GE Ethernet line cards (such as A9K-8x100G-LB-SE and A9K-8x100G-LB-TR) to accept up to five IPv4 and/or IPv6 ACLs in the ingress direction only. There can be any combination of common and/or interface ACLs up to a total of five ACLs.

Task ID

Task ID	Operation
acl	read, write
network	read, write
config-services	read, write

The following example shows how to apply filters on packets inbound from GigabitEthernet interface 0/1/0/0:

```
Router#  interface GigabitEthernet 0/1/0/0
```

```
ipv4 access-group common acl_c1 common acl_c2 acl_i2 acl_i4 acl_i5 ingress
```

The following example shows a sample configuration of multiple ACLs:

```
Router#  show running-config interface tenGigE 0/1/0/0/0 interface TenGigE0/1/0/0/0
 ipv4 address 10.1.1.2 255.255.255.0
 ipv6 address 2001::33/64
 ipv4 access-group common acl_c1 common acl_c2 acl_i2 acl_i4 acl_i5 ingress
!
```

ipv4 access-group

To control access to an interface, use the **ipv4 access-group** command in interface configuration mode. To remove the specified access group, use the **no** form of this command.

ipv4 access-group *access-list-name* **ingress**

Syntax Description

access-list-name	Name of an IPv4 access list as specified by an **ipv4 access-list** command.
ingress	Filters on inbound packets.

Command Default

The interface does not have an IPv4 access list applied to it.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0	This command was introduced.
Release 7.2.1	Support to configure multiple ACLs was added.

Usage Guidelines

Filtering of MPLS packets through interface ACL is not supported.

If the access list permits the addresses, the software continues to process the packet. If the access list denies the address, the software discards the packet and returns an Internet Control Message Protocol (ICMP) host unreachable message.

If the specified access list does not exist, all packets are passed.

Task ID

Task ID	Operations
acl	read, write
network	read, write

Examples

The following example shows how to apply filters on packets from tenGigE interface 0/0/0/2:

```
Router(config)# interface tenGigE 0/0/0/2
Router(config-if)# ipv4 access-group p-ingress-filter ingress
```

ipv6 access-group

To control access to an interface, use the **ipv6 access-group** command in interface configuration mode. To remove the specified access group, use the **no** form of this command.

ipv6 access-group *access-list-name* **ingress**

Syntax Description

access-list-name	Name of an IPv4 access list as specified by an **ipv4 access-list** command.
ingress	Filters on inbound packets.

Command Default

The interface does not have an IPv6 access list applied to it.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

Filtering of MPLS packets through interface ACL is not supported.

If the access list permits the addresses, the software continues to process the packet. If the access list denies the address, the software discards the packet and returns an Internet Control Message Protocol (ICMP) host unreachable message.

If the specified access list does not exist, all packets are passed.

Task ID

Task ID	Operations
acl	read, write
ipv6	read, write

Examples

The following example shows how to apply filters on packets from tenGigE interface 0/0/0/2:

```
Router(config)# interface tenGigE 0/0/0/2
Router(config-if)# ipv6 access-group p-ingress-filter ingress
```

ipv4 access-list

To define an IPv4 access list by name, use the **ipv4 access-list** command in XR Config mode. To remove all entries in an IPv4 access list, use the **no** form of this command.

ipv4 access-list [*name* | **icmp-off**]
no ipv4 access-list [*name* | **icmp-off**]

Syntax Description

name	Name of the access list. Names cannot contain a space or quotation marks.

Command Default

No IPv4 access list is defined.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **ipv4 access-list** command to configure an IPv4 access list. This command places the router in access list configuration mode, in which the denied or permitted access conditions must be defined with the **deny** or **permit** command.

Use the **ipv4 access-group** command to apply the access list to an interface.

Task ID

Task ID	Operations
acl	read, write

Examples

This example shows how to define a standard access list named Internetfilter and disable ICMP Unreachable messages at global configuration:

```
Router(config)# ipv4 access-list Internetfilter
Router(config-ipv4-acl)# 10 permit 192.168.34.0 0.0.0.255
Router(config-ipv4-acl)# 20 permit 172.16.0.0 0.0.255.255
Router(config-ipv4-acl)# 30 permit 10.0.0.0 0.255.255.255
Router(config-ipv4-acl)# 39 remark Block BGP traffic from 172.16 net.
Router(config-ipv4-acl)# 40 deny tcp host 172.16.0.0 eq bgp host 192.168.202.203 range 1300
 1400

Router(config)# ipv4 access-list icmp-off
```

ipv6 access-list

To define an IPv6 access list and to place the router in IPv6 access list configuration mode, use the **ipv6 access-list** command in interface configuration mode. To remove the access list, use the **no** form of this command.

ipv6 access-list [*name* | **icmp-off**]
no ipv6 access-list [*name* | **icmp-off**]

Syntax Description

name Name of the IPv6 access list. Names cannot contain a space or quotation mark, or begin with a numeric.

Command Default

No IPv6 access list is defined.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

The **ipv6 access-list** command is similar to the **ipv4 access-list** command, except that it is IPv6-specific.

The IPv6 access lists are used for traffic filtering based on source and destination addresses, IPv6 option headers, and optional, upper-layer protocol type information for finer granularity of control. IPv6 access lists are defined by using the **ipv6 access-list** command in mode and their permit and deny conditions are set by using the **deny** and **permit** commands in IPv6 access list configuration mode. Configuring the **ipv6 access-list** command places the router in IPv6 access list configuration mode—the router prompt changes to router (config-ipv6-acl)#. From IPv6 access list configuration mode, permit and deny conditions can be set for the defined IPv6 access list.

See the “Examples” section for an example of a translated IPv6 access control list (ACL) configuration.



Note No more than one IPv6 access list can be applied to an interface per direction.



Note Every IPv6 access list has an implicit **deny ipv6 any any** statement as its last match condition. An IPv6 access list must contain at least one entry for the implicit **deny ipv6 any any** statement to take effect.



Note IPv6 prefix lists, not access lists, should be used for filtering routing protocol prefixes.

Use the **ipv6 access-group** interface configuration command with the *access-list-name* argument to apply an IPv6 access list to an IPv6 interface.

Note An IPv6 access list applied to an interface with the **ipv6 access-group** command filters traffic that is forwarded, not originated, by the router.

Note Every IPv6 ACL has implicit **permit icmp any any nd-na**, **permit icmp any any nd-ns**, and **deny ipv6 any any** statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.) An IPv6 ACL must contain at least one entry for the implicit **deny ipv6 any any** statement to take effect.**permit icmp any any nd-na permit icmp any any nd-ns deny ipv6 any any deny ipv6 any any**.

The IPv6 neighbor discovery process makes use of the IPv6 network layer service; therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, makes use of a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Task ID

Task ID	Operations
acl	read, write
ipv6	read, write

Examples

This example shows how to configure the IPv6 access list named list2 and applies the ACL to traffic on interface HundredGigE 0/2/0/2. Specifically, the first ACL entry keeps all packets from the network fec0:0:0:2::/64 (packets that have the site-local prefix fec0:0:0:2 as the first 64 bits of their source IPv6 address) from exiting out of interface HundredGigE 0/2/0/2. The second entry in the ACL permits all other traffic to exit out of interface HundredGigE 0/2/0/2. The second entry is necessary because an implicit deny all condition is at the end of each IPv6 ACL.

```
Router(config)# ipv6 access-list list2
Router(config-ipv6-acl)# 10 deny fec0:0:0:2::/64 any
Router(config-ipv6-acl)# 20 permit any any

Router# show ipv6 access-lists list2

ipv6 access-list list2
  10 deny ipv6 fec0:0:0:2::/64 any
  20 permit ipv6 any any

Router(config)# interface HundredGigE 0/2/0/2
```

Note IPv6 is automatically configured as the protocol type in **permit any any** and **deny any any** statements that are translated from mode to IPv6 access list configuration mode.



Note An IPv6 router does not forward to another network an IPv6 packet that has a link-local address as either its source or destination address (and the source interface for the packet is different from the destination interface for the packet).

This example shows how to disable ICMP Unreachable messages at global configuration:

```
Router(config)# ipv6 access-list icmp-off
```

ipv4 access-list log-update rate

To specify the rate at which IPv4 access lists are logged, use the **ipv4 access-list log-update rate** command in XR Config mode. To return the update rate to the default setting, use the **no** form of this command.

ipv4 access-list log-update rate *rate-number*
no ipv4 access-list log-update rate *rate-number*

Syntax Description

rate-number	Rate at which IPv4 access hit logs are generated per second on the router. Range is 1 to 1000.

Command Default

Default is 1.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The *rate-number* argument applies to all the IPv4 access-lists configured on the interfaces. That is, at any given time there can be between 1 and 1000 log entries for the system.

Task ID

Task ID	Operations
ipv4	read, write
acl	read, write

Examples

The following example shows how to configure a IPv4 access hit logging rate for the system:

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list log-update rate 10
```

ipv6 access-list log-update rate

To specify the rate at which IPv6 access lists are logged, use the **ipv6 access-list log-update rate** command in . To return the update rate to the default setting, use the **no** form of this command.

ipv6 access-list log-update rate *rate-number*
no ipv6 access-list log-update rate *rate-number*

Syntax Description

rate-number	Rate at which IPv6 access hit logs are generated per second on the router. Range is 1 to 1000.

Command Default

Default is 1.

Command Modes

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

The *rate-number* argument applies to all the IPv6 access-lists configured on the interfaces. That is, at any given time there can be between 1 and 1000 log entries for the system.

Task ID

Task ID	Operations
ipv6	read, write
acl	read, write

Examples

This example shows how to configure a IPv6 access hit logging rate for the system:

```
RP/0/(config)# ipv6 access-list log-update rate 10
```

ipv4 access-list log-update threshold

To specify the number of updates that are logged for IPv4 access lists, use the **ipv4 access-list log-update threshold** command in XR Config mode. To return the number of logged updates to the default setting, use the **no** form of this command.

ipv4 access-list log-update threshold *update-number*
no ipv4 access-list log-update threshold *update-number*

Syntax Description

update-number	Number of updates that are logged for every IPv4 access list configured on the router. Range is 0 to 2147483647.

Command Default

For IPv4 access lists, 2147483647 updates are logged.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

IPv4 access list updates are logged at 5-minute intervals, following the first logged update. Configuring a lower number of updates (a number lower than the default) is useful when more frequent update logging is desired.

Task ID

Task ID	Operations
basic-services	read, write
acl	read, write

Examples

This example shows how to configure a log threshold of ten updates for every IPv4 access list configured on the router:

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list log-update threshold 10
```

ipv6 access-list log-update threshold

To specify the number of updates that are logged for IPv6 access lists (ACLs), use the **ipv6 access-list log-update threshold** command in . To return the number of logged updates to the default setting, use the **no** form of this command.

ipv6 access-list log-update threshold *update-number*
no ipv6 access-list log-update threshold *update-number*

Syntax Description

update-number	Number of updates that are logged for every IPv6 access list configured on the router. Range is 0 to 2147483647.

Command Default

For IPv6 access lists, 350000 updates are logged.

Command Modes

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

The **ipv6 access-list log-update threshold** command is similar to the **ipv4 access-list log-update threshold** command, except that it is IPv6-specific.

IPv6 access list updates are logged at 5-minute intervals, following the first logged update. Configuring a lower number of updates (a number lower than the default) is useful when more frequent update logging is desired.

Task ID

Task ID	Operations
acl	read, write
ipv6	read, write

Examples

This example shows how to configure a log threshold of ten updates for every IPv6 access list configured on the router:

```
RP/0/(config)# ipv6 access-list log-update threshold 10
```

ipv6 access-list maximum ace threshold

To set the maximum number of access control entries (ACEs) for IPv6 access lists, use the **ipv6 access-list maximum ace threshold** command in . To reset the ACE limit for IPv6 access lists, use the **no** form of this command.

ipv6 access-list maximum ace threshold *ace-number*
no ipv6 access-list maximum ace threshold *ace-number*

Syntax Description

ace-number	Maximum number of configurable ACEs allowed. Range is 50000 to 350000.

Command Default

50,000 ACEs are allowed for IPv6 access lists.

Command Modes

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **ipv6 access-list maximum ace threshold** command to set the maximum number of configurable ACEs for IPv6 access lists. Out of resource (OOR) limits the number of ACEs that can be configured in the system. When the maximum number of configurable ACEs is reached, configuration of new ACEs is rejected.

Task ID

Task ID	Operations
acl	read, write
ipv6	read, write

Examples

This example shows how to set the maximum number of ACEs for IPv6 access lists to 75000:

```
Router(config)# ipv6 access-list maximum ace threshold 75000
```

object-group network

To configure a network object group, and to enter the network object group configuration mode, use the **object-group network** command in the global configuration mode. To de-configure the network object group, use the **no** form of this command.

object-group network { **ipv4 | ipv6** } *object-group-name*
no object-group network { **ipv4 | ipv6** } *object-group-name*

Syntax Description

ipv4	Configures the operation state of an IPV4 network object group.
ipv6	Configures the operation state of an IPV6 network object group.
object-group-name	Name of the object-group.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

Inherited object-groups up to four levels are supported in this release.

If an ACL is applied on an interface with non-zero compression level (implying it contains no ABF ACEs), a user cannot add an ACE with object-group.

Task ID

Task ID	Operation
system	read, write

Example

This example shows how to configure a network object-group, and to enter the network object-group configuration mode:

```
Router# configure
Router(config)# object-group network ipv4 ipv4_type5_obj1
Router(config-object-group-ipv4)#
```

Related Commands

Command	Description
show object-group port , on page 90	Displays the operation state of a network object group.

object-group port

To configure a port object group, and to enter the port object group configuration mode, use the **object-group port** command in the global configuration mode. To de-configure the port object group, use the **no** form of this command.

object-group port *object-group-name*
no object-group port *object-group-name*

Syntax Description

object-group-name	Name of the object-group.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

Inherited object-groups upto four levels are supported.

Note If any ACE in an ACL contains ABF clause, this ACL cannot be applied at any non-zero compression level.

Task ID

Task ID	Operation
system	read, write

Example

This example show how to configure a port object-group, and to enter the port object-group configuration mode:

```
Router# configure
Router(config)# object-group port ipv4_type5_obj1
Router(config-object-group-port)#
```

Related Commands

Command	Description
show object-group port , on page 90	Displays the operation state of a port object group.

permit (IPv4)

To set conditions for an IPv4 access list, use the **permit** command in access list configuration mode. There are two versions of the **permit** command: **permit** (source), and **permit** (protocol). To remove a condition from an access list, use the **no** form of this command.

[*sequence-number*] **permit** *source* [*source-wildcard*] [**log** | **log-input**]
[*sequence-number*] **permit** *protocol net-group source-net-object-group-name destination source-port-object-group-name* **net-group** *destination-net-object-group-name* **port-group** *destination-port-object-group-name* [**capture**] [**precedence** *precedence*]] [**dscp** *dscp* **bitmask** *value*] [**fragments**] [**log** | **log-input**] [**ttl** *ttl value* [*value1* . . . *value2*]] [**counter** *counter-name*]
no *sequence-number*

Internet Control Message Protocol (ICMP)
[*sequence-number*] **permit icmp** *source source-wildcard destination destination-wildcard* [*icmp-type*] [*icmp-code*] [**precedence** *precedence*] [**dscp** *dscp*] [**fragments**] [**log** | **log-input**][**counter** *counter-name*]

Internet Group Management Protocol (IGMP)
[*sequence-number*] **permit igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**dscp** *value*] [**fragments**] [**log** | **log-input**][**counter** *counter-name*]

User Datagram Protocol (UDP)
[*sequence-number*] **permit udp** *source source-wildcard* [*operator* {*portprotocol-port*}] *destination destination-wildcard* [*operator* {*portprotocol-port*}] [**precedence** *precedence*] [**dscp** *dscp*] [**fragments**] [**log** | **log-input**][**counter** *counter-name*]

Syntax Description

sequence-number	(Optional) Number of the **permit** statement in the access list. This number determines the order of the statements in the access list. Range is 1 to 2147483644. (By default, the first statement is number 10, and the subsequent statements are incremented by 10.)

source	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part dotted-decimal format. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use the **host** *source* combination as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
source-wildcard	Wildcard bits to be applied to the source. There are three alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use the **host** *source* combination as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
protocol	Name or number of an IP protocol. It can be one of the keywords , **esp** , , **icmp** , **igmp** , **igrp** , **ip** , **ipinip** , **nos** , **ospf** , **pim** , **pcp** , **sctp** , **tcp** , or **udp** , or an integer from 0 to 255 representing an IP protocol number. To match any Internet protocol (including ICMP, SCTP TCP, and UDP), use the **ip** keyword. ICMP, and TCP allow further qualifiers, which are described later in this table.

destination	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part dotted-decimal format. • Use the **any** keyword as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use the **host** *destination* combination as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
destination-wildcard	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: • Use a 32-bit quantity in four-part dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use the **host** *destination* combination as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.

precedence *precedence*	(Optional) Packets can be filtered by precedence level (as specified by a number from 0 to 7) or by the following names: • **Routine** —Match packets with routine precedence (0) • **priority** —Match packets with priority precedence (1) • **immediate** —Match packets with immediate precedence (2) • **flash** —Match packets with flash precedence (3) • **flash-override** —Match packets with flash override precedence (4) • **critical** —Match packets with critical precedence (5) • **internet** —Match packets with internetwork control precedence (6) • **network** —Match packets with network control precedence (7)
capture	Captures matching traffic. When the acl command is configured on the source mirroring port, if the ACL configuration command does not use the **capture** keyword, no traffic gets mirrored. If the ACL configuration uses the **capture** keyword, but the acl command is not configured on the source port, then the whole port traffic is mirrored and the **capture** action does not have any affect.

dscp *dscp*

(Optional) Differentiated services code point (DSCP) provides quality of service control. The values for *dscp* are as follows:

- 0–63—Differentiated services codepoint value
- af11—Match packets with AF11 dscp (001010)
- af12—Match packets with AF12 dscp (001100)
- af13—Match packets with AF13 dscp (001110)
- af21—Match packets with AF21 dscp (010010)
- af22—Match packets with AF22 dscp (010100)
- af23—Match packets with AF23 dscp (010110)
- af31—Match packets with AF31 dscp (011010)
- af32—Match packets with AF32 dscp (011100)
- af33—Match packets with AF33 dscp (011110)
- af41—Match packets with AF41 dscp (100010)
- af42—Match packets with AF42 dscp (100100)
- af43–Match packets with AF43 dscp (100110)
- cs1—Match packets with CS1 (precedence 1) dscp (001000)
- cs2—Match packets with CS2 (precedence 2) dscp (010000)
- cs3—Match packets with CS3 (precedence 3) dscp (011000)
- cs4—Match packets with CS4 (precedence 4) dscp (100000)
- cs5—Match packets with CS5 (precedence 5) dscp (101000)

- cs6—Match packets with CS6 (precedence 6) dscp (110000)
- cs7—Match packets with CS7 (precedence 7) dscp (111000)
- default—Default DSCP (000000)
- ef—Match packets with EF dscp (101110)

dscp range *dscp dscp*

(Optional) Differentiated services code point (DSCP) provides quality of service control. The values for *dscp* are as follows:

- 0–63—Differentiated services codepoint value
- af11—Match packets with AF11 dscp (001010)
- af12—Match packets with AF12 dscp (001100)
- af13—Match packets with AF13 dscp (001110)
- af21—Match packets with AF21 dscp (010010)
- af22—Match packets with AF22 dscp (010100)
- af23—Match packets with AF23 dscp (010110)
- af31—Match packets with AF31 dscp (011010)
- af32—Match packets with AF32 dscp (011100)
- af33—Match packets with AF33 dscp (011110)
- af41—Match packets with AF41 dscp (100010)
- af42—Match packets with AF42 dscp (100100)
- af43–Match packets with AF43 dscp (100110)
- cs1—Match packets with CS1 (precedence 1) dscp (001000)
- cs2—Match packets with CS2 (precedence 2) dscp (010000)
- cs3—Match packets with CS3 (precedence 3) dscp (011000)
- cs4—Match packets with CS4 (precedence 4) dscp (100000)
- cs5—Match packets with CS5 (precedence 5) dscp (101000)

	• cs6—Match packets with CS6 (precedence 6) dscp (110000) • cs7—Match packets with CS7 (precedence 7) dscp (111000) • default—Default DSCP (000000) • ef—Match packets with EF dscp (101110)
fragments	(Optional) Causes the software to examine noninitial fragments of IPv4 packets when applying this access list entry. When this keyword is specified, fragments are subject to the access list entry.
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the access list number, whether the packet was permitted or denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches a flow, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval.
log-input	(Optional) Provides the same function as the **log** keyword, except that the log-message also includes the input interface.
ttl	(Optional) Turns on matching against time-to-life (TTL) value.

ttl value [*value1 ... value2*]	(Optional) TTL value used for filtering. Range is 1 to 255. If only *value* is specified, the match is against this value. If both *value1* and *value2* are specified, the packet TTL is matched against the range of TTLs between *value1* and *value2* .
icmp-type	(Optional) ICMP message type for filtering ICMP packets. Range is from 0 to 255.
icmp-code	(Optional) ICMP message code for filtering ICMP packets. Range is from 0 to 255.
igmp-type	(Optional) IGMP message type (0 to 15) or message name for filtering IGMP packets, as follows: • dvmrp • host-query • host-report • mtrace • mtrace-response • pim • precedence • trace • v2-leave • v2-report • v3-report

operator	(Optional) Operator is used to compare source or destination ports. Possible operands are **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source* and *source-wildcard* values, it must match the source port. If the operator is positioned after the *destination* and *destination-wildcard* values, it must match the destination port. If the operator is positioned after the **ttl** keyword, it matches the TTL value. The **range** operator requires two port numbers. All other operators require one port number.
port	Decimal number a TCP or UDP port. Range is 0 to 65535. TCP ports can be used only when filtering TCP. UDP ports can be used only when filtering UDP.
protocol-port	Name of a TCP or UDP port. TCP and UDP port names are listed in the "Usage Guidelines" section. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.
established	(Optional) For the TCP protocol only: Indicates an established connection.
match-any	(Optional) For the TCP protocol only: Filters on any combination of TCP flags.
match-all	(Optional) For the TCP protocol only: Filters on all TCP flags.

+ | -	(Required) For the TCP protocol **match-any** , **match-all** : Prefix *flag-name* with + or - . Use the + *flag-name* argument to match packets with the TCP flag set. Use the - *flag-name* argument to match packets when the TCP flag is not set.
flag-name	(Optional) For the TCP protocol **match-any** , **match-all** . Flag names are: **ack** , **fin** , **psh** , **rst** , **syn** , **urg** .
counter	(Optional) Enables accessing ACL counters using SNMP query.
counter-name	Defines an ACL counter name.

Command Default

There is no specific condition under which a packet is denied passing the IPv4 access list.

ICMP message generation is enabled by default.

Command Modes

IPv4 access list configuration

Command History

Release	Modification
Release 7.5.4	**bitmask** keyword was introduced.
Release 6.0	This command was introduced.

Usage Guidelines

Use the **permit** command following the **ipv4 access-list** command to specify conditions under which a packet can pass the access list.

By default, the first statement in an access list is number 10, and the subsequent statements are incremented by 10.

You can add **permit**, **deny**, or **remark** statements to an existing access list without retyping the entire list. To add a new **s**tatement anywhere other than at the end of the list, create a new statement with an appropriate entry number that falls between two existing entry numbers to indicate where it belongs.



Note If any ACE in an ACL contains ABF clause, this ACL cannot be applied at any non-zero compression level.

The following is a list of precedence names:

- critical
- flash
- flash-override

- immediate
- internet
- network
- priority
- routine

The following is a list of ICMP message type names:

- administratively-prohibited
- alternate-address
- conversion-error
- dod-host-prohibited
- dod-net-prohibited
- echo
- echo-reply
- general-parameter-problem
- host-isolated
- host-precedence-unreachable
- host-redirect
- host-tos-redirect
- host-tos-unreachable
- host-unknown
- host-unreachable
- information-reply
- information-request
- mask-reply
- mask-request
- mobile-redirect
- net-redirect
- net-tos-redirect
- net-tos-unreachable
- net-unreachable
- network-unknown
- no-room-for-option

- option-missing
- packet-too-big
- parameter-problem
- port-unreachable
- precedence-unreachable
- protocol-unreachable
- reassembly-timeout
- redirect
- router-advertisement
- router-solicitation
- source-quench
- source-route-failed
- time-exceeded
- timestamp-reply
- timestamp-request
- traceroute
- ttl-exceeded
- unreachable

The following is a list of TCP port names that can be used instead of port numbers. Refer to the current *Assigned Numbers* RFC to find a reference to these protocols. You can find port numbers corresponding to these protocols by typing a ? in the place of a port number.

- bgp
- chargen
- cmd
- daytime
- discard
- domain
- echo
- exec
- finger
- ftp
- ftp-data

- gopher
- hostname
- ident
- irc
- klogin
- kshell
- login
- lpd
- nntp
- pim-auto-rp
- pop2
- pop3
- smtp
- sunrpc
- tacacs
- talk
- telnet
- time
- uucp
- whois
- www

The following UDP port names can be used instead of port numbers. Refer to the current *Assigned Numbers* RFC to find a reference to these protocols. You can find port numbers corresponding to these protocols by typing a ? in the place of a port number.

- biff
- bootpc
- bootps
- discard
- dnsix
- domain
- echo
- isakmp

- mobile-ip
- nameserver
- netbios-dgm
- netbios-ns
- netbios-ss
- ntp
- pim-auto-rp
- rip
- snmp
- snmptrap
- sunrpc
- syslog
- tacacs
- talk
- tftp
- time
- who
- xdmcp

Use the following flags in conjunction with the **match-any** and **match-all** keywords and the + and - signs to select the flags to display:

- ack
- fin
- psh
- rst
- syn

For example, **match-all** +*ack* +*syn* displays TCP packets with both the ack *and* syn flags set, or **match-any** +*ack* – - *syn* displays the TCP packets with the ack set *or* the syn not set.

Task ID

Task ID	Operations
ipv4	read, write
acl	read, write

Examples

The following example shows how to set a permit condition for an access list named Internetfilter:

```
Router(config)# ipv4 access-list Internetfilter
Router(config-ipv4-acl)# 10 permit 192.168.34.0 0.0.0.255
Router(config-ipv4-acl)# 20 permit 172.16.0.0 0.0.255.255
Router(config-ipv4-acl)# 25 permit tcp host 172.16.0.0 eq bgp host 192.168.202.203 range
1300 1400
Router(config-ipv4-acl)# deny 10.0.0.0 0.255.255.255
```

This example shows how you can configure DSCP bitmask on ingress ERSPAN.

```
Router# config
Router(config)# ipv4 access-list acl1
Router(config-ipv4-acl)# 10 permit ipv4 host 192.0.2.1 any dscp af22 bitmask 0x3f
Router(config-ipv4-acl)# commit
Router(config-ipv4-acl)# exit
Router(config)# interface HundredGigE0/0/0/6
Router(config-if)# ipv4 address 192.0.2.51 255.255.255.0
Router(config-if)# monitor-session TEST ethernet direction rx-only port-level acl ipv4 acl1
Router(config-if)# commit
```

permit (IPv6)

To set permit conditions for an IPv6 access list, use the **permit** command in IPv6 access list configuration mode. To remove the permit conditions, use the **no** form of this command.

[sequence-number] **permit** *source* { *source-ipv6-prefix/ prefix-length* | *any* | *host source-ipv6-address ipv6-wildcard-mask/prefix-length* } [*operator* { *port* | *protocol-port* }] `capture`] [**dscp** *value*] [**routing**] [**hop-by-hop**] [**authen**] [**destopts**] [**fragments**] [*packet-length operator packet-length value*] [**log** | **log-input**] [**ttl** *operator ttl value*]
counter *counter-name*
[sequence-number] **permit** *protocol* { *source-ipv6-prefix/ prefix-length* | *any* | *host source-ipv6-address ipv6-wildcard-mask/prefix-length* } { *source-ipv6-prefix/ prefix-length* | *any* | *host source-ipv6-address* } [*operator* { *port* | *protocol-port* } `capture`] [**dscp** *value* [**bitmask** *value*] [**routing**] [**hop-by-hop**] [**authen**] [**destopts**] [**fragments**] [*packet-length operator packet-length value*] [**log** | **log-input**] [**ttl** *operator ttl value*]
counter *counter-name*
no *sequence-number*

Internet Control Message Protocol (ICMP)
[sequence-number] **permit icmp** { *source-ipv6-prefix/ prefix-length* | *any* | *host source-ipv6-address ipv6-wildcard-mask/prefix-length* } { *source-ipv6-prefix/ prefix-length* | *any* | *host source-ipv6-address* } { *destination-ipv6-prefix/ prefix-length* | *any* | *host destination-ipv6-address ipv6-wildcard-mask/prefix-length* } [*icmp-type*] [*icmp-code*] [**dscp** *value*] [**routing**] [**hop-by-hop**] [**authen**] [**destopts**] [**fragments**] [**log** | **log-input**] [**counter** *counter-name*]

Transmission Control Protocol (TCP)
[sequence-number] **permit tcp** { *source-ipv6-prefix/ prefix-length* | *any* | *host source-ipv6-address ipv6-wildcard-mask/prefix-length* } [*operator* { *port* | *protocol-port* }] { *destination-ipv6-prefix/ prefix-length* | *any* | *host destination-ipv6-address ipv6-wildcard-mask/prefix-length* } [*operator* { *port* | *protocol* | *port* }] [**dscp** *value*] [**routing**] [**hop-by-hop**] [**authen**] [**destopts**] [**fragments**] [**established**] { **match-any | match-all | + | -** } [*flag-name*] [**log** | **log-input**] [**counter** *counter-name*]

User Datagram Protocol (UDP)
[sequence-number] **permit tcp** { *source-ipv6-prefix/ prefix-length* | *any* | *host source-ipv6-address ipv6-wildcard-mask/prefix-length* } [*operator* { *port* | *protocol-port* }] { *destination-ipv6-prefix/ prefix-length* | *any* | *host destination-ipv6-address ipv6-wildcard-mask/prefix-length* } [*operator* { *port* | *protocol* | *port* }] [**dscp** *value*] [**routing**] [**hop-by-hop**] [**authen**] [**destopts**] [**fragments**] [**established**] [*flag-name*] [**log** | **log-input**] [**counter** *counter-name*]

Syntax Description

sequence-number	(Optional) Number of the **permit** statement in the access list. This number determines the order of the statements in the access list. Range is from 1 to 2147483644. (By default, the first statement is number 10, and the subsequent statements are incremented by 10.)

protocol	Name or number of an Internet protocol. It can be one of the keywords **ahp**, **esp**, , **icmp**, **igmp**, **igrp**, **isinip**, **ipv6**, **nos**, **ospf**, **pcp**, **sctp**, **tcp**, or **udp**, or an integer that ranges from 0 to 255, representing an IPv6 protocol number.
source-ipv6-prefix / *prefix-length*	Source IPv6 network or class of networks about which permit conditions are to be set. This argument must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.
any	An abbreviation for the IPv6 prefix ::/0.
capture	Captures matching traffic. When the acl command is configured on the source mirroring port, if the ACL configuration command does not use the **capture** keyword, no traffic gets mirrored. If the ACL configuration uses the **capture** keyword, but the acl command is not configured on the source port, then the whole port traffic is mirrored and the **capture** action does not have any effect.
host *source-ipv6-address*	Source IPv6 host address about which to set permit conditions. This *source-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.
ipv6-wildcard-mask	IPv6 wildcard mask. The IPv6 wildcard mask can take any IPv6 address value which is used instead of prefix length.
vrf *vrf-name*	Specifies VPN routing and forwarding (VRF) instance.

operator {*port* | *protocol-port*}	(Optional) Operand that compares the source or destination ports of the specified protocol. Operands are **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source-ipv6-prefix / prefix-length* argument, it must match the source port. If the operator is positioned after the *destination-ipv6-prefix / prefix-length* argument, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number. The *port* argument is the decimal number of a TCP or UDP port. A port number is a number whose range is from 0 to 65535. The *protocol-port* argument is the name of a TCP or UDP port. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.
destination-ipv6-prefix / prefix-length	Destination IPv6 network or class of networks about which permit conditions are to be set. This argument must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.
host *destination-ipv6-address*	Specifies the destination IPv6 host address about which permit conditions are to be set. This *destination-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.

dscp *value*	(Optional) Matches a differentiated services code point (DSCP) value against the traffic class value in the Traffic Class field of each IPv6 packet header. Range is from 0 to 63.
routing	(Optional) Matches source-routed packets against the routing extension header within each IPv6 packet header.
hop-by-hop	(Optional) Supports Jumbo-grams. With the Router Alert option, it is an integral part in the operation of Multicast Listener Discovery (MLD). Router Alert [3] is an integral part in the operations of IPv6 Multicast through MLD and RSVP for IPv6.
authen	(Optional) Matches if the IPv6 authentication header is present.
destopts	(Optional) Matches if the IPv6 destination options header is present.
fragments	(Optional) Matches noninitial fragmented packets where the fragment extension header contains a nonzero fragment offset. The **fragments** keyword is an option available only if the *operator* [*port-number*] arguments are not specified.

log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the access list name and sequence number, and whether the packet is permitted; the protocol, and whether it is TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first matching packet, and then at 5-minute intervals, including the number of packets permitted in the prior 5-minute interval.
log-input	(Optional) Provides the same function as the **log** keyword, except that the log-message also includes the input interface.
ttl	(Optional) Turns on matching against time-to-live (TTL) value.
operator	(Optional) Operand that compares the source or destination ports of the specified protocol. Operands are **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range).
ttl value [*value1 value2*]	(Optional) TTL value used for filtering. Range is from 1 to 255. If only *value* is specified, the match is against this value. If both *value1* and *value2* are specified, the packet TTL is matched against the range of TTLs between *value1* and *value2* .
icmp-type	(Optional) ICMP message type for filtering ICMP packets. Range is from 0 to 255.
icmp-code	(Optional) ICMP message code for filtering ICMP packets. Range is from 0 to 255.

established	(Optional) For the TCP protocol only: Indicates an established connection.
match-any	(Optional) For the TCP protocol only: Filters on any combination of TCP flags.
match-all	(Optional) For the TCP protocol only: Filters on all TCP flags.
+ | -	(Required) For the TCP protocol **match-any** , **match-all** : Prefix *flag-name* with **+** or **-** . Use the **+** *flag-name* argument to match packets with the TCP flag set. Use the **-** *flag-name* argument to match packets when the TCP flag is not set.
flag-name	(Required) For the TCP protocol **match-any**, **match-all**. Flag names are: **ack**, **fin**, **psh**, **rst**, **syn**, **urg**.
counter	(Optional) Enables accessing ACL counters using SNMP query.
counter-name	Defines an ACL counter name.

Command Default

No IPv6 access list is defined.

ICMP message generation is enabled by default.

Command Modes

IPv6 access list configuration

Command History

Release	Modification
Release 7.5.4	**bitmask** keyword was introduced.
Release 6.0.1	This command was introduced.

Usage Guidelines

The **permit** (IPv6) command is similar to the **permit** (IPv4) command, except that it is IPv6-specific.

Use the **permit** (IPv6) command following the **ipv6 access-list** command to define the conditions under which a packet passes the access list.

Specifying **ipv6** for the *protocol* argument matches against the IPv6 header of the packet.

By default, the first statement in an access list is number 10, and the subsequent statements are numbered in increments of 10.

You can add **permit**, **deny, or remark** statements to an existing access list without retyping the entire list. To add a new statement anywhere other than the end of the list, create a new statement with an appropriate entry number that falls between two existing entry numbers to indicate where it belongs.

Both the *source-ipv6-prefix/prefix-length* and *destination-ipv6-prefix/prefix-length* arguments are used for traffic filtering (the source prefix filters traffic based upon the traffic source; the destination prefix filters traffic based upon the traffic destination).



Note IPv6 prefix lists, and not access lists, should be used for filtering routing protocol prefixes.

The **fragments** keyword is an option available only if the *operator* [*port* | *protocol-port*] arguments are not specified.

Task ID

Task ID	Operations
acl	read, write

Examples

This example shows how to configure the IPv6 access list named v6-abf-acl and apply the access list to inbound traffic on HundredGigE interface 0/0/2/0.

```
Router(config)# ipv6 access-list v6-abf-acl
Router(config-ipv6-acl)# 10 permit ipv6 any any
Router(config-ipv6-acl)# 20 permit ipv4 any any
Router(config)# interface HundredGigE 0/0/2/0
Router(config-if)# ipv6 access-group v6-abf-acl ingress
```

The following example shows how you can configure DSCP bitmask on ingress ERSPAN.

```
Router# config
Router(config)# ipv6 access-list acl1
Router(config-ipv6-acl)# 10 permit ipv6 host 2001:DB8::2/32 any dscp 33 bitmask 0x3f
Router(config-ipv6-acl)# commit
Router(config-ipv6-acl)# exit
Router(config)# interface HundredGigE 0/0/10/3
Router(config-if)# ipv6 address 2001:DB8::1/32
Router(config-if)# monitor-session TEST ethernet direction rx-only port-level acl ipv6 acl1
Router(config-if)# commit
```

remark (IPv4)

To write a helpful comment (remark) for an entry in an IPv4 access list, use the **remark** command in IPv4 access list configuration mode. To remove the remark, use the **no** form of this command.

[*sequence-number*] **remark** *remark*
no *sequence-number*

Syntax Description

sequence-number	(Optional) Number of the **remark** statement in the access list. This number determines the order of the statements in the access list. Range is 1 to 2147483646. (By default, the first statement is number 10; subsequent statements are incremented by 10.)
remark	Comment that describes the entry in the access list, up to 255 characters long.

Command Default

The IPv4 access list entries have no remarks.

Command Modes

IPv4 access list configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **remark** command to write a helpful comment for an entry in an IPv4 access list. To remove the remark, use the **no** form of this command.

The remark can be up to 255 characters; anything longer is truncated.

If you know the sequence number of the remark you want to delete, you can remove it by entering the **no** *sequence-number* command.

Task ID

Task ID	Operations
ipv4	read, write
acl	read, write

Examples

In the following example, the user1 subnet is not allowed to use outbound Telnet:

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list telnetting
RP/0/RP0/CPU0:router(config-ipv4-acl)# 10 remark Do not allow user1 to telnet out
RP/0/RP0/CPU0:router(config-ipv4-acl)# 20 deny tcp host 172.16.2.88 255.255.0.0 any eq
telnet
RP/0/RP0/CPU0:router(config-ipv4-acl)# 30 permit icmp any any
RP/0/RP0/CPU0:router# show ipv4 access-list telnetting

ipv4 access-list telnetting
  0 remark Do not allow user1 to telnet out
```

```
20 deny tcp 172.16.2.88 255.255.0.0 any eq telnet out
30 permit icmp any any
```

remark (IPv6)

To write a helpful comment (remark) for an entry in an IPv6 access list, use the **remark** command in IPv6 access list configuration mode. To remove the remark, use the **no** form of this command.

[*sequence-number*] **remark** *remark*
no *sequence-number*

Syntax Description

sequence-number	(Optional) Number of the **remark** statement in the access list. This number determines the order of the statements in the access list. Range is 1 to 2147483646. (By default, the first statement is number 10, and the subsequent statements are incremented by 10.)
remark	Comment that describes the entry in the access list, up to 255 characters long.

Command Default

The IPv6 access list entries have no remarks.

Command Modes

IPv6 access list configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

The **remark** (IPv6) command is similar to the **remark** (IPv4) command, except that it is IPv6-specific.

Use the **remark** command to write a helpful comment for an entry in an IPv6 access list. To remove the remark, use the **no** form of this command.

The remark can be up to 255 characters; anything longer is truncated.

If you know the sequence number of the remark you want to delete, you can remove it by entering the **no** *sequence-number* command.

Task ID

Task ID	Operations
acl	read, write

Examples

In this example, a remark is added:

```
RP/0/(config)# ipv6 access-list Internetfilter
RP/0/(config-ipv6-acl)# 10 permit ipv6 3333:1:2:3::/64 any
RP/0/(config-ipv6-acl)# 20 permit ipv6 4444:1:2:3::/64 any
RP/0/(config-ipv6-acl)# 30 permit ipv6 5555:1:2:3::/64 any
RP/0/(config-ipv6-acl)# 39 remark Block BGP traffic from a given host
RP/0/(config-ipv6-acl)# 40 deny tcp host 6666:1:2:3::10 eq bgp host 7777:1:2:3::20 range
1300 1400
RP/0/# show ipv6 access-list Internetfilter
```

```
ipv6 access-list Internetfilter
  10 permit ipv6 3333:1:2:3::/64 any
  20 permit ipv6 4444:1:2:3::/64 any
  30 permit ipv6 5555:1:2:3::/64 any
  39 remark Block BGP traffic from a given host
  40 deny tcp host 6666:1:2:3::10 eq bgp host 7777:1:2:3::20 range host 6666:1:2:3::10 eq
bgp host 7777:1:2:3::20 range 1300 1400
```

resequence access-list ipv4

To renumber existing statements and increment subsequent statements to allow a new IPv4 access list statement (**permit**, **deny**, or **remark**) to be added, use the **resequence access-list ipv4** command in XR EXEC mode.

resequence access-list ipv4 *name* [*base* [*increment*]]

Syntax Description

name	Name of an IPv4 access list.
base	(Optional) Number of the first statement in the specified access list, which determines its order in the access list. Maximum value is 2147483644. Default is 10.
increment	(Optional) Number by which the base sequence number is incremented for subsequent statements. Maximum value is 2147483644. Default is 10.

Command Default

base: 10

increment: 10

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **resequence access-list ipv4** command to add a **permit**, **deny**, or **remark** statement between consecutive entries in an existing IPv4 access list. Specify the first entry number (the *base*) and the increment by which to separate the entry numbers of the statements. The software renumbers the existing statements, thereby making room to add new statements with the unused entry numbers.

Task ID

Task ID	Operations
acl	read, write

Examples

In this example, suppose you have an existing access list:

```
ipv4 access-list marketing
  1 permit 10.1.1.1
  2 permit 10.2.0.0 0.0.255.255
  3 permit tcp host 10.2.2.2 255.255.0.0 any eq telnet
```

You want to add additional entries in the access list. First you resequence the entries, renumbering the statements starting with number 20 and an increment of 5, and then you have room for four additional statements between each of the existing statements:

```
RP/0/RP0/CPU0:router# resequence access-list ipv4 marketing 20 5
RP/0/RP0/CPU0:router# show access-lists ipv4 marketing
```

```
ipv4 access-list marketing
  20 permit 10.1.1.1
  25 permit 10.2.0.0
  30 permit tcp host 10.2.2.2 255.255.0.0 any eq telnet
```

Now you add your new entries.

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list marketing
RP/0/RP0/CPU0:router(config-ipv4-acl)# 3 remark Do not allow user1 to telnet out
RP/0/RP0/CPU0:router(config-ipv4-acl)# 4 deny tcp host 172.16.2.88 255.255.0.0 any eq telnet
RP/0/RP0/CPU0:router(config-ipv4-acl)# 29 remark Allow user2 to telnet out
RP/0/RP0/CPU0:router# show access-lists ipv4 marketing

ipv4 access-list marketing
  3 remark Do not allow user1 to telnet out
  4 deny tcp host 171.69.2.88 255.255.0.0 any eq telnet
  20 permit 10.1.1.1
  25 permit 10.2.0.0
  29 remark Allow user2 to telnet out
  30 permit tcp host 10.2.2.2 255.255.0.0 any eq telnet
```

resequence access-list ipv6

To renumber existing statements and increment subsequent statements to allow a new IPv6 access list statement (**permit**, **deny**, or **remark**) to be added, use the **resequence access-list ipv6** command in .

resequence access-list ipv6 *name* [*base* [*increment*]]

Syntax Description

name	Name of an IPv6 access list.
base	(Optional) Number of the first statement in the specified access list, which determines its order in the access list. Maximum value is 2147483646. Default is 10.
increment	(Optional) Number by which the base sequence number is incremented for subsequent statements. Maximum value is 2147483644. Default is 10.

Command Default

base: 10

increment: 10

Command Modes

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

The **resequence access-list ipv6** command is similar to the **resequence access-list ipv4** command, except that it is IPv6 specific.

Use the **resequence access-list ipv6** command to add a **permit**, **deny**, or **remark** statement between consecutive entries in an existing IPv6 access list. Specify the first entry number (the *base*) and the increment by which to separate the entry numbers of the statements. The software renumbers the existing statements, thereby making room to add new statements with the unused entry numbers.

Task ID

Task ID	Operations
acl	read, write

Examples

In the following example, suppose you have an existing access list:

```
ipv6 access-list Internetfilter
  10 permit ipv6 3333:1:2:3::/64 any
  20 permit ipv6 4444:1:2:3::/64 any
  30 permit ipv6 5555:1:2:3::/64 any
```

You want to add additional entries in the access list. First, you resequence the entries, renumbering the statements starting with number 20 and an increment of 5, and then you have room for four additional statements between each of the existing statements:

```
RP/0/# resequence access-list ipv6 Internetfilter 20 5
RP/0/# show access-lists ipv6 Internetfilter

ipv6 access-list Internetfilter
  20 permit ipv6 3333:1:2:3::/64 any
  25 permit ipv6 4444:1:2:3::/64 any
  30 permit ipv6 5555:1:2:3::/64 any
```

Now you add your new entries.

```
RP/0/(config)# ipv6 access-list Internetfilter
RP/0/(config-ipv6-acl)# 3 remark Block BGP traffic from a given host
RP/0/(config-ipv6-acl)# 4 deny tcp host 6666:1:2:3::10 eq bgp host 7777:1:2:3::20 range
1300 1400
RP/0/# show access-lists ipv6 Internetfilter

ipv6 access-list Internetfilter
  3 remark Block BGP traffic from a given host
  4 deny tcp host 6666:1:2:3::10 eq bgp host 7777:1:2:3::20 range 1300 1404 deny tcp host
171.69.2.88 255.255.0.0 any eq telnet
  20 permit ipv6 3333:1:2:3::/64 any
  25 permit ipv6 4444:1:2:3::/64 any
  30 permit ipv6 5555:1:2:3::/64 any
```

set qos-group

To set the quality of service (QoS) group identifiers on packets, use the **set qos-group** command in policy map class configuration mode. To leave the QoS group values unchanged, use the **no** form of this command.

set qos-group *qos-group-value*
no set qos-group *qos-group-value*

Syntax Description

qos-group-value	QoS group ID. An integer from 1 to 7, to be marked on the packet. The *qos-group-value* is used to select a CoSQ and eventually to a VOQ

Command Default

No group ID is specified.

Command Modes

Policy map class configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **set qos-group** command is supported only in the ingress direction.

The **set qos-group** will be used as internal priority to choose the queue on the egress port.

The **set qos-group** action overrides the default marking section.

In the ingress policy-map, in order to designate the traffic class to a certain CoSQ other than CoSQ 0, the class-map needs to have an explicit set qos-group x statement, where 'x' is the CoSQ in the range of 0 to 7. The default COSQ is 0. In the egress policy-map, a class-map with a corresponding match qos-group x will allow further Quality of Service actions to be applied to the traffic class. For example,

```
class-map prec1
  match prec 1

policy-map test-ingress
  class prec1
    set qos-group 1
    police rate percent 50


class-map qg1
  match qos-group 1


policy-map test-egress
  class qg1
    shape average percent 70
```

Task ID

Task ID	Operations
qos	read, write

Examples

This example sets the QoS group to 5 for packets that match the MPLS experimental bit 1:

```
Router(config)# class-map class1
Router(config-cmap)# match mpls experimental topmost 1
Router(config-cmap)# exit

Router(config)# policy-map policy-in
Router(config-pmap)# class class1...
Router(config-pmap-c)# set qos-group 5
Router(config-pmap-c)# exit
Router(config-pmap)# exit

Router(config)# interface TenGigE 0/1/0/9
Router(config-if)# service-policy input policy-in
```

show access-lists afi-all

To display the contents of current IPv4 and IPv6 access lists, use the **show access-lists afi-all** command in XR EXEC mode.

show access-lists afi-all

Syntax Description

This command has no keywords or arguments.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
acl	read

Examples

This sample output is from the **show access-lists afi-all** command:

```
RP/0/RP0/CPU0:router# show access-lists afi-all

ipv4 access-list crypto-1
 10 permit ipv4 65.21.21.0 0.0.0.255 65.6.6.0 0.0.0.255
 20 permit ipv4 192.168.241.0 0.0.0.255 192.168.65.0 0.0.0.255
```

show access-lists ipv4

To display the contents of current IPv4 access lists, use the **show access-lists ipv4** command in XR EXEC mode.

show access-lists ipv4 [*access-list-name* **hardware** { **ingress** | **verify** } [**interface** *type*] { **sequence** *number* | **location** *node-id* } | **summary** [*access-list-name*] | *access-list-name* [*sequence-number*] | **maximum** [**detail**] [**usage pfilter** { **location** *node-id* | **all** }]]

Syntax Description

access-list-name	(Optional) Name of a particular IPv4 access list. The name cannot contain spaces or quotation marks, but can include numbers.
hardware	(Optional) Identifies the access list as an access list for an interface.
ingress	(Optional) Specifies an inbound interface.
verify	(Optional) Verifies the ACL configured.
interface	(Optional) Displays interface statistics.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
sequence *number*	(Optional) Sequence number of a particular IPv4 access list. Range is 1 to 2147483644.
location *node-id*	(Optional) Location of a particular IPv4 access list. The *node-id* argument is entered in the *rack/slot/module* notation.
summary	(Optional) Displays a summary of all current IPv4 access lists.
sequence-number	(Optional) Sequence number of a particular IPv4 access list. Range is 1 to 2147483644.
maximum	(Optional) Displays the current maximum number of configurable IPv4 access control lists (ACLs) and access control entries (ACEs).
detail	(Optional) Displays TCAM entries.

usage	(Optional) Displays the usage of the access list on a given line card.
pfilter	(Optional) Displays the packet filtering usage for the specified line card.
all	(Optional) Displays the location of all the line cards.

Command Default

The default displays all IPv4 access lists.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.9.1	The ACL counters displays statistics in bytes.
Release 6.0	This command was introduced.

Usage Guidelines

Use the **show access-lists ipv4** command to display the contents of all IPv4 access lists. To display the contents of a specific IPv4 access list, use the *name* argument. Use the *sequence-number* argument to specify the sequence number of the access list.

Use the **hardware , ingress** and **location** keywords to display the access list hardware contents and counters for all interfaces that use the specified access list in a given direction. To display the contents of a specific access list entry, use the **sequence** *number* keyword and argument. The access group for an interface must be configured using the **ipv4 access-group** command for access list hardware counters to be enabled.

Use the **show access-lists ipv4 summary** command to display a summary of all current IPv4 access lists. To display a summary of a specific IPv4 access list, use the *name* argument.

Use the **show access-list ipv4 usage** command to display a summary of all interfaces and access lists programmed on the specified line card.

ACL on **egress** is not supported in Release 6.0

Task ID

Task ID	Operations
acl	read

Examples

In the following example, the contents of all IPv4 access lists are displayed:

```
Router# show access-lists ipv4

ipv4 access-list 101
  10 deny udp any any eq ntp
  20 permit tcp any any
  30 permit udp any any eq tftp
  40 permit icmp any any
```

```
  50 permit udp any any eq domain
ipv4 access-list Internetfilter
  10 permit tcp any 172.16.0.0 0.0.255.255 eq telnet
  20 deny tcp any any
  30 deny udp any 172.18.0.0 0.0.255.255 lt 1024
  40 deny ipv4 any any log
```

This table describes the significant fields shown in the display.

Table 2: show access-lists ipv4 hardware Field Descriptions

Field	Description
ACL name	Name of the ACL programmed in hardware.
Sequence Number	Each ACE sequence number is programmed into hardware with all the fields that are corresponding to the values set in ACE.
Grant	Depending on the ACE rule, the grant is set to deny, permit, or both.
Logging	Logging is set to on if ACE uses a log option to enable logs.
Per ace icmp	If Per ace icmp is set to on in the hardware, ICMP is unreachable, is rate-limited, and is generated. The default is set to on.
Hits	Hardware counter for that ACE.

In the following example, a summary of all IPv4 access lists are displayed:

```
Router# show access-lists ipv4 summary

ACL Summary:
  Total ACLs configured: 3
  Total ACEs configured: 11
```

This table describes the significant fields shown in the display.

Table 3: show access-lists ipv4 summary Field Descriptions

Field	Description
Total ACLs configured	Number of configured IPv4 ACLs.
Total ACEs configured	Number of configured IPV4 ACEs.

This example displays the packet filtering usage for the specified line card:

```
Router# show access-lists ipv4 usage pfilter location 0/RP0/CPU0

Interface : tenGigE 0/0/0/1
Input Common-ACL : ipv4_c_acl  ACL : ipv4_i_acl_1
Output ACL : ipv4_i_acl_1
```

Note To display the packet filtering usage for bundle interfaces, use the **show access-lists ipv4 usage pfilter location all** command.

In the following example, the statistics IPv4 access lists are displayed in bytes and packet counts:

```
Router:ios# show access-lists ipv4 ac hardware ingress location 0/0/CPU0
ipv4 access-list ac
 10 permit ipv4 any 2.2.0.0 0.0.255.255 dscp af11 (477 matches) (30528 byte matches)
 20 permit ipv4 any 2.2.0.0 0.0.255.255 police 5 gbps (Accepted: 464 matches, Dropped: 0)
(Accepted: 29696 byte matches, Dropped: 0 bytes)
```

In the following example, the IPv4 access list is displayed using **detail** keyword:

```
Router# show access-lists ipv4 objv4acl hardware ingress detail location 0/0/CPU0
objv4acl Details:
Sequence Number: 10
NPU ID: 0
Number of DPA Entries: 1
ACL ID: 2
ACE Action: PERMIT
ACE Logging: DISABLED
ABF Action: 0(ABF_NONE)
Hit Packet Count: 477 Byte Count: 30528
Source Address: 0.0.0.1 (Mask 255.255.255.254)
Destination Address: 0.0.0.1 (Mask 255.255.255.254)
DPA Entry: 1
        Entry Index: 0
        DPA Handle: 0x8E08F0A8
        DSCP: 0x28 (Mask 0xFC)
Sequence Number: IMPLICIT DENY
NPU ID: 0
Number of DPA Entries: 1
ACL ID: 2
ACE Action: DENY
ACE Logging: DISABLED
ABF Action: 0(ABF_NONE)
Hit Packet Count: 0 Byte Count: 0
Source Address: 0.0.0.2 (Mask 255.255.255.253)
Destination Address: 0.0.0.2 (Mask 255.255.255.253)
DPA Entry: 1
        Entry Index: 0
        DPA Handle: 0x8E08F390
```

show access-lists ipv6

To display the contents of current IPv6 access lists, use the **show access-lists ipv6** command in .

show access-lists ipv6 [*access-list-name* **hardware** { **ingress** | **verify** } [**interface** *type*] { **sequence** *number* | **location** *node-id* } | **summary** [*access-list-name*] | *access-list-name* [*sequence-number*] | **maximum** [**detail**] [**usage pfilter** { **location** *node-id* | **all** }]]

Syntax Description

access-list-name	(Optional) Name of a particular IPv6 access list. The name cannot contain a spaces or quotation marks, but can include numbers.
hardware	(Optional) Identifies the access list as an access list for an interface.
ingress	(Optional) Specifies an inbound interface.
verify	Verifies the ACL configured. **Note** The **verify** keyword is not supported on NC57-24DD and NC57-18DD-SE line cards.
interface	(Optional) Displays interface statistics.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
sequence *number*	(Optional) Sequence number of a particular IPv6 access list. Range is 1 to 2147483644.
location *node-id*	(Optional) Location of a particular IPv6 access list. The *node-id* argument is entered in the *rack/slot/module* notation.
summary	(Optional) Displays a summary of all current IPv6 access lists.
sequence-number	(Optional) Sequence number of a particular IPv6 access list. Range is 1 to 2147483644.
maximum	(Optional) Displays the current maximum number of configurable IPv6 access control lists (ACLs) and access control entries (ACEs).
detail	(Optional) Displays TCAM entries.
usage	(Optional) Displays the usage of the access list on a given line card.
pfilter	(Optional) Displays the packet filtering usage for the specified line card.
all	(Optional) Displays the location of all the line cards.

Command Default

Displays all IPv6 access lists.

Command Modes

Command History

Release	Modification
Release 7.9.1	The ACL counters displays statistics in bytes.
Release 6.0.1	This command was introduced.

Usage Guidelines

The **show access-lists ipv6** command is similar to the **show access-lists ipv4** command, except that it is IPv6 specific.

Use the **show access-lists ipv6** command to display the contents of all IPv6 access lists. To display the contents of a specific IPv6 access list, use the *name* argument. Use the *sequence-number* argument to specify the sequence number of the access list.

Use the **hardware , ingress** and **location** keywords to display the access list hardware contents and counters for all interfaces that use the specified access list in a given direction. To display the contents of a specific access list entry, use the **sequence** *number* keyword and argument. The access group for an interface must be configured using the **ipv6 access-group** command for access list hardware counters to be enabled.

Use the **show access-lists ipv6 summary** command to display a summary of all current IPv6 access lists. To display a summary of a specific IPv6 access list, use the *name* argument.

Use the **show access-list ipv6 usage** command to display a summary of all interfaces and access lists programmed on the specified line card.

Task ID

Task ID	Operations
acl	read

Examples

In the following example, the IPv6 ACL is configured with the source IPv6 wildcard mask FF:0:FFFF:AA:20 and the destination wildcard mask 0:FFFF:2233::FFFF, the show command displays these wildcard mask:

```
Router# config
Router(config)# ipv6  access-list acl1
Router(config-ipv6-acl)# permit 1:2::3 FF:0:FFFF:AA:20:: 4:5::6 0:FFFF:2233::FFFF
Router(config-ipv6-acl)# commit
Router# show run ipv6 access-list
ipv6 access-list ACL1
 10 permit ipv6 1:2::3 ff:0:ffff:aa:20:: 4:5::6 0:ffff:2233::ffff
```

In the following example, the contents of all IPv6 access lists are displayed:

```
Router# show access-lists ipv6

ipv6 access-list test_ipv6
 10 permit ipv6 any any
 20 permit tcp any eq 3000 any eq 3000
```

In the following example, the contents of an access list named Internetfilter is displayed:

```
Router# show access-lists ipv6 Internetfilter

ipv6 access-list Internetfilter
  3 remark Block BGP traffic from a given host
  4 deny tcp host 6666:1:2:3::10 eq bgp host 7777:1:2:3::20 range 1300 1404 deny tcp host
171.69.2.88 255.255.0.0 any eq telnet
  20 permit ipv6 3333:1:2:3::/64 any
  25 permit ipv6 4444:1:2:3::/64 any
  30 permit ipv6 5555:1:2:3::/64 any
```

In the following example, the contents of an access list named Test that has ACL-based policing is configured is displayed:

```
Router# show ipv6 access-lists Test hardware ingress location 0/1/CPU0
10 permit fec0:0:0:2::/64 any (Accepted: 24303 packets, Dropped: 0 packets)
20 permit any any (Accepted: 13 packets, Dropped: 0 packets)
```

In the following example, a summary of all IPv6 access lists is displayed:

```
Router# show access-lists ipv6 summary

ACL Summary:
  Total ACLs configured: 3
  Total ACEs configured: 11
```

This table describes the significant fields shown in the display.

Table 4: show access-lists ipv6 summary Command Field Descriptions

Field	Description
Total ACLs configured	Number of configured IPv6 ACLs.
Total ACEs configured	Number of configured IPV6 ACEs.

In the following example, the statistics IPv6 access lists are displayed in bytes and packet counts:

```
Router# show ipv6 access-lists Test hardware ingress location 0/1/CPU0
ipv6 access-list Test
10 permit fec0:0:0:2::/64 any (24303 matches) (2459695 byte matches)
20 permit any any (13 matches) (246 byte matches)
```

In the following example, the IPv6 access list is displayed using **detail** keyword:

```
Router# show access-lists ipv6 v6t1 hardware ingress detail location 0/0/CPU0
v6t1 Details:
Sequence Number: 10
NPU ID: 0
Number of DPA Entries: 1
ACL ID: 1
ACE Action: PERMIT
ACE Logging: DISABLED
ABF Action: 0(ABF_NONE)
Hit Packet Count: 0 Byte Count: 0
Source Address: 0:0:0:0::
 Source Address Mask: 0:0:0:0::
Destination Address: 2222:0:0:0::
 Destination Address Mask: ffff:ffff:ffff:ffff::
DPA Entry: 1
```

```
        Entry Index: 0
        DPA Handle: 0x8E3000A8
        DSCP: 0x28 (Mask 0xFC)
Sequence Number: 20
NPU ID: 0
Number of DPA Entries: 1
ACL ID: 1
ACE Action: PERMIT
ACE Logging: DISABLED
ABF Action: 0(ABF_NONE)
Hit Packet Count: 0 Byte Count: 0
TCP Flags: 0x01 (Mask 0x01)
Protocol: 0x06 (Mask 0xFF)
Source Address: 0:0:0:0::
 Source Address Mask: 0:0:0:0::
Destination Address: 2222:0:0:0::
 Destination Address Mask: ffff:ffff:ffff:ffff::
DPA Entry: 1
        Entry Index: 0
        DPA Handle: 0x8E300390
Sequence Number: IMPLICIT NDNA PERMIT
NPU ID: 0
Number of DPA Entries: 1
ACL ID: 1
ACE Action: PERMIT
ACE Logging: DISABLED
ABF Action: 0(ABF_NONE)
Hit Packet Count: 0 Byte Count: 0
Protocol: 0x3A (Mask 0xFF)
Source Address: 0:0:0:0::
 Source Address Mask: 0:0:0:0::
Destination Address: 0:0:0:0::
 Destination Address Mask: 0:0:0:0::
DPA Entry: 1
        Entry Index: 0
        DPA Handle: 0x8E300678
Sequence Number: IMPLICIT NDNS PERMIT
NPU ID: 0
Number of DPA Entries: 1
ACL ID: 1
ACE Action: PERMIT
ACE Logging: DISABLED
ABF Action: 0(ABF_NONE)
Hit Packet Count: 0 Byte Count: 0
Protocol: 0x3A (Mask 0xFF)
Source Address: 0:0:0:0::
 Source Address Mask: 0:0:0:0::
Destination Address: 0:0:0:0::
 Destination Address Mask: 0:0:0:0::
DPA Entry: 1
        Entry Index: 0
        DPA Handle: 0x8E300960
Sequence Number: IMPLICIT DENY
NPU ID: 0
Number of DPA Entries: 1
ACL ID: 1
ACE Action: DENY
ACE Logging: DISABLED
ABF Action: 0(ABF_NONE)
Hit Packet Count: 0 Byte Count: 0
Source Address: 0:0:0:0::
 Source Address Mask: 0:0:0:0::
Destination Address: 0:0:0:0::
 Destination Address Mask: 0:0:0:0::
```

```
DPA Entry: 1
        Entry Index: 0
        DPA Handle: 0x8E300C48
```

show object-group network

To display the operation state of a network object group, use the **show object-group network** command in XR EXEC mode.

show object-group network { **ipv4 | ipv6** } *object-group-name*

Syntax Description

ipv4	Displays the operation state of an IPV4 network object group.
ipv6	Displays the operation state of an IPV6 network object group.
object-group-name	Name of the object-group.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
root-system	read
system	read

Example

This example shows how to display the operation state of an IPV4 network object group:

```
Router# show object-group network ipv4 ipv4_type5_obj1

50.0.0.0/16
50.1.0.0/16
50.2.0.0/16
50.3.0.0/16
50.4.0.0/16
host 40.0.0.1
host 40.0.0.2
host 40.0.0.3
host 40.0.0.4
host 40.0.0.5
object-group ipv4_type1_obj1
range 60.0.0.1 60.0.1.100
!
```

This example shows how to display the operation state of an IPV6 network object group:

```
Router# show object-group network ipv6 ipv6_type5_obj1

50::/120
50::100/120
50::200/120
50::300/120
50::400/120
host 40::1
host 40::2
host 40::3
host 40::4
host 40::5
object-group ipv6_type2_obj1
range 60::10 60::20
!
```

Related Commands

Command	Description
show object-group port , on page 90	Displays the operation state of a port object group.

show object-group port

To display the operation state of a port object group, use the **show object-group port** command in XR EXEC mode.

show object-group port *object-group-name*

Syntax Description

object-group-name	Name of the object-group.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
root-system	read
system	read

Example

This example shows how to display the operation state of a port object group:

```
Router# show object-group port port_type4_obj1

object-group port port_type4_obj1
eq 40
object-group port_type1_obj1
range 50 60
!
```

Related Commands

Command	Description
show object-group network, on page 88	Displays the operation state of a network object group.



ARP Commands

This chapter describes the commands used to configure and monitor the Address Resolution Protocol (ARP) on NCS 5000 routers.

For detailed information about ARP concepts, configuration tasks, and examples, refer to the *IP Addresses and Services Configuration Guide for Cisco NCS 5000 Series Routers*.

- arp, on page 92
- arp dagr, on page 94
- arp gratuitous ignore, on page 95
- arp learning, on page 96
- arp purge-delay, on page 97
- arp timeout, on page 98
- clear arp-cache, on page 99
- local-proxy-arp, on page 101
- peer (DAGR), on page 102
- priority-timeout, on page 103
- proxy-arp, on page 104
- route distance, on page 105
- route metric, on page 106
- show arp, on page 107
- show arp idb, on page 111
- show arp dagr, on page 113
- show arp traffic, on page 114
- timers (DAGR), on page 117

arp

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

arp [**vrf** *vrf-name*] *ip-address hardware-address encapsulation-type* [**alias**]
no arp [**vrf** *vrf-name*] *ip-address hardware-address encapsulation-type* [**alias**]

Syntax Description

vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) VRF instance that identifies a VPN.
ip-address	IPv4 (network layer) address for which a permanent entry is added to the ARP cache. Enter the IPv4 address in a four-part dotted-decimal format that corresponds to the local data-link address (a 32-bit address).
hardware-address	Hardware (data link layer) address that the IPv4 address is linked to. Enter the local data-link address (a 48-bit address), such as 0800.0900.1834.
encapsulation-type	Encapsulation type. The encapsulation types are: • arpa • srp • srpa • srpb For Ethernet interfaces, this is typically the arpa keyword.
alias	(Optional) Causes the software to respond to ARP requests as if it were the owner of both the specified IP address and hardware address, whether proxy ARP is enabled or not.

Command Default

No entries are permanently installed in the ARP cache.

Command Modes

XR Config mode

Host-tracking configuration

Command History

Release	Modification
Release 6.0	This command was introduced.
Release 24.1.1	This command was made available in the host-tracking configuration mode.

Usage Guidelines

The 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.

Static entries are permanent entries that map a network layer address (IPv4 address) to a data-link layer address (MAC address). If the **alias** keyword is specified when creating the entry, the interface to which the entry

is attached will act as if it is the owner of the specified addresses, that is, it will respond to ARP request packets for this network layer address with the data link layer address in the entry.

The software does not respond to any ARP requests received for the specified IP address unless proxy ARP is enabled on the interface on which the request is received. When proxy ARP is enabled, the software responds to ARP requests with its own local interface hardware address.

To remove all nonstatic entries from the ARP cache, enter the clear arp-cache, on page 99 in the appropriate configuration mode.

Task ID

Task ID	Operations
cef	read, write

Examples

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

```
Router# configure
Router(config)# arp 192.168.7.19 0800.0900.1834 arpa
```

The following is an example of configuring ARP in host-tracking configuration mode:

```
Router#(config)# interface BVI1
Router#(config-if)# host-routing
Router#(config-if)# vrf vrf_1
Router#(config-if)# ipv4 address 10.0.0.1 255.255.0.0
Router#(config-if)# mac-address 0.dc1.dc2
Router#(config-if)# host-tracking
Router#(config-if-host-tracking)# bgp-gateway
Router#(config-if-host-tracking)# arp
Router#(config-if-host-tracking-arp)# bfd fast-detect
Router#(config-if-host-tracking-arp)#
```

arp dagr

To configure Direct Attached Gateway Redundancy (DAGR), use the **arp dagr** command in interface configuration mode.

arp dagr

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

This command has no keywords or arguments.

Task ID

Task ID	Operations
cef	write

Examples

The following example enables DAGR configuration:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface TenGigE 0/0/0/1
RP/0/RP0/CPU0:router(config-if)# arp dagr
RP/0/RP0/CPU0:router(config-if-dagr)#
```

arp gratuitous ignore

To ignore receipt of gratuitous Address Resolution Protocol (ARP) packets, use the **arp gratuitous ignore** command in interface configuration mode. To receipt gratuitous ARP packets, use the no form of this command.

arp gratuitous ignore
no arp gratuitous ignore

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
cef	write

Examples

This example shows how to configure **arp gratuitous ignore** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface TenGigE 0/0/0/1
RP/0/RP0/CPU0:router(config-if)# arp gratuitous ignore
```

arp learning

To enable the dynamic learning of ARP entries for a local subnet or all subnets, use the **arp learning** command.

To disable this command, use the **no** prefix or the **disable** option for this command.

arp learning local
no arp learning local
arp learning disable
no arp learning disable

Syntax Description

local	Enables the dynamic learning of ARP entries for local subnets. When arp learning local is configured on an interface or sub-interface, it learns only the ARP entries from ARP packets on the same subnet.
disable	Disables the dynamic learning of all ARP entries.

Command Default

This command has no keywords or arguments.

Command Modes

Sub-interface configuration mode

```
RP/0/RP0/CPU0:router(config)#interface GigabitEthernet 0/0/0/1
RP/0/RP0/CPU0:router(config-if)# ipv4 address 12.1.3.4 255.255.255.0
RP/0/RP0/CPU0:router(config-if)# arp learning local
RP/0/RP0/CPU0:router(config-if)# no shut
RP/0/RP0/CPU0:router(config-if)# commit
```

```
RP/0/RP0/CPU0:router(config)# interface GigabitEthernet 0/0/0/1
RP/0/RP0/CPU0:router(config-if)# ipv4 address 12.1.3.4 255.255.255.0
RP/0/RP0/CPU0:router(config-if)# arp learning disable
RP/0/RP0/CPU0:router(config-if)# commit
```

arp purge-delay

To delay purging Address Resolution Protocol (ARP) entries when an interface goes down, use the **arp purge-delay** command in interface configuration mode. To turn off the purge delay feature, use the **no** form of this command.

arp purge-delay *value*
no arp purge-delay *value*

Syntax Description

value	Sets the purge delay time in seconds. Range is 1 to 65535.

Command Default

Default value is off.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **arp purge-delay** command to delay purging ARP entries when an interface goes down. If the interface comes up within the delay time, then the ARP entries are restored to prevent packet loss with Equal Cost Multipath (ECMP) configured.

Task ID

Task ID	Operations
cef	read, write

Examples

The following is an example of setting the purge delay to 50 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface TenGigE 0/0/0/0
RP/0/RP0/CPU0:router(config-if)# arp purge-delay 50
```

arp timeout

To specify the duration of dynamic entries learned on an interface remain in the Address Resolution Protocol (ARP) cache, enter the **arp timeout** command in interface configuration mode. To remove the **arp timeout** command from the configuration file and restore the system to its default condition with respect to this command, enter the **no** form of this command.

arp timeout *seconds*
no arp timeout *seconds*

Syntax Description

seconds	Indicates the time, in seconds, for which an entry remains in the ARP cache. Range is 30 to 4294967295.

Command Default

Entries remain in the ARP cache for 14,400 seconds (4 hours).

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0	This command was supported.

Usage Guidelines

This command is ignored when issued on interfaces that do not use ARP. Also, ARP entries that correspond to the local interface or that are statically configured by the user never time out.

The **arp timeout** command applies only to the interface that is entered. When the timeout is changed for an interface the change applies only to that interface.

The **show interfaces** command displays the ARP timeout value in hours:minutes:seconds, as follows:

```
ARP type: ARPA, ARP Timeout 04:00:00
```

Task ID

Task ID	Operations
cef	read, write

Examples

The following example shows how to set the ARP timeout to 3600 seconds to allow entries to time out more quickly than the default:

```
RP/0/RP0/CPU0:router#configure
RP/0/RP0/CPU0:router(config)#interface TenGigE 0/0/0/0
RP/0/RP0/CPU0:router(config-if)# arp timeout 3600
```

clear arp-cache

To delete all dynamic entries from the Address Resolution Protocol (ARP) cache, clear the fast-switching cache, and clear the IP route cache, use the **clear arp-cache** command in XR EXEC mode.

clear arp-cache {**traffic** *type interface-path-id* | **location** *node-id*}

Syntax Description

traffic	Deletes traffic statistics on the specified interface.
t ype	Interface type. For more information, use the question mark (?) online help function.

interface- path-id	Either a physical interface instance or a virtual interface instance as follows:
	• Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation.
	  • *rack*: Chassis number of the rack.
	  • *slot*: Physical slot number of the modular services card or line card.
	  • *module*: Module number. A physical layer interface module (PLIM) is always 0.
	  • *port*: Physical port number of the interface.
	• Virtual interface instance. Number range varies depending on interface type.
	For more information about the syntax for the router, use the question mark (?) online help function.

location *node-id*	Clears the ARP entries for a specified location. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

When issued without keywords or arguments, the **clear arp-cache** command clears all entries in the ARP cache.

Task ID

Task ID	Operations
cef	execute

Examples

The following example shows how to remove traffic statistic entries from the ARP cache that match the specified interface:

```
RP/0/RP0/CPU0:router# clear arp-cache traffic TenGigE 0/0/0/1 location 0/1/CPU0
```

The following example shows how to remove entries from the ARP cache that match the specified location:

```
RP/0/RP0/CPU0:router# clear arp-cache location 0/1/CPU0
```

local-proxy-arp

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

local-proxy-arp
no local-proxy-arp

Syntax Description

This command has no keywords or arguments.

Command Default

Local proxy ARP is disabled on all interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

When local proxy ARP is enabled, the networking device responds to ARP requests that meet all the following conditions:

- The target IP address in the ARP request, the IP address of the ARP source, and the IP address of the interface on which the ARP request is received are on the same Layer 3 network.
- The next hop for the target IP address is through the same interface as the request is received.

Typically, local proxy ARP is used to resolve MAC addresses to IP addresses in the same Layer 3 network such as, private VLANs that are Layer 2-separated. Local proxy ARP supports all types of interfaces supported by ARP and unnumbered interfaces.

Using the **no** form of the command removes the specified command from the configuration file and restores the system to its default condition with respect to the command.

Task ID

Task ID	Operations
cef	read, write

peer (DAGR)

To create a Direct Attached Gateway Redundancy (DAGR) group for a virtual IP address, use the **peer** command in DAGR interface configuration mode.

peer ipv4 *IP-address*

Syntax Description

IP-address	Virtual IPv4 address for the DAGR group.

Command Default

None

Command Modes

DAGR interface configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
cef	write

Examples

The following example configures a DAGR group peer:

```
RP/0/RP0/CPU0:router(config-if-dagr)# peer ipv4 192.168.7.19
RP/0/RP0/CPU0:router(config-if-dagr-peer)#
```

priority-timeout

To configure the timer to time out a high-priority Direct Attached Gateway Redundancy (DAGR) route and reverting to normal priority, use the **priority-timeout** command in DAGR peer interface configuration mode.

priority-timeout *time*

Syntax Description

time	Time in seconds after which a high-priority route reverts to a normal priority route. The range of values is 1 to 10000.

Command Default

Default for *time* is 20 seconds.

Command Modes

DAGR peer interface configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When this function is applied, the DAGR group configuration is updated in the database.

The new timer values take effect the next time the timer is set. No immediate timer restarts are triggered on the basis of this event.

Task ID

Task ID	Operations
cef	write

Examples

The following example configures a priority timeout of 25 seconds:

```
RP/0/RP0/CPU0:router(config-if-dagr-peer)# priority-timeout 25
RP/0/RP0/CPU0:router(config-if-dagr-peer)#
```

proxy-arp

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

proxy-arp
no proxy-arp

Syntax Description

This command has no keywords or arguments.

Command Default

Proxy ARP is disabled on all interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

When proxy ARP is disabled, the networking device responds to ARP requests received on an interface only if one of the following conditions is met:

- The target IP address in the ARP request is the same as the interface IP address on which the request is received.
- The target IP address in the ARP request has a statically configured ARP alias.

When proxy ARP is enabled, the networking device also responds to ARP requests that meet all of the following conditions:

- The target IP address is not on the same physical network (LAN) on which the request is received.
- The networking device has one or more routes to the target IP address.
- All of the routes to the target IP address go through interfaces other than the one on which the request is received.

Using the **no** form of the command removes the specified command from the configuration file and restores the system to its default condition with respect to the command.

Task ID

Task ID	Operations
cef	read, write

Examples

The following example shows how to enable proxy ARP on tenGigE interface 0/0/0/0:

```
RP/0/RP0/CPU0:router#(config)# interface TenGigE  0/0/0/0
RP/0/RP0/CPU0:router#(config-if)# proxy-arp
```

route distance

To configure route distance for a given Direct Attached Gateway Redundancy (DAGR) group, use the **route distance** command in DAGR peer interface configuration mode.

route distance normal *normal-distance* **priority** *priority-distance*

Syntax Description

normal *normal-distance*	Sets normal route (administrative) distance. Range is 0 to 256.
priority *priority-distance*	Sets priority route (administrative) distance. Range is 0 to 256.

Command Default

Default for *normal-distance* default is 150 and the default for *priority-distance* is 5.

Command Modes

DAGR peer interface configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The default setting for a priority distance takes precedence over that of a typical Internet Gateway Protocol (IGP). The normal distance setting does not.

When this setting is applied, the DAGR group is updated in the database.

Task ID

Task ID	Operations
cef	write

Examples

The following example configures a DAGR group peer with a normal route distance of 48 and priority route distance of 5:

```
RP/0/RP0/CPU0:router(config-if-dagr-peer)# route distance normal 48 priority 5
RP/0/RP0/CPU0:router(config-if-dagr-peer)#
```

route metric

To configure normal and priority route metrics for a given Direct Attached Gateway Redundancy (DAGR) group, use the **route metric** command in DAGR peer interface configuration mode.

route metric normal *normal-metric* **priority** *priority-metric*

Syntax Description

normal *normal-metric*	Sets a normal value for routes installed in the Routing Information Base (RIB). The range of values is 0 to 256.
priority *priority-metric*	Sets a priority value for routes installed in the RIB. The range of values is 0 to 256.

Command Default

The default for *normal-metric* is 100, and the default for *priority-metric* is 90.

Command Modes

DAGR peer interface configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The route metric values are of less significance than the **route distance** command values. Setting a route metric allows the configuration of values for routers installed in the RIB.

When this setting is applied, the DAGR group is updated in the database.

Task ID

Task ID	Operations
cef	write

Examples

The following example configures a DAGR group peer with a normal metric of 48 and a priority metric of 5:

```
RP/0/RP0/CPU0:router(config-if-dagr-peer)# route metric normal 48 priority 5
RP/0/RP0/CPU0:router(config-if-dagr-peer)#
```

show arp

To display the Address Resolution Protocol (ARP), enter the **show arp** command in XR EXEC mode.

show arp `vrf` *vrf-name* [*ip-address hardware-address interface-path-id*] **location** *node-id*

Syntax Description

vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) VRF instance that identifies a VPN.
ip-address	(Optional) The ARP entries you want to display.
hardware-address	(Optional) The ARP entries that match the 48-bit MAC address are displayed.
interface- path-id	(Optional) Either a physical interface instance or a virtual interface instance as follows: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation. • *rack*: Chassis number of the rack. • *slot*: Physical slot number of the modular services card or line card. • *module*: Module number. A physical layer interface module (PLIM) is always 0. • *port*: Physical port number of the interface. • Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
location *node-id*	(Optional) Displays the ARP entry for a specific location. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

The active RSP is the default location.

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

ARP establishes correspondences between network addresses (an IP address, for example) and Ethernet hardware addresses. A record of each correspondence is kept in a cache for a predetermined amount of time and then discarded.

For **show arp** *interface-type interface-instance* form, the **location** *node-id* keyword and argument is mandatory for Bundle and VLAN-on-Bundle interfaces to indicate which location the cache entries for the bundle should be displayed. For physical interfaces, specifying the **location** *node-id* keyword and argument is optional since the interface can only exist on one node.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output from the **show arp** command with no location specified:

```
RP/0/RP0/CPU0:router# show arp

------------------------------------------------------------------------------
0/RP0/CPU0
------------------------------------------------------------------------------
Address         Age        Hardware Addr   State      Type  Interface
5.28.0.1        03:13:25   0000.0c07.ac1c  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.0.2        00:00:29   d824.bd90.2180  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.0.3        00:00:30   d824.bd90.2100  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.7.111      00:06:11   000c.29e4.c25f  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.10.10      01:19:49   0022.bdd9.0948  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.11.4       02:29:58   d46d.5037.29c0  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.11.12      01:31:08   4055.395f.4408  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.11.66      01:10:34   d46d.5028.9e20  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.12.31      00:40:01   00a0.c900.0000  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.12.58      01:19:37   a80c.0d1f.8278  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.12.59      01:11:06   6c9c.ed75.9f78  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.12.89      00:35:53   10f3.1111.90c8  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.12.100     -          c472.95a6.2a80  Interface  ARPA  MgmtEth0/RP0/CPU0/0
5.28.14.52      00:12:36   8478.ac36.08e0  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.14.55      00:19:38   a80c.0d19.0808  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.14.59      01:16:19   d46d.5064.b080  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.17.3       01:20:21   e0ac.f16c.a6d0  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.20.111     00:22:15   000c.2925.d81f  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.21.1       01:47:22   28c7.ce01.f830  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.21.6       01:29:30   c472.95a6.2390  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.21.7       01:15:56   c472.95a6.1740  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.22.1       01:22:32   d867.d955.2888  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.22.2       01:27:29   c472.95a6.fa20  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.22.3       01:27:15   001a.6c40.e232  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.22.4       01:26:11   c472.95a6.f7c0  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.22.5       01:20:44   6c9c.ed6b.a888  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.22.6       01:30:06   c472.95a6.e930  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.22.7       01:21:08   0001.0203.0406  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.22.8       01:12:40   28c7.ce01.df50  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.22.9       01:29:06   28c7.ce01.dc20  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.22.10      01:14:46   c472.95a6.0600  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.22.109     00:30:33   28c7.ce01.dc20  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.100.50     03:43:05   000c.29c2.f21d  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
5.28.201.28     03:12:40   c472.95a6.a161  Dynamic    ARPA  MgmtEth0/RP0/CPU0/0
20.30.1.1       -          c472.95a6.2a86  Interface  ARPA  TenGigE0/0/0/1
20.30.1.2       00:01:47   6c9c.ed2c.a060  Dynamic    ARPA  TenGigE0/0/0/1
20.31.1.1       -          c472.95a6.2a87  Interface  ARPA  TenGigE0/0/0/2
```

The following is sample output from the **show arp** command with the *interface-type interface-instance* argument:

```
RRP/0/RP0/CPU0:router# show arp tenGigE 0/0/0/1

------------------------------------------------------------------------------
0/RP0/CPU0
------------------------------------------------------------------------------
```

```
Address         Age        Hardware Addr   State      Type  Interface
20.30.1.1       -          c472.95a6.2a86  Interface  ARPA  TenGigE0/0/0/1
20.30.1.2       00:04:58   6c9c.ed2c.a060  Dynamic    ARPA  TenGigE0/0/0/1
```

The following is sample output from the **show arp** command with the *hardware-address* designation:

```
RP/0/RP0/CPU0:router# show arp 0005.5f1d.8100

Address Age Hardware Addr State Type Interface
172.16.7.2 - 0005.5f1d.8100 Interface ARPA TenGigE0/0/0/2
```

The following is sample output from the **show arp** command with the **location** keyword and *node-id* argument:

```
RP/0/RP0/CPU0:router# show arp location 0/2/CPU0

Address Age Hardware Addr State Type Interface
192.168.15.1 - 00dd.00ee.00ff Alias ARPA
192.168.13.1 - 00aa.00bb.00cc Static ARPA
172.16.7.1 00:35:49 0002.fc0e.9600 Dynamic ARPA TenGigE0/0/0/2
172.16.7.2 - 0005.5f1d.8100 Interface ARPA TenGigE0/0/0/2
```

This table describes the significant fields shown in the display.

Table 5: show arp Command Field Descriptions

Field	Description
Address	Displays the network address that corresponds to the hardware address.
Age	Displays the age in hours:minutes:seconds of the cache entry. A hyphen (-) means the address is local.
Hardware Addr	Displays the LAN hardware address of a MAC address that corresponds to the network address.
State	Displays the current state of the cache entry. Values are: • Dynamic • Interface • Alias • Static • "-" (indicates global static and alias entries)
Type	Displays the encapsulation type the Cisco IOS XR software is using for the network address in this entry. Value is ARPA.
Interface	Displays the interface associated with this network address.
ARP statistics	Displays ARP packet and error statistics.

Field	Description
ARP cache	Displays general information about the IP address and MAC address association entries in the ARP cache.
IP Packet drop count for node */*/*	Displays the number of IP packets dropped because the buffer ran out of space before an ARP response was received. **Note** */*/* represents the node ID in the format *rack/slot/module*.

show arp idb

To display the ARP database statistics for an interface, use the **show arp idb** command in EXEC mode.

show arp idb *interface-name* **location** *node-id*

Syntax Description

interface-name	Name of the interface
node-id	Location of the interface. LC node for physical interfaces, RP or LC node for virtual interfaces

Command Default

There is no default location, location needs to be provided in the CLI.

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

The **show arp idb** command is useful to verify the IP addresses, Mac address, ARP configuration(s) applied on the interface and the entry statistics.

For **show arp idb** *interface-type interface-instance* form, the **location** *node-id* keyword and argument is mandatory for Bundle and VLAN-on-Bundle interfaces to indicate which location the cache entries for the bundle should be displayed.

Task ID

Task ID	Operations
cef	read

Examples

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

```
RP/0/0/CPU0:ios#show arp idb GigabitEthernet 0/0/0/0 location 0/0/CPU0
Mon Jan 30 10:32:15.387 IST
GigabitEthernet0/0/0/0 (0x00000060):
IDB Client: default
IPv4 address 1.1.1.1, Vrf ID 0x60000000
VRF Name default
Dynamic learning: Enable
Dynamic entry timeout: 14400 secs
Drop adjacency timeout: Disable
Purge delay: off
Cache limit: 128000
Incomplete glean count: 1
```

Complete glean count: 0
Complete protocol count: 0
Dropped glean count: 0
Dropped protocol count: 0
IPv4 caps added (state up)
MPLS caps not added
Interface not virtual, not client fwd ref,
Proxy arp not configured, not enabled
Local Proxy arp not configured
Packet IO layer is NetIO
Srg Role : DEFAULT
Idb Flag : 49292
IDB is Complete
IDB Flag Description:
[CAPS | COMPLETE | IPV4_CAPS_CREATED | SPIO_ATTACHED |
SPIO_SUPPORTED]
Idb Flag Ext : 0x0
Idb Oper Progress : NONE
Client Resync Time : Jan 30 10:07:10.736787
Total entries : 9
| Event Name | Time Stamp | S, M
| idb-create | Jan 30 10:07:10.784 | 1, 0
| idb-state-up | Jan 30 10:07:10.784 | 0, 0
| caps-state-update | Jan 30 10:07:10.784 | 0, 1
| address-update | Jan 30 10:07:10.784 | 0, 0
| idb-complete | Jan 30 10:07:10.784 | 0, 0
| idb-entry-create | Jan 30 10:07:10.784 | 0, 0
| idb-caps-add | Jan 30 10:07:10.784 | 0, 0
| idb-caps-add-cb | Jan 30 10:07:10.784 | 0, 0
| idb-last-garp-sent | Jan 30 10:07:11.808 | 0, 0

show arp dagr

To display the operational state of all Direct Attached Gateway Redundancy (DAGR) groups, use the **show arp dagr** command in XR EXEC mode

show arp dagr [*interface* [*IP-address*]]

Syntax Description

interface [*IP-address*]	(Optional) Restricts the output to a specific interface and virtual IP address.

Command Default

None

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

This command has no keywords or arguments.

Task ID

Task ID	Operations
cef	read, write

Examples

The following example shows the current operational state of the DAGR groups:

```
RP/0/RP0/CPU0:router# show arp dagr

------------------------------------------------------------------------------
0/1/CPU0
------------------------------------------------------------------------------
Interface                 Virtual IP      State     Query-pd Dist Metr
GigabitEthernet0/1/0/2    192.168.7.19    Active    None     150  100
GigabitEthernet0/1/0/2    193.24.0.45     Query     1        None None
GigabitEtherget0/1/0/3    192.66.0.45     Init      None     None None
```

show arp traffic

To display Address Resolution Protocol (ARP) traffic statistics, enter the **show arp traffic** command in XR EXEC mode.

show arp traffic [**vrf** *vrf-name*] [*interface-path-id*] [**location** *node-id*]

Syntax Description

vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) VRF instance that identifies a VPN.

interface- path-id	(Optional) Either a physical interface instance or a virtual interface instance as follows:
	• Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation.
	  • *rack*: Chassis number of the rack.
	  • *slot*: Physical slot number of the modular services card or line card.
	  • *module*: Module number. A physical layer interface module (PLIM) is always 0.
	  • *port*: Physical port number of the interface.
	• Virtual interface instance. Number range varies depending on interface type.
	For more information about the syntax for the router, use the question mark (?) online help function.

location *node-id*	(Optional) Displays the ARP entry for a specific location. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

The active RSP is the default location.

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

ARP establishes correspondences between network addresses (an IP address, for example) and Ethernet hardware addresses. A record of each correspondence is kept in a cache for a predetermined amount of time and then discarded.

For **show arp traffic,** *interface-instance*, the **location***node-id* keyword and argument is mandatory for Bundle and VLAN-on-Bundle interfaces to indicate which location the cache entries for the bundle should be displayed. For physical interfaces, specifying the **location** *node-id* keyword and argument is optional since the interface can only exist on one node.

Task ID

Task ID	Operations
cef	read

Examples

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

```
RP/0/RP0/CPU0:router# show arp traffic

show arp traffic
Thu Dec 10 09:51:38.761 UTC

------------------------------------------------------------------------------
0/6/CPU0
------------------------------------------------------------------------------

ARP statistics:
  Recv: 163 requests, 79 replies
  Sent: 14138 requests, 177 replies (0 proxy, 0 local proxy, 14 gratuitous)
  Resolve requests rcvd: 7204
  Resolve requests dropped: 295
  Errors: 0 out of memory, 0 no buffers, 0 out of sunbet

ARP cache:
  Total ARP entries in cache: 22
  Dynamic: 11, Interface: 11, Standby: 0
  Alias: 0,   Static: 0,    DHCP: 0

  IP Packet drop count for node 0/6/CPU0: 6909

  Total ARP-IDB:19


------------------------------------------------------------------------------
0/2/CPU0
------------------------------------------------------------------------------

ARP statistics:
  Recv: 162532 requests, 243 replies
  Sent: 15879 requests, 162561 replies (0 proxy, 0 local proxy, 29 gratuitous)
  Resolve requests rcvd: 47593
  Resolve requests dropped: 0
  Errors: 0 out of memory, 0 no buffers, 0 out of sunbet

ARP cache:
  Total ARP entries in cache: 125
  Dynamic: 112, Interface: 13, Standby: 0
  Alias: 0,   Static: 0,    DHCP: 0

  IP Packet drop count for node 0/2/CPU0: 44804

  Total ARP-IDB:13
```

The following is sample output from the **show arp traffic** command with the **location** keyword and *node-id* argument:

```
RP/0/RP0/CPU0:router# show arp traffic location 0/4/CPU0

Thu Dec 10 09:51:56.209 UTC
```

```
ARP statistics:
  Recv: 364474 requests, 96 replies
  Sent: 14131 requests, 364499 replies (0 proxy, 0 local proxy, 25 gratuitous)
  Resolve requests rcvd: 5699
  Resolve requests dropped: 94
  Errors: 0 out of memory, 0 no buffers, 0 out of sunbet

ARP cache:
  Total ARP entries in cache: 18
  Dynamic: 9, Interface: 9, Standby: 0
  Alias: 0,   Static: 0,    DHCP: 0

  IP Packet drop count for node 0/4/CPU0: 5603

  Total ARP-IDB:18
```

timers (DAGR)

To configure the Direct Attached Gateway Redundancy (DAGR) timers for sending ARP requests, use the **timers** command in DAGR peer interface configuration mode.

timers query *query-time* **standby** *standby-time*

Syntax Description

query *query-time*	The value is a time (in seconds) between successive ARP requests being sent out to the virtual IP address, when the group is in the query state. The range of values is 1 to 10000.
standby *standby-time*	The value is a time (in seconds) between successive ARP requests being sent out to the virtual IP address, when the group is in the standby state. The range of values is 1 to 10000.

Command Default

The default for *query-time* is 1 second, and the default for *standby-time* is 20 seconds.

Command Modes

DAGR peer interface configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

When this function is applied, the DAGR group configuration is updated in the database. The new timer values take effect the next time the timer is set. No immediate timer restarts are triggered on the basis of this event.

Task ID

Task ID	Operations
cef	write

Examples

The following example configures a DAGR group peer with a query time of 2 and a standby time of 40:



Cisco Express Forwarding Commands

This chapter describes the commands used to configure and monitor Cisco Express Forwarding (CEF) on on NCS 5000 routers.

For detailed information about CEF concepts, configuration tasks, and examples, see *Cisco IP Addresses and Services Configuration Guide*.

- bgp policy accounting, on page 121
- cef adjacency route override rib, on page 123
- clear cef ipv4 drops, on page 125
- clear cef ipv4 exceptions, on page 127
- clear cef ipv6 drops, on page 129
- clear cef ipv6 exceptions, on page 131
- show adjacency, on page 133
- show cef, on page 135
- show cef ipv4, on page 137
- show cef ipv4 adjacency, on page 140
- show cef ipv4 drops, on page 142
- show cef ipv4 hardware, on page 144
- show cef ipv4 exact-route, on page 147
- show cef ipv4 exceptions, on page 149
- show cef ipv4 resource, on page 151
- show cef ipv4 summary, on page 153
- show cef ipv4 unresolved, on page 155
- show cef ipv6 , on page 157
- show cef ipv6 adjacency, on page 161
- show cef ipv6 adjacency hardware, on page 165
- show cef ipv6 drops, on page 168
- show cef ipv6 exact-route, on page 170
- show cef ipv6 exceptions, on page 172
- show cef ipv6 hardware, on page 174
- show cef ipv6 interface, on page 176
- show cef ipv6 resource, on page 179
- show cef ipv6 summary, on page 181
- show cef ipv6 unresolved, on page 183
- show cef mpls adjacency, on page 185

- show cef mpls adjacency hardware, on page 187
- show cef mpls interface, on page 189
- show cef mpls unresolved, on page 191
- show cef summary, on page 192

bgp policy accounting

To enable Border Gateway Protocol (BGP) policy accounting, use the **bgp policy accounting** command in interface configuration mode. To disable BGP policy accounting, use the **no** form of this command.

ipv4 bgp policy accounting { **input** | **output** { **destination-accounting** [**source-accounting**] | **source-accounting** [**destination-accounting**] } }

ipv6 bgp policy accounting { **input** | **output** { **destination-accounting** [**source-accounting**] | **source-accounting** [**destination-accounting**] } }

Syntax Description

input	Enables BGP policy accounting policy on the ingress IPv4 or IPv6 unicast interface.
destination-accounting	Enables accounting policy on the basis of the destination address.

Command Default

There is no BGP policy accounting.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

- To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
- To specify the accounting policy, the proper route policy configuration must be in place, matching specific BGP attributes using the **set traffic-index** command. In BGP router configuration mode, use the **table-policy** command to modify the accounting buckets when the IP routing table is updated with routes learned from BGP. To display accounting policy information, use the **show cef interface bgp-policy-statistics**, **show bgp policy**, and **show route bgp** commands.
- The functionality of the following keywords are not supported:
  - **output**
  - **source-accounting**
  - **output destination-accounting**
- This feature is applicable for the following address families:
  - IPv4
  - IPv6

Task ID

Task ID	Operations
network	read, write

Examples

The following example shows how to configure the BGP policy accounting:

For IPv4:

```
Router(config)# interface HundredGigE 0/5/0/0
Router(config-if)# ipv4 bgp policy accounting output source-accounting
Router(config-if)# commit
```

For IPv6:

```
Router(config)# interface HundredGigE 0/5/0/0
Router(config-if)# ipv6 bgp policy accounting output source-accounting
Router(config-if)# commit
```

cef adjacency route override rib

Use this command to enable CEF prefer Adjacency Information Base (AIB) prefixes over Routing Information Base (RIB) prefixes in the Global configuration mode. To disable CEF prefer AIB prefixes over RIB prefixes, use the **no** form of this command.

cef adjacency route override rib

no cef adjacency route override rib

Syntax Description

route	Enables adjacency route configuration .
override	Sets override options for the adjacency routes.
rib	Sets options for adjacency routes to override the RIB routes.

Command Default

By default, CEF prefers RIB prefixes over AIB prefixes.

Command Modes

Global configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

CEF may prefer the L2 adjacency for forwarding over the RIB (routing) entry under the following conditions:

- When there is no local ARP entry (yet).

  ARP learning may result in the router creating a forwarding entry.

- A forwarding entry of /32 (or /128 for IPv6) RIB routes are overridden when there is a covering connected or attached route.

  If an interface has a larger subnet, and you want to redirect a /32 out of that subnet of a different interface via a static route.

This can be seen in scenarios of EVPN and or HSRP, or in bridge domains with a BVI and multiple EFP's.

To deviate from the behavior of preferring a L2 adjacency for forwarding over a route entry, use the **cef adjacency route override rib** command.

Task ID

Task ID	Operation
cef	read, write

Example

The following example shows how to override the CEF adjacency route:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router# cef adjacency route override rib
```

clear cef ipv4 drops

To clear Cisco Express Forwarding (CEF) IPv4 packet drop counters, use the **clear cef ipv4 drops**command in XR EXEC mode.

clear cef ipv4 drops location *node-id*

Syntax Description

location *node-id*	Clears IPv4 packet drop counters for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, this command will clear IPv4 CEF drop counters only for the node on which the command is issued.

Task ID

Task ID	Operations
basic-services	read, write
cef	read, write

Examples

The following example displays sample output for the IPv4 Cisco Express Forwarding (CEF) table packet drop counters, and clears IPv4 CEF drop counters for location 0/RP0/CPU0:

```
RP/0/RP0/CPU0:router# show cef ipv4 drops

CEF Drop Statistics
Node: 0/RP0/CPU0
  Unresolved drops     packets :              0
  Unsupported drops    packets :             61
  Null0 drops          packets :              0
  No route drops       packets :          74026
  No Adjacency drops   packets :              0
  Checksum error drops packets :              0
  RPF drops            packets :              0
  RPF suppressed drops packets :              0
  RP destined drops    packets :              0
  Discard drops        packets :              0
  GRE lookup drops     packets :              0
  GRE processing drops packets :              0
  LISP punt drops      packets :              0
  LISP encap err drops packets :              0
  LISP decap err drops packets :              0
```

```
RP/0/RP0/CPU0:router# clear cef ipv4 drops location 0/RP0/CPU0

  Node: 0/RP0/CPU0
  Clearing CEF Drop Statistics
```

clear cef ipv4 exceptions

To clear IPv4 Cisco Express Forwarding (CEF) exception packet counters, use the **clear cef ipv4 exceptions** command in XR EXEC mode mode.

clear cef ipv4 exceptions location *node-id*

Syntax Description

location *node-id*	Clears IPv4 CEF exception packet counters for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, this command will clear IPv4 CEF exception packet counters for all nodes.

Task ID

Task ID	Operations
basic-services	read, write
cef	read, write

Examples

The following example displays sample output for the IPv4 Cisco Express Forwarding (CEF) exception packet counters, and clear s IPv4 CEF exception packets node 0/RP0/CPU0:

```
RP/0/RP0/CPU0:router# show cef ipv4 exceptions

CEF Exception Statistics
Node: 0/RP0/CPU0
  Slow encap  packets :               0
  Unsupported packets :               0
  Redirect    packets :               0
  Receive     packets :               0
  Broadcast   packets :               0
  IP options  packets :               0
  TTL expired packets :               0
  Fragmented  packets :               0

RP/0/RP0/CPU0:router# clear cef ipv4 exceptions location 0/RP0/CPU0

Node: 0/RP0/CPU0
```

```
Clearing CEF Exception Statistics
```

clear cef ipv6 drops

To clear Cisco Express Forwarding (CEF) IPv6 packet drop counters, use the **clear cef ipv6 drop** command in XR EXEC mode.

clear cef ipv6 drops location *node-id*

Syntax Description

location *node-id*	Clears IPv6 packet drop counters for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, this command clears IPv6 CEF drop counters for all nodes.

Task ID

Task ID	Operations
basic-services	read, write
cef	read, write

Examples

The following example displays sample output for the IPv6 Cisco Express Forwarding (CEF) table packet drop counters, and clears IPv6 CEF drop counters for location 0/RP0/CPU0:

```
RP/0/RP0/CPU0:router# show cef ipv6 drops

CEF Drop Statistics
Node: 0/RP0/CPU0
  Unresolved drops     packets :              0
  Unsupported drops    packets :              0
  Null0 drops          packets :              0
  No route drops       packets :              0
  No Adjacency drops   packets :              0
  Checksum error drops packets :              0
  RPF drops            packets :              0
  RPF suppressed drops packets :              0
  RP destined drops    packets :              0
  Discard drops        packets :              0
  GRE lookup drops     packets :              0
  GRE processing drops packets :              0
  LISP punt drops      packets :              0
  LISP encap err drops packets :              0
```

```
  LISP decap err drops packets :               0

RP/0/RP0/CPU0:router# clear cef ipv6 drop

Node: 0/RP0/CPU0
Clearing CEF Drop Statistics
```

clear cef ipv6 exceptions

To clear IPv6 Cisco Express Forwarding (CEF) exception packet counters, use the **clear cef ipv6 exceptions** command in XR EXEC mode .

clear cef ipv6 exceptions location *node-id*

Syntax Description

location *node-id*	Clears IPv6 CEF exception packet counters for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, this command clears IPv6 CEF exception packet counters for all nodes.

Task ID

Task ID	Operations
basic-services	read, write
cef	read, write

Examples

The following example displays sample output for the IPv6 Cisco Express Forwarding (CEF) exception packet counters, and clears the IPv6 CEF exception packets for location:

```
RP/0/RP0/CPU0:router# show cef ipv6 exceptions

CEF Exception Statistics
Node: 0/RP0/CPU0
  Slow encap  packets :               0
  Unsupported packets :               0
  Redirect    packets :               0
  Receive     packets :               0
  Broadcast   packets :               0
  IP options  packets :               0
  TTL expired packets :               0
  Fragmented  packets :               0

RP/0/RP0/CPU0:router# clear cef ipv6 exceptions location 0/RP0/CPU0

Node: 0/RP0/CPU0
```

```
Clearing CEF Exception Statistics
```

show adjacency

To display Cisco Express Forwarding (CEF) adjacency table information, use the **show adjacency** command in XR EXEC mode.

show adjacency [**ipv4** [**nexthop** *ipv4-address*] | **mpls** | **ipv6**] [*interface type interface-instance*] [**remote**] [**detail**] [**location** *node-id*]

Syntax Description

ipv4	(Optional) Displays only IPv4 adjacencies.
nexthop *ipv4-address*	(Optional) Displays adjacencies that are destined to the specified IPv4 nexthop.
mpls	(Optional) Displays only MPLS adjacencies.
ipv6	(Optional) Displays only IPv6 adjacencies.
interface-type	(Optional) Interface type. For more information, use the question mark (?) online help function.

interface-instance	Either a physical interface instance or a virtual interface instance:
	• Physical interface instance. Naming notation is *rack/slot/module/port* and a slash mark between values is required as part of the notation.
	  • *rack*: Chassis number of the rack.
	  • *slot*: Physical slot number of the line card.
	  • *module*: Module number. A physical layer interface module (PLIM) is always 0.
	  • *port*: Physical port number of the interface.
	• Virtual interface instance. Number range varies depending on interface type.
	For more information about the syntax for the router, use the question mark (?) online help function.

remote	(Optional) Displays only remote adjacencies. A remote adjacency is an internal adjacency used to forward packets between line cards.
detail	(Optional) Displays detailed adjacency information, including Layer 2 information.
location *node-id*	(Optional) Displays detailed CEF information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

This command is used to verify that an adjacency exists for a connected device, that the adjacency is valid, and that the MAC header rewrite string is correct.

If you do not specify a node with the **location** keyword and *node-id* argument, this command displays the CEF adjacency table for the node on which the command is issued.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output from **show adjacency** command with the **location** keyword specified:

This table describes the significant fields shown in the display.

Table 6: show adjacency Command Field Descriptions

Field	Description
Interface	Outgoing interface associated with the adjacency.
Address	Address can represent one of these addresses: • Next hop IPv4 or IPv6 address • Point-to-Point address Information in parentheses indicates different types of adjacency.
Version	Version number of the adjacency. Updated whenever the adjacency is updated.
Refcount	Number of references to this adjacency.
Protocol	Protocol for which the adjacency is associated.
0f000800 and 000c86f33d330800453a21c10800	Layer 2 encapsulation string.
mtu	Value of the maximum transmission unit (MTU).
flags	Internal field.
packets	Number of packets going through the adjacency.
bytes	Number of bytes going through the adjacency.

show cef

To display information about packets forwarded by Cisco Express Forwarding (CEF), use the **show cef** command in XR EXEC mode.

show cef [*prefix* [*mask*]] [**hardware** {**egress** | **ingress**} | **detail**] [**location** {*node-id* | **all**}]

Syntax Description

prefix	(Optional) Longest matching CEF entry for the specified IPv4 destination prefix.
mask	(Optional) Exact CEF entry for the specified IPv4 prefix and mask.
hardware	(Optional) Displays detailed information about hardware.
egress	Displays information from the egress packet switch exchange (PSE) file.
ingress	Displays information from the ingress packet switch exchange (PSE) file.
detail	(Optional) Displays full details.
location *node-id*	(Optional) Displays detailed CEF information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
all	(Optional) Displays all locations.

Command Default

When the prefix is not explicitly specified, this command displays all the IPv4 prefixes that are present in CEF. When not specified, the location defaults to the active Route Processor (RP) node.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
cef	read

Examples

The following sample output shows the load information flag from the **show cef** command for both **hardware** and **ingress** keywords.

```
RP/0/RP0/CPU0:router# show cef 101.1.3.0/24 hardware ingress location 0/RP0/CPU0
101.1.3.0/24, version 0, internal 0x40000001 (0x598491e8) [1], 0x0 (0x0),
(0x0)
 local adjacency 10.0.101.2
 Prefix Len 24, traffic index 0, precedence routine (0)
```

```
 BGP Attribute: id: 8, Local id: 6, Origin AS: 1003, Next Hop AS: 4

   via 10.0.101.2, 2 dependencies, recursive
    next hop 10.0.101.2 via 10.0.101.2/32


 Number of Mnodes:   2
 Mnode 0 HW Location: 0x00080404  HW Value
[ 0x0081a600 00000000 00000000 00000000 ]

 Leaf Mnode 1  HW Location: 0x040d3030
 Hardware Leaf:      PLU Leaf Value
[ 0x8000d800 028842c6 00000000 1fff2000 ]

 FCR  2 TLU Address 0x00210b19 TI 0 AS 6

VPN Label 1 0

 ************* IGP LoadInfo *****************
 Loadinfo HW Max Index  0
 Loadinfo SW Max Index  0
 PBTS Loadinfo Attached: No
 LI Path [ 0]  HFA Info: 0x10204028   FCR: 4
 ******************************************

------------------------------------------------
 HW Rx Adjacency  0 Detail:
------------------------------------------------
    Rx Adj HW Address   0x02040280  (ADJ)
    packets 0  bytes 0
    HFA Bits 0x80 gp 16 mtu 9248 (Fabric MTU) TAG length 0
    OI 0x409 (Tx uidb 0 PPindex 1033)
    OutputQ 0 Output-port 0x0 local-outputq 0x8000

[ 0x80181040 00002420 00000409 00008000 ]
[ 0x00000000 00000000 00000000 00000000 ]
[ 0x00000000 00000000 00000000 00000000 ]
```

show cef ipv4

To display the IPv4 Cisco Express Forwarding (CEF) table, use the **show cef ipv4** command in XR EXEC mode.

show cef ipv4 [*prefix* [*mask*] | *interface-type interface-instance*] [**detail**] [**location** *node-id*]

Syntax Description

prefix	(Optional) Longest matching CEF entry for the specified IPv4 destination prefix.
mask	(Optional) Exact CEF entry for the specified IPv4 prefix and mask.
interface-type	(Optional) Interface type. For more information, use the question mark (?) online help function.

interface-instance	Either a physical interface instance or a virtual interface instance:
	• Physical interface instance. Naming notation is *rack/slot/module/port* and a slash mark between values is required as part of the notation.
	  • *rack*: Chassis number of the rack.
	  • *slot*: Physical slot number of the line card.
	  • *module*: Module number. A physical layer interface module (PLIM) is always 0.
	  • *port*: Physical port number of the interface.
	Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RSP0) and the module is CPU0. Example: interface MgmtEth0/RSP0 /CPU0/0.
	• Virtual interface instance. Number range varies depending on interface type.
	For more information about the syntax for the router, use the question mark (?) online help function.

detail	(Optional) Displays full CEF entry information.
location *node-id*	(Optional) Displays the IPv4 CEF table for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

If the location is not specified, the command defaults to the active RP node.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 24.4.1	The command is enhanced to include additional details about Layer 2 IPv4 prefixes that resolve as nexthop Layer 3 prefixes.

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, this command displays the CEF table on the node in which the command is issued. Otherwise, the command is effective on the node specified by the **location** *node-id* keyword and argument.

Task ID

Task ID	Operations
cef	read

Examples

The following sample output is from the **show cef ipv4** command:

This table describes the significant fields shown in the display.

Table 7: show cef ipv4 Command Field Descriptions

Field	Description
Prefix	Prefix in the IPv4 CEF table.
Next Hop	Next hop of the prefix.
Interface	Interface associated with the prefix.

In the following example, the IPv4 Layer 2 prefixes, which resolve as nexthop for Layer 3 prefixes are collapsed.

```
Router#show cef ipv4 209.165.201.1 detail
Output received:
Mon Dec  2 08:31:43.765 UTC
209.165.201.1/27, version 47031, internal 0x5000001 0x40 (ptr 0x98246ad8) [1], 0x0 (0x0),
0x0 (0x0)
Updated Dec  2 08:27:35.523
Prefix Len 32, traffic index 0, precedence n/a, priority 4
gateway array (0x98099098) reference count 1, flags 0x2010, source rib (7), 0 backups
[1 type 3 flags 0x40441 (0x98134438) ext 0x0 (0x0)]
LW-LDI[type=0, refc=0, ptr=0x0, sh-ldi=0x0]
gateway array update type-time 1 Dec  2 08:27:35.523
LDI Update time Dec  2 08:31:14.951

Level 1 - Load distribution: 0 1
[0] via 209.165.200.225/27, recursive
[1] via 209.165.200.226/27, recursive

via 209.165.200.225/27, 3 dependencies, recursive, bgp-multipath [flags 0x6080]
path-idx 0 NHID 0x0 [0x982355c8 0x0]
next hop 209.165.200.225/27 via 209.165.200.225/27

Load distribution: 0 1 2 2 (refcount 1)

Hash  OK  Interface                 Address
0     Y   HundredGigE0/0/0/0/2      fe80::2
1     Y   Bundle-Ether1201          fe80::2
```

```
2     Y   Bundle-Ether1301          fe80::3
3     Y   Bundle-Ether1301          fe80::3

via 209.165.200.226/27, 3 dependencies, recursive, bgp-multipath [flags 0x6080]
path-idx 1 NHID 0x0 [0x98235678 0x0]
next hop 209.165.200.226/27 via 209.165.200.226/27

Load distribution: 0 1 2 2 (refcount 1)

Hash  OK  Interface                 Address
4     Y   HundredGigE0/0/0/0/2      fe80::2
5     Y   Bundle-Ether1201          fe80::2
6     Y   Bundle-Ether1301          fe80::3
7     Y   Bundle-Ether1301          fe80::3
```

show cef ipv4 adjacency

To display Cisco Express Forwarding (CEF) IPv4 adjacency status and configuration information, use the **show cef ipv4 adjacency** command in XR EXEC mode.

show cef ipv4 adjacency [*interface-type interface-path-id*] [**location** *node-id*] [**detail**] [**discard**] [**glean**] [**null**] [**punt**] [**remote**] [**protected**]

Syntax Description

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

interface- path-id	(Optional) Either a physical interface instance or a virtual interface instance:
	• Physical interface instance. Naming notation is *rack/slot/module/port* and a slash mark between values is required as part of the notation.
	  • *rack*: Chassis number of the rack.
	  • *slot*: Physical slot number of the line card.
	  • *module*: Module number. A physical layer interface module (PLIM) is always 0.
	  • *port*: Physical port number of the interface.
	• Virtual interface instance. Number range varies depending on interface type.
	For more information about the syntax for the router, use the question mark (?) online help function.

location *node-id*	(Optional) Displays detailed CEF information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
detail	(Optional) Displays the detailed adjacency information.
discard	(Optional) Filters out and displays only the discarded adjacency information.
glean	(Optional) Filters out and displays only the glean adjacency information.
null	(Optional) Filters out and displays only the adjacency information.
punt	(Optional) Filters out and displays only the punt adjacency information.
remote	(Optional) Filters out and displays only the remote adjacency information.
protected	(Optional) Filters out and displays only the IP-Fast Reroute (FRR) protected adjacency information.

Command Default

No default behavior or values

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, the **show cef ipv4 adjacency** command displays the CEF adjacency table for the node on which the command is issued.

Task ID

Task ID	Operations
cef	read

Examples

The following sample output is from **show cef ipv4 adjacency** command :

```
RP/0/RP0/CPU0:router# show cef ipv4 adjacency tenGigE 0/0/0/0

Display protocol is ipv4
Interface    Address                                          Type    Refcount
Mg0/RSP0/CPU0/0Prefix: 10.25.0.3/32                            local   2
             Adjacency: PT:0x782a2900 12.25.0.3/32
             Interface: Mg0/RSP0/CPU0/0
             MAC: 00.d0.02.75.ab.fd.00.11.93.ef.e3.50.08.00
             Interface Type: 0x8, Base Flags: 0x1
             Dependent adj type: remote
             Dependent adj intf: Mg0/RSP0/CPU0/0
Mg0/RSP0/CPU0/0Prefix: 10.24.0.32/32                           remote  6
             Adjacency: PT:0x782a2b58
             Interface: Mg0/RSP0/CPU0/0
             MAC: 28.4e.4f.4e.45.29
             Interface Type: 0x8, Base Flags: 0x0
```

This table describes the significant fields shown in the display.

Table 8: show cef ipv4 adjacency Command Field Descriptions

Field	Description
Interface	Interface associated with the prefix.
Address	Prefix address information.
Type	Type of adjacency, can be either local or remote.
Refcount	Number of times the adjacency is referenced by other routers.

show cef ipv4 drops

To display IPv4 Cisco Express Forwarding (CEF) table packet drop counters, use the **show cef ipv4 drops** command in XR EXEC mode.

show cef ipv4 drops [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Displays IPv4 CEF table packet drop counters for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

A packet might be dropped from the IPv4 CEF table because of unresolved CEF entries, unsupported features, absence of route information, absence of adjacency information, or an IP checksum error.

If you do not specify a node with the **location** keyword and *node-id* argument, this command displays IPv4 CEF packet drop counters for all nodes.

The **show cef ipv4 drop** command output counters include CEF table packet drop counters for IPv4 and IPv6 packets.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output from the **show cef ipv4 drops** for location command:

```
RP/0/RP0/CPU0:router# show cef ipv4 drops

CEF Drop Statistics
Node: 0/RP0/CPU0
  Unresolved drops     packets :              0
  Unsupported drops    packets :             61
  Null0 drops          packets :              0
  No route drops       packets :          74026
  No Adjacency drops   packets :              0
  Checksum error drops packets :              0
  RPF drops            packets :              0
  RPF suppressed drops packets :              0
  RP destined drops    packets :              0
  Discard drops        packets :              0
  GRE lookup drops     packets :              0
  GRE processing drops packets :              0
  LISP punt drops      packets :              0
  LISP encap err drops packets :              0
  LISP decap err drops packets :              0
```

Table 9: show cef ipv4 drop Command Field Descriptions

Field	Description
Unresolved drops	Drops due to unresolved routes.
Unsupported drops	Drops due to an unsupported feature.
Null0 drops	Drops to the Null0 interface.
No route drops	Number of packets dropped because there were no routes to the destination.
No Adjacency drops	Number of packets dropped because there were no adjacencies established.
Checksum error drops	Drops due to IPv4 checksum error.
RPF drops	Drops due to IPv4 unicast RPF[1].
RPF suppressed drops	Drops suppressed due to IPv4 unicast RPF.
RP destined drops	Drops destined for the router.
Discard drops	Drops those were discarded.
GRE lookup drops	GRE packets dropped during GRE Lookup.
GRE processing drops	GRE packets dropped during GRE Processing.
LISP punt drops	LISP packets dropped during software processing of the packets.
LISP encap err drops	LISP encap packets dropped due to errors.
LISP decap err drops	LISP Decap packets dropped due to errors.

[1] RPF = Reverse Path Forwarding

show cef ipv4 hardware

To display Cisco Express Forwarding (CEF) IPv4 hardware status and configuration information, use the **show cef ipv4 hardware** command in XR EXEC mode.

show cef [**vrf** *vrf-name*] **ipv4 hardware** {**egress** | **ingress** [**detail** | **location** *node-id*]}

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
egress	Displays information from the egress packet switch exchange (PSE) file.
ingress	Displays information from the ingress packet switch exchange (PSE) file.
detail	(Optional) Displays full details.
location *node-id*	(Optional) Displays detailed CEF information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
cef	read

Examples

The following sample output is from the **show cef ipv4 hardware** command:

```
RP/0/RP0/CPU0:router#  sh cef ipv4 hardware egress

Prefix              Next Hop            Interface
------------------- ------------------- ------------------
0.0.0.0/0           7.35.0.1/32         <recursive>
0.0.0.0/32          broadcast
5.5.5.1/32          receive             Loopback0
7.35.0.0/16         attached            MgmtEth0/RP0/CPU0/0
7.35.0.0/32         broadcast           MgmtEth0/RP0/CPU0/0
7.35.0.1/32         7.35.0.1/32         MgmtEth0/RP0/CPU0/0
7.35.0.2/32         7.35.0.2/32         MgmtEth0/RP0/CPU0/0
7.35.0.3/32         7.35.0.3/32         MgmtEth0/RP0/CPU0/0
```

```
7.35.0.5/32         7.35.0.5/32         MgmtEth0/RP0/CPU0/0
7.35.0.6/32         7.35.0.6/32         MgmtEth0/RP0/CPU0/0
7.35.0.56/32        7.35.0.56/32        MgmtEth0/RP0/CPU0/0
7.35.0.245/32       7.35.0.245/32       MgmtEth0/RP0/CPU0/0
7.35.10.38/32       7.35.10.38/32       MgmtEth0/RP0/CPU0/0
7.35.10.44/32       7.35.10.44/32       MgmtEth0/RP0/CPU0/0
7.35.10.47/32       receive             MgmtEth0/RP0/CPU0/0
7.35.10.74/32       7.35.10.74/32       MgmtEth0/RP0/CPU0/0
7.35.10.113/32      7.35.10.113/32      MgmtEth0/RP0/CPU0/0
7.35.11.22/32       7.35.11.22/32       MgmtEth0/RP0/CPU0/0
7.35.11.27/32       7.35.11.27/32       MgmtEth0/RP0/CPU0/0
7.35.11.32/32       7.35.11.32/32       MgmtEth0/RP0/CPU0/0
7.35.11.78/32       7.35.11.78/32       MgmtEth0/RP0/CPU0/0
7.35.11.111/32      7.35.11.111/32      MgmtEth0/RP0/CPU0/0
7.35.11.112/32      7.35.11.112/32      MgmtEth0/RP0/CPU0/0
7.35.12.11/32       7.35.12.11/32       MgmtEth0/RP0/CPU0/0
7.35.12.23/32       7.35.12.23/32       MgmtEth0/RP0/CPU0/0
7.35.12.24/32       7.35.12.24/32       MgmtEth0/RP0/CPU0/0
7.35.12.29/32       7.35.12.29/32       MgmtEth0/RP0/CPU0/0
7.35.12.30/32       7.35.12.30/32       MgmtEth0/RP0/CPU0/0
7.35.12.44/32       7.35.12.44/32       MgmtEth0/RP0/CPU0/0
7.35.15.83/32       7.35.15.83/32       MgmtEth0/RP0/CPU0/0
7.35.15.84/32       7.35.15.84/32       MgmtEth0/RP0/CPU0/0
7.35.15.86/32       7.35.15.86/32       MgmtEth0/RP0/CPU0/0
7.35.15.92/32       7.35.15.92/32       MgmtEth0/RP0/CPU0/0
7.35.15.93/32       7.35.15.93/32       MgmtEth0/RP0/CPU0/0
7.35.15.95/32       7.35.15.95/32       MgmtEth0/RP0/CPU0/0
7.35.15.96/32       7.35.15.96/32       MgmtEth0/RP0/CPU0/0
7.35.15.97/32       7.35.15.97/32       MgmtEth0/RP0/CPU0/0
7.35.15.98/32       7.35.15.98/32       MgmtEth0/RP0/CPU0/0
7.35.15.103/32      7.35.15.103/32      MgmtEth0/RP0/CPU0/0
7.35.15.119/32      7.35.15.119/32      MgmtEth0/RP0/CPU0/0
7.35.15.123/32      7.35.15.123/32      MgmtEth0/RP0/CPU0/0
7.35.15.133/32      7.35.15.133/32      MgmtEth0/RP0/CPU0/0
7.35.15.173/32      7.35.15.173/32      MgmtEth0/RP0/CPU0/0
7.35.15.175/32      7.35.15.175/32      MgmtEth0/RP0/CPU0/0
7.35.15.178/32      7.35.15.178/32      MgmtEth0/RP0/CPU0/0
7.35.15.179/32      7.35.15.179/32      MgmtEth0/RP0/CPU0/0
7.35.15.188/32      7.35.15.188/32      MgmtEth0/RP0/CPU0/0
7.35.19.124/32      7.35.19.124/32      MgmtEth0/RP0/CPU0/0
7.35.19.127/32      7.35.19.127/32      MgmtEth0/RP0/CPU0/0
7.35.19.180/32      7.35.19.180/32      MgmtEth0/RP0/CPU0/0
7.35.19.181/32      7.35.19.181/32      MgmtEth0/RP0/CPU0/0
7.35.19.182/32      7.35.19.182/32      MgmtEth0/RP0/CPU0/0
7.35.19.183/32      7.35.19.183/32      MgmtEth0/RP0/CPU0/0
7.35.19.201/32      7.35.19.201/32      MgmtEth0/RP0/CPU0/0
7.35.19.205/32      7.35.19.205/32      MgmtEth0/RP0/CPU0/0
7.35.20.157/32      7.35.20.157/32      MgmtEth0/RP0/CPU0/0
7.35.21.156/32      7.35.21.156/32      MgmtEth0/RP0/CPU0/0
7.35.21.212/32      7.35.21.212/32      MgmtEth0/RP0/CPU0/0
7.35.23.59/32       7.35.23.59/32       MgmtEth0/RP0/CPU0/0
7.35.25.48/32       7.35.25.48/32       MgmtEth0/RP0/CPU0/0
7.35.25.77/32       7.35.25.77/32       MgmtEth0/RP0/CPU0/0
7.35.25.100/32      7.35.25.100/32      MgmtEth0/RP0/CPU0/0
7.35.25.101/32      7.35.25.101/32      MgmtEth0/RP0/CPU0/0
7.35.25.102/32      7.35.25.102/32      MgmtEth0/RP0/CPU0/0
7.35.25.107/32      7.35.25.107/32      MgmtEth0/RP0/CPU0/0
7.35.25.148/32      7.35.25.148/32      MgmtEth0/RP0/CPU0/0
7.35.25.198/32      7.35.25.198/32      MgmtEth0/RP0/CPU0/0
7.35.25.210/32      7.35.25.210/32      MgmtEth0/RP0/CPU0/0
7.35.25.223/32      7.35.25.223/32      MgmtEth0/RP0/CPU0/0
7.35.25.232/32      7.35.25.232/32      MgmtEth0/RP0/CPU0/0
7.35.25.233/32      7.35.25.233/32      MgmtEth0/RP0/CPU0/0
7.35.26.107/32      7.35.26.107/32      MgmtEth0/RP0/CPU0/0
```

```
7.35.26.188/32      7.35.26.188/32      MgmtEth0/RP0/CPU0/0
7.35.49.94/32       7.35.49.94/32       MgmtEth0/RP0/CPU0/0
7.35.104.155/32     7.35.104.155/32     MgmtEth0/RP0/CPU0/0
7.35.255.255/32     broadcast           MgmtEth0/RP0/CPU0/0
202.153.144.25/32   7.35.0.1/32         MgmtEth0/RP0/CPU0/0
224.0.0.0/4         0.0.0.0/32
224.0.0.0/24        receive
255.255.255.255/32  broadcast
```

show cef ipv4 exact-route

To display an IPv4 Cisco Express Forwarding (CEF) exact route, use the **show cef ipv4 exact-route** command in XR EXEC mode.

show cef ipv4 exact-route {*source-address destination-address*} [**protocol***protocol-name*] [**source-port***source-port*] [**destination-port***destination-port*] [**ingress-interface***type interface-path-id*] [*policy-class-value*] [**detail** | **location** *node-id*]

Syntax Description

source-address	The IPv4 source address in x.x.x.x format.
destination-address	The IPv4 destination address in x.x.x.x format.
protocol *protocol name*	(Optional) Displays the specified protocol for the route.
source-port *source-port*	(Optional) Sets the UDP source port. The range is from 0 to 65535.
destination-port *destination-port*	(Optional) Sets the UDP destination port. The range is from 0 to 65535.
ingress-interface	(Optional) Sets the ingress interface.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
policy-class *value*	(Optional) Displays the class for the policy-based tunnel selection. The range for the tunnel policy class value is from 1 to 7.
detail	(Optional) Displays full CEF entry information.
location *node-id*	(Optional) Displays the IPv4 CEF table for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

If the Layer 4 information is enabled, the source-port, destination-port, ingress-interface, and protocol fields are required. Otherwise, the output of the **show cef ipv4 exact-route** command is not correct.

Task ID

Task ID	Operations
cef	read

Examples

The following sample output is from the **show cef ipv4 exact-route** command:

```
RP/0/RP0/CPU0:router# show cef ipv4 exact-route 10.1.1.1 10.1.1.2 detail

0.0.0.0/0, version 432, proxy default, internal 0x2000201[1]
 Prefix Len 0, traffic index 0, precedence routine (0)
   via tenGigE0/RSP0RP1/CPU0/0
```

This table describes the significant fields shown in the display.

Table 10: show cef ipv4 exact-route Command Field Descriptions

Field	Description
Prefix	Prefix in the IPv4 CEF table .
Next Hop	Next hop of the prefix
Interface	Interface associated with the prefix

show cef ipv4 exceptions

To display IPv4 Cisco Express Forwarding (CEF) exception packet counters, use the **show cef ipv4 exceptions** command in .

show cef ipv4 exceptions [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Displays CEF exception packet counters for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

CEF exception packets are those packets that have been sent from the hardware to the software because they require additional handling. The types of IPv4 CEF exception packets are displayed in the command's output and are defined.

If you do not specify a node with the **location** keyword and *node-id* argument, this command displays IPv4 CEF exception packet counters on all nodes.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output from the **show cef ipv4 exceptions** command:

```
RP/0/# show cef ipv4 exceptions

CEF Exception Statistics
Node: 0/RP0/CPU0
  Slow encap  packets :              0
  Unsupported packets :              0
  Redirect    packets :              0
  Receive     packets :              0
  Broadcast   packets :              0
  IP options  packets :              0
  TTL expired packets :              0
  Fragmented  packets :              0
```

This table describes the significant fields shown in the display.

Table 11: show cef ipv4 exceptions Command Field Descriptions

Field	Description
Slow encap	Number of packets requiring special processing during encapsulation.
Redirect	Number of ICMP[2] redirect messages sent.
Receive	Number of packets destined to the router.
Broadcast	Number of broadcasts received.
IP options	Number of IP option packets.
TTL expired	Number of packets with expired TTLs[3].
Fragmented	Number of packets that have been fragmented.

[2] ICMP = internet control message protocol
[3] TTL = time to live

show cef ipv4 resource

To display the IPv4 nonrecursive prefix entries in the IPv4 Cisco Express Forwarding (CEF) table, use the **show cef ipv4 resource** command in XR EXEC mode.

show cef ipv4 resource [**detail**] [**hardware** {**egress** | **ingress**}] [**location** *node-id*]

Syntax Description

detail	(Optional) Displays detailed information resources listed in the IPv4 CEF table.
hardware	(Optional) Displays detailed information about hardware.
egress	(Optional) Displays egress packet switch exchange (PSE).
ingress	(Optional) Displays ingress packet switch exchange (PSE).
location *node-id*	(Optional) Displays the IPv4 resource entries in the IPv4 CEF table for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, the output displays the IPv4 CEF nonrecursive routes for the node on which the command is issued.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output from the **show cef ipv4 resource** command:

```
RP/0/RP0/CPU0:router# show cef ipv4 resource detail

CEF resource availability summary state: GREEN
  ipv4 shared memory resource:
        CurrMode GREEN, CurrUtil 0%
        CurrAvail 1874526208 bytes, MaxAvail 1875693568 bytes
  ipv6 shared memory resource:
        CurrMode GREEN, CurrUtil 0%
        CurrAvail 1874591744 bytes, MaxAvail 1875365888 bytes
  mpls shared memory resource:
        CurrMode GREEN, CurrUtil 0%
        CurrAvail 1874407424 bytes, MaxAvail 1875038208 bytes
  common shared memory resource:
```

```
      CurrMode GREEN, CurrUtil 0%
      CurrAvail 1873215488 bytes, MaxAvail 1874972672 bytes
TABLE hardware resource: GREEN
LEAF hardware resource: GREEN
LOADINFO hardware resource: GREEN
NHINFO hardware resource: GREEN
LABEL_INFO hardware resource: GREEN
IDB hardware resource: GREEN
FRR_NHINFO hardware resource: GREEN
LDSH_ARRAY hardware resource: GREEN
RSRC_MON hardware resource: GREEN
```

show cef ipv4 summary

To display a summary of the IPv4 Cisco Express Forwarding (CEF) table, use the **show cef ipv4 summary** command in XR EXEC mode.

show cef ipv4 summary [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Displays a summary of the IPv4 CEF table for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, this command displays a summary of the IPv4 CEF table for the node on which the command is issued.

Task ID

Task ID	Operations
cef	read

Examples

The following sample output is from the **show cef ipv4 summary** command:

```
RP/0/RP0/CPU0:router# show cef ipv4 summary
Router ID is
10
0
.0.0.0

IP CEF with switching (Table Version 0)

  Load balancing: L3
  Tableid 0xe0000000, Vrfid 0x60000000, Vrid 0x20000000, Flags 0x301
  Vrfname default, Refcount 367
  193 routes, 0 reresolve, 0 unresolved (0 old, 0 new), 13896 bytes
  204 load sharing elements, 51904 bytes, 154 references
  17 shared load sharing elements, 5536 bytes
  187 exclusive load sharing elements, 46368 bytes
  0 CEF route update drops, 175 revisions of existing leaves
  Resolution Timer: 15s
  0 prefixes modified in place
  0 deleted stale prefixes
  16 prefixes with label imposition, 51 prefixes with label information
Adjacency Table has 44 adjacencies
  1 incomplete adjacency
```

This table describes the significant fields shown in the display.

Table 12: show cef ipv4 summary Command Field Descriptions

Field	Description
Load balancing	Current load-balancing mode. The default value is L3.
Table Version	Version of the CEF table.
tableid	Table identification number.
vrfid	VPN routing and forwarding (VRF) identification (vrfid) number.
vrfname	VRF name.
vrid	Virtual router identification (vrid) number.
flags	Option value for the table
routes	Total number of routes.
reresolve	Total number of routes being reresolved.
unresolved (*x* old, *x* new)	Number of routes not yet resolved.
load sharing elements	Total number of internal load-sharing data structures.
bytes	Total memory used by internal load sharing data structures.
references	Total reference count of all internal load sharing data structures.
CEF resets	Number of CEF table resets.
revisions of existing leaves	Number of updates to existing prefixes.
Exponential (currently *x*s, peak *x*s)	Currently not used.
prefixes modified in place	Prefixes modified in place.
Adjacency Table has *x* adjacencies	Total number of adjacencies.
x incomplete adjacency	Total number of incomplete adjacencies.

show cef ipv4 unresolved

To display unresolved routes in the IPv4 Cisco Express Forwarding (CEF) table, use the **show cef ipv4 unresolved** command in XR EXEC mode.

show cef ipv4 unresolved [**detail**] [**hardware** {**egress** | **ingress**}] [**location** *node-id*]

Syntax Description

detail	(Optional) Displays detailed information unresolved routes listed in the IPv4 CEF table.
hardware	(Optional) Displays detailed information about hardware.
egress	(Optional) Displays egress packet switch exchange (PSE).
ingress	(Optional) Displays ingress packet switch exchange (PSE).
location *node-id*	(Optional) Displays the unresolved routes in the IPv4 CEF table for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, the output displays the unresolved routes for the node on which the command is issued.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output from the **show cef ipv4 unresolved** command when an unresolved route is detected:

```
RP/0/RP0/CPU0:router# show cef ipv4 unresolved

Prefix              Next Hop            Interface
10.3.3.3              102.2.2.2               ?
```

This table describes the significant fields shown in the display.

Table 13: show cef ipv4 unresolved Command Field Descriptions

Field	Description
Prefix	Prefix of the unresolved CEF.
Next Hop	Next hop of the unresolved CEF.
Interface	Next hop interface. A question mark (?) indicates that the interface has not been resolved.

show cef ipv6

To display the IPv6 Cisco Express Forwarding (CEF) table, use the **show cef ipv6** command in XR EXEC mode.

show cef] **ipv6** [*interface-type interface-number* | *ipv6-prefix/ prefix-length*] [**detail**] [**location***node-id*]

Syntax Description

interface-type interface-number	(Optional) IPv6 prefixes going through the specified next hop interface.
ipv6-prefix/prefix-length	(Optional) Longest prefix entry in the CEF table matching the specified IPv6 prefix and prefix length.
detail	(Optional) Displays detailed IPv6 CEF table information.
location *node-id*	(Optional) Displays the IPv6 CEF table for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 24.4.1	The command is enhanced to include additional details about Layer 2 IPv6 prefixes that resolve as nexthop Layer 3 prefixes.
Release 6.0	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, this command displays the IPv6 CEF table for the node on which the command is issued.

Task ID

Task ID	Operations
cef	read

Examples

The following sample output is from the **show cef ipv6** command:

```
RP/0/RP0/CPU0:router# show cef ipv6

::/0

::/128
  drop
::1/128
  loopback
66::4/128
  receive    Loopback0
2222::/64
  connected  tenGigE0/0/0/4
```

```
2222::1/128
  receive    tenGigE0/0/0/4
3333::/64
  connected  tenGigE0/0/0/3
3333::2/128
  receive    tenGigE0/0/0/3
5656::2/128
  recursive  fe80::3031:48ff:fe53:5533, tenGigE0/0/0/3
7777::/64
  connected  tenGigE0/0/0/0
7777::2/128
  receive    tenGigE0/0/0/0
9999::1/128
  recursive  fe80::205:5fff:fe1d:7600, tenGigE0/0/0/4
ff00::/8
  drop
ff02::1/128
  receive
ff02::2/128
  receive
ff02::5/128
  receive
ff02::6/128
  receive
ff02::1:ff00:0/104
  receive
```

This table describes the significant fields shown in the display.

Table 14: show cef ipv6 Command Field Descriptions

Field	Description
drop	Indicates that packets sent to the destination prefix are dropped.
loopback	Indicates that the prefix points to a loopback address. Packets sent to loopback addresses are dropped.
receive	Indicates that the prefix is configured on one of the router interfaces. Packets sent to those prefixes are received by the router.
connected	Indicates that the prefix points to a directly connected next-hop interface.
recursive	Indicates that the prefix is not directly connected but is reachable through the next-hop prefix displayed.

The following sample output is from the **show cef ipv6** with the **detail** keyword:

```
RP/0/RP0/CPU0:router# show cef ipv6 detail


::/0
  flags: source_rib
  Loadinfo owner: <this route>
  fast adj: glean
  path 1:
    flags     :
    next hop  : ::
    interface :
tenGigE/0/0/0
```

```
::/128
  flags: drop, source_fib
  Loadinfo owner: <this route>
  fast adj: drop
  path 1:
    flags     :
    next hop  : ::
    interface : <not specified>

::1/128
  flags: loopback, source_fib
  Loadinfo owner: <this route>
  fast adj: loopback
  path 1:
    flags     :
    next hop  : ::
    interface : <not specified>

66::4/128
  flags: receive, source_rib
  Loadinfo owner: <this route>
  fast adj: receive
  path 1:
    flags     : point-to-point
    next hop  : ::
    interface : Loopback0
```

This table describes the significant output fields shown in the display.

Table 15: show cef ipv6 detail Command Field Descriptions

Field	Description
flags:	Properties of the indicated prefix.
Loadinfo owner:	Owner of the Loadinfo used by the prefix for forwarding. The Loadinfo owner is the prefix that owns the array of pointers to adjacencies.
fast adj:	Cached adjacency used for forwarding.
path 1:	The following three items are displayed below path 1: • flags–Properties of the path. • next hop–Next-hop prefix if the packet is being forwarded. • interface–Next-hop interface if the packet is being forwarded.

In the following example, the IPv6 Layer 2 prefixes, which resolve as nexthop for Layer 3 prefixes are collapsed. This is indicated by the **collapsed** keyword in the output. The SRv6 SID lists indicate the different encapsulation layers or hierarchy.

```
Router#show cef ipv6 2001:DB8:A:B::1/64
Thu Jun  6 12:48:52.399 EDT
2001:DB8:A:B::1/64, version 8, SRv6 Headend, internal 0x1000001 0x0 (ptr 0x63851c98) [1],
0x1400 (0x63851da0), 0x0 (0x638b2128)
 Updated Jun  6 12:41:10.589
 Prefix Len 64, traffic index 0, precedence n/a, priority 0, encap-id 0x11deadbeef
  gateway array (0x61e1a798) reference count 1, flags 0x10, source rib (7), 0 backups
                [2 type 3 flags 0x40008501 (0x63853e38) ext 0x0 (0x0) (collapsed)]
```

```
 LW-LDI[type=3, refc=1, ptr=0x63851da0, sh-ldi=0x63853e38]
 gateway array update type-time 1 Jun  6 12:41:10.589
LDI Update time Jun  6 12:41:10.629
LW-LDI-TS Jun  6 12:41:10.629
Accounting: Disabled
  via 2001:DB8::1/128, 1 dependency, recursive [flags 0x3000000]
   path-idx 0 NHID 0x0 [0x63a2c098 0x0]
   next hop 2001:DB8::1/128 via  2001:DB8::1
   SRv6 H.Encaps.Red SID-list {2001:DB8:1:e002::}
     SRv6 H.Insert.Red SID-list {}
     SRv6 H.Insert.Red SID-list {bbbb:bbbb:3:: bbbb:bbbb:4::}
  via 2001:DB8::1/128, 1 dependency, recursive [flags 0x3000000]
   path-idx 1 NHID 0x0 [0x63a2c270 0x0]
   next hop 2001:DB8::1/128 via 2001:DB8::1
   SRv6 H.Encaps.Red SID-list {bbbb:bbbb:2:e002::}
      SRv6 H.Insert.Red SID-list {}

   Load distribution: 0 1 2 2 (refcount 2)

   Hash  OK  Interface                Address
   0     Y   UNKNOWN intf 0x00000013   10::2
   1     Y   UNKNOWN intf 0x00000014   20::2
   2     Y   UNKNOWN intf 0x00000013   10::2
   3     Y   UNKNOWN intf 0x00000013   10::2
```

show cef ipv6 adjacency

To display Cisco Express Forwarding (CEF) IPv6 adjacency status and configuration information, use the **show cef ipv6 adjacency** command in XR EXEC mode.

show cef ipv6 adjacency [*interface-type interface-path-id*] [**location** *node-id*] [**detail**] [**discard**] [**glean**] [**null**] [**punt**] [**remote**]

Syntax Description

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

interface- path-id	(Optional) Either a physical interface instance or a virtual interface instance:
	• Physical interface instance. Naming notation is *rack/slot/module/port* and a slash mark between values is required as part of the notation.
	  • *rack*: Chassis number of the rack.
	  • *slot*: Physical slot number of the line card.
	  • *module*: Module number. A physical layer interface module (PLIM) is always 0.
	  • *port*: Physical port number of the interface.
	Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RSP0) and the module is CPU0. Example: interface MgmtEth0/RSP0 /CPU0/0.
	• Virtual interface instance. Number range varies depending on interface type.
	For more information about the syntax for the router, use the question mark (?) online help function.

location *node-id*	(Optional) Displays detailed CEF information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
detail	(Optional) Displays the detailed adjacency information.
discard	(Optional) Filters out and displays only the discarded adjacency information.
glean	(Optional) Filters out and displays only the glean adjacency information.
null	(Optional) Filters out and displays only the null adjacency information.
punt	(Optional) Filters out and displays only the punt adjacency information.
remote	(Optional) Filters out and displays only the remote adjacency information.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, this command displays the CEF adjacency table for the node on which the command is issued.

Task ID

Task ID	Operations
cef	read

Examples

The following sample output is from the **show cef ipv6 adjacency** command:

```
RP/0/RP0/CPU0:router# show cef ipv6 adjacency

Display protocol is ipv6
Interface    Address                                          Type    Refcount

Te0/0/0/9                                                     special 2
             Interface: Te0/0/0/9 Type:  glean
             Interface Type: 0x1e, Base Flags: 0x220 (0x8a796038)
             Nhinfo PT: 0x8a796038, Idb PT: 0x8a3e09a0, If Handle: 0x8000088
             Dependent adj type: remote (0x8c34c238)
             Dependent adj intf: Te0/0/0/9
             Ancestor If Handle: 0x0
 Update time Dec 19 06:43:23.354


Te0/0/0/9    Prefix: 9::2/128                                 local   3
             Adjacency: PT:0x88155c18 9::2/128
             Interface: Te0/0/0/9
             NHID: 0x0
             MAC: 10.f3.11.25.39.5b.28.c7.ce.01.ec.20.86.dd
             Interface Type: 0x1e, Base Flags: 0x1 (0x8c39e238)
             Nhinfo PT: 0x8c39e238, Idb PT: 0x8a3e09a0, If Handle: 0x8000088
             Dependent adj type: remote (0x8c34c238)
             Dependent adj intf: Te0/0/0/9
             Ancestor If Handle: 0x0
 Update time Dec 19 06:44:49.548


Te0/0/0/9    Prefix: fe80::12f3:11ff:fe25:395b/128            local   3
             Adjacency: PT:0x881559c8 fe80::12f3:11ff:fe25:395b/128
             Interface: Te0/0/0/9
             NHID: 0x0
             MAC: 10.f3.11.25.39.5b.28.c7.ce.01.ec.20.86.dd
             Interface Type: 0x1e, Base Flags: 0x1 (0x8c39e568)
             Nhinfo PT: 0x8c39e568, Idb PT: 0x8a3e09a0, If Handle: 0x8000088
             Dependent adj type: remote (0x8c34c238)
             Dependent adj intf: Te0/0/0/9
             Ancestor If Handle: 0x0
 Update time Dec 19 06:44:59.553


Te0/0/0/8                                                     special 2
             Interface: Te0/0/0/8 Type:  glean
```

```
             Interface Type: 0x1e, Base Flags: 0x220 (0x8a795ea8)
             Nhinfo PT: 0x8a795ea8, Idb PT: 0x8a3e0920, If Handle: 0x8000080
             Dependent adj type: remote (0x8c34c0a0)
             Dependent adj intf: Te0/0/0/8
             Ancestor If Handle: 0x0
 Update time Dec 19 06:43:23.351


Te0/0/0/8    Prefix: 8::2/128                                local   3
             Adjacency: PT:0x88155e68 8::2/128
             Interface: Te0/0/0/8
             NHID: 0x0
             MAC: 10.f3.11.25.39.5a.28.c7.ce.01.ec.1f.86.dd
             Interface Type: 0x1e, Base Flags: 0x1 (0x8c39e0a0)
             Nhinfo PT: 0x8c39e0a0, Idb PT: 0x8a3e0920, If Handle: 0x8000080
             Dependent adj type: remote (0x8c34c0a0)
             Dependent adj intf: Te0/0/0/8
             Ancestor If Handle: 0x0
 Update time Dec 19 06:44:46.155


Te0/0/0/8    Prefix: fe80::12f3:11ff:fe25:395a/128           local   3
             Adjacency: PT:0x88155d40 fe80::12f3:11ff:fe25:395a/128
             Interface: Te0/0/0/8
             NHID: 0x0
             MAC: 10.f3.11.25.39.5a.28.c7.ce.01.ec.1f.86.dd
             Interface Type: 0x1e, Base Flags: 0x1 (0x8c39e3d0)
             Nhinfo PT: 0x8c39e3d0, Idb PT: 0x8a3e0920, If Handle: 0x8000080
             Dependent adj type: remote (0x8c34c0a0)
             Dependent adj intf: Te0/0/0/8
             Ancestor If Handle: 0x0
 Update time Dec 19 06:44:56.154
```

This is a sample output from the **show cef ipv6 adjacency remote detail** command:

```
RP/0/RP0/CPU0:router# show cef ipv6 adjacency remote detail location 0/RP0/CPU0

Display protocol is ipv6
Interface    Address                                         Type    Refcount

Te0/2/0/3    Ifhandle: 0x8000240                             remote  2
             Adjacency: PT:0xa1bed9e4
             Interface: Te0/2/0/3
             Interface Type: 0x0, Base Flags: 0x0 (0xa55f3114)
             Nhinfo PT: 0xa55f3114, Idb PT: 0xa2d850d8, If Handle: 0x8000240
             Ancestor If Handle: 0x0


tt103        Ifhandle: 0x120                                 remote  1
             no next-hop adj
             Interface: NULLIFHNDL
             tunnel adjacency
             Interface Type: 0x24, Base Flags: 0x200 (0xa61ddc30)
             Nhinfo PT: 0xa61ddc30, Idb PT: 0xa2d851d8, If Handle: 0x120
             Ancestor If Handle: 0x0


tt2993       Ifhandle: 0xf9a0                                remote  1
             no next-hop adj
             Interface: NULLIFHNDL
             tunnel adjacency
             Interface Type: 0x24, Base Flags: 0x200 (0xa65634f0)
             Nhinfo PT: 0xa65634f0, Idb PT: 0xa2d94a58, If Handle: 0xf9a0
```

```
                Ancestor If Handle: 0x0


tt2994          Ifhandle: 0xf9e0                                remote  1
                no next-hop adj
                Interface: NULLIFHNDL
                tunnel adjacency
                Interface Type: 0x24, Base Flags: 0x200 (0xa65641e0)
                Nhinfo PT: 0xa65641e0, Idb PT: 0xa2d94a98, If Handle: 0xf9e0
                Ancestor If Handle: 0x0


tt2995          Ifhandle: 0xfa20                                remote  1
                no next-hop adj
                Interface: NULLIFHNDL
                tunnel adjacency
                Interface Type: 0x24, Base Flags: 0x200 (0xa6564350)
                Nhinfo PT: 0xa6564350, Idb PT: 0xa2d94ad8, If Handle: 0xfa20
                Ancestor If Handle: 0x0
```

show cef ipv6 adjacency hardware

To display Cisco Express Forwarding (CEF) IPv6 adjacency hardware status and configuration information, use the **show cef ipv6 adjacency hardware** command in XR EXEC mode.

show cef ipv6 adjacency hardware {**egress** | **ingress**} [**detail** | **discard** | **drop** | **glean** | **location** *node-id* | **null** | **punt** | **remote**]

Syntax Description

egress	Displays information from the egress packet switch exchange (PSE) file.
ingress	Displays information from the ingress packet switch exchange (PSE) file.
detail	(Optional) Displays full details.
discard	(Optional) Displays the discard adjacency information.
drop	(Optional) Displays the drop adjacency information.
glean	(Optional) Displays the glean adjacency information.
location *node-id*	(Optional) Displays detailed CEF information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
null	(Optional) Displays the null adjacency information.
punt	(Optional) Displays the punt adjacency information.
remote	(Optional) Displays the remote adjacency information.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
cef	read

Examples

The following sample output is from the **show cef ipv6 adjacency hardware** command:

```
RP/0/RP0/CPU0:router# show cef ipv6 adjacency hardware egress
```

```
Display protocol is ipv6
Interface    Address                                          Type    Refcount

Te0/0/0/9                                                     special 2
             Interface: Te0/0/0/9 Type:  glean
             Interface Type: 0x1e, Base Flags: 0x220 (0x8a796038)
             Nhinfo PT: 0x8a796038, Idb PT: 0x8a3e09a0, If Handle: 0x8000088
             Dependent adj type: remote (0x8c34c238)
             Dependent adj intf: Te0/0/0/9
             Ancestor If Handle: 0x0
 Update time Dec 19 06:43:23.354

 Show-data Print at RPLC


RX H/W Result on NP:10 [Adj ptr:0x40 (BE)]:
Rx-Adj is NOT required on this platform

TX H/W Result for NP:10 (index: 0x186ac (BE)):

 Next Hop Data
 Next Hop Valid:         YES
 Next Hop Index:         100012
 Egress Next Hop IF:     100012
 Hw Next Hop Intf:       0
 HW Port:                0
 Next Hop Flags:         DISCARD PUNT
 Next Hop MAC:           0000.0000.0000



Te0/0/0/9    Prefix: 9::2/128                                 local   3
             Adjacency: PT:0x88155c18 9::2/128
             Interface: Te0/0/0/9
             NHID: 0x0
             MAC: 10.f3.11.25.39.5b.28.c7.ce.01.ec.20.86.dd
             Interface Type: 0x1e, Base Flags: 0x1 (0x8c39e238)
             Nhinfo PT: 0x8c39e238, Idb PT: 0x8a3e09a0, If Handle: 0x8000088
             Dependent adj type: remote (0x8c34c238)
             Dependent adj intf: Te0/0/0/9
             Ancestor If Handle: 0x0
 Update time Dec 19 06:44:49.548

 Show-data Print at RPLC


TX H/W Result for NP:0 (index: 0x186bd (BE)):

 Next Hop Data
 Next Hop Valid:         YES
 Next Hop Index:         100029
 Egress Next Hop IF:     100028
 Hw Next Hop Intf:       15
 HW Port:                10
 Next Hop Flags:         COMPLETE
 Next Hop MAC:           10f3.1125.395b

NHINDEX H/W Result for NP:0 (index: 0 (BE)):
NhIndex is NOT required on this platform

NHINDEX STATS: pkts 0, bytes 0 (all NPs combined, no stats)

RX H/W Result on NP:0 [Adj ptr:0x40 (BE)]:
Rx-Adj is NOT required on this platform
```

```
Te0/0/0/9    Prefix: fe80::12f3:11ff:fe25:395b/128           local   3
             Adjacency: PT:0x881559c8 fe80::12f3:11ff:fe25:395b/128
             Interface: Te0/0/0/9
             NHID: 0x0
             MAC: 10.f3.11.25.39.5b.28.c7.ce.01.ec.20.86.dd
             Interface Type: 0x1e, Base Flags: 0x1 (0x8c39e568)
             Nhinfo PT: 0x8c39e568, Idb PT: 0x8a3e09a0, If Handle: 0x8000088
             Dependent adj type: remote (0x8c34c238)
             Dependent adj intf: Te0/0/0/9
             Ancestor If Handle: 0x0
 Update time Dec 19 06:44:59.554

 Show-data Print at RPLC


TX H/W Result for NP:0 (index: 0x186bf (BE)):

 Next Hop Data
 Next Hop Valid:         YES
 Next Hop Index:         100031
 Egress Next Hop IF:     100030
 Hw Next Hop Intf:       15
 HW Port:                10
 Next Hop Flags:         COMPLETE
 Next Hop MAC:           10f3.1125.395b

NHINDEX H/W Result for NP:0 (index: 0 (BE)):
NhIndex is NOT required on this platform

NHINDEX STATS: pkts 0, bytes 0 (all NPs combined, no stats)

RX H/W Result on NP:0 [Adj ptr:0x40 (BE)]:
Rx-Adj is NOT required on this platform
```

show cef ipv6 drops

To display IPv6 Cisco Express Forwarding (CEF) table packet drop counters, use the **show cef ipv6 drops** command in XR EXEC mode.

show cefipv6 drops [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Displays IPv6 CEF table packet drop counters for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

A packet might be dropped by the IPv6 CEF table because of unresolved CEF entries, unsupported features, absence of route information, absence of adjacency information, or an IP checksum error.

If you do not specify a node with the **location** keyword and *node-id* argument, this command displays the packet drops for all nodes.

Note Because no hardware forwarding occurs on the route processor (RP), no packet drop information is displayed for that node.

The **show cef ipv6 drop** command output counters include CEF table packet drop counters for IPv4 and IPv6 packets.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output from the **show cef ipv6 drops** command:

```
RP/0/RP0/CPU0:router# show cef ipv6 drops location 0/RP0/CPU0

CEF Drop Statistics
Node: 0/RP0/CPU0
  Unresolved drops     packets :              0
  Unsupported drops    packets :              0
  Null0 drops          packets :              0
  No route drops       packets :              0
  No Adjacency drops   packets :              0
```

```
Checksum error drops packets :              0
RPF drops            packets :              0
RPF suppressed drops packets :              0
RP destined drops    packets :              0
Discard drops        packets :              0
GRE lookup drops     packets :              0
GRE processing drops packets :              0
LISP punt drops      packets :              0
LISP encap err drops packets :              0
LISP decap err drops packets :              0
```

Table 16: show cef ipv6 drops Command Field Descriptions

Field	Description
Unresolved drops	Drops due to unresolved routes.
Unsupported drops	Drops due to an unsupported feature.
Null0 drops	Drops to the Null0 interface.
No route drops	Number of packets dropped because there were no routes to the destination.
No Adjacency drops	Number of packets dropped because there were no adjacencies established.
Checksum error drops	Drops due to IPv6 checksum error.
RPF drops	Drops due to IPv6 unicast RPF[4].
RPF suppressed drops	Drops suppressed due to IPv6 unicast RPF.
RP destined drops	Drops destined for the router.
Discard drops	Drops those were discarded
GRE lookup drops	GRE packets dropped during GRE Lookup.
GRE processing drops	GRE packets dropped during GRE Processing.
LISP punt drops	LISP packets dropped during software processing of the packets.
LISP encap err drops	LISP encap packets dropped due to errors.
LISP decap err drops	LISP Decap packets dropped due to errors.

[4] RPF = Reverse Path Forwarding

show cef ipv6 exact-route

To display the path an IPv6 flow comprising a source and destination address would take, use the **show cef ipv6 exact-route** command in XR EXEC mode.

show cef ipv6 exact-route {*source-address destination-address* } [**protocol***protocol name*] [**source-port***source-port*] [**destination-port***destination-port*] [**ingress-interface***type interface-path-id*] [**policy-class** *value*] [**detail | location** *node-id]*]

Syntax Description

source-address	The IPv6 source address in x:x::x format.
destination-address	The IPv6 destination address in x:x::x format.
protocol *protocol name*	(Optional) Displays the specified protocol for the route.
source-port *source-port*	(Optional) Sets the UDP source port. The range is from 0 to 65535.
destination-port *destination-port*	(Optional) Sets the UDP destination port. The range is from 0 to 65535.
ingress-interface	(Optional) Sets the ingress interface.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
policy-class *value*	(Optional) Displays the class for the policy-based tunnel selection. The range for the tunnel policy class value is from 1 to 7.
detail	(Optional) Displays full CEF entry information.

location *node-id*	(Optional) Displays the IPv6 CEF table for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

If the Layer 4 information is enabled, the source-port, destination-port, protocol, and ingress-interface fields are required. Otherwise, the output of the **show cef ipv6 exact-route** command is not correct.

Task ID

Task ID	Operations
cef	read

Examples

The following sample output is from the **show cef ipv6 exact-route** command:

```
RP/0/RP0/CPU0:router# show cef ipv6 exact-route 222::2 9999::6751 location

0/RP0/CPU0 source address: 222::2 destination address: 9999::6751
interface : tenGigE 0/0/0/3 non local interface
```

show cef ipv6 exceptions

To display IPv6 Cisco Express Forwarding (CEF) exception packet counters, use the **show cef ipv6 exceptions** command in XR EXEC mode.

show cef ipv6 exceptions [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Displays IPv6 CEF exception packet counters for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

CEF exception packets are those packets that have been sent from the hardware to the software because they require additional handling. The types of IPv6 CEF exception packets are displayed in the output of **show cef ipv6 exceptions**.

If you do not specify a node with **location** keyword and *node-id* argument, this command displays IPv6 CEF exception packet counters for all nodes.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output from the **show cef ipv6 exceptions** command:

```
RP/0/RP0/CPU0:router# show cef ipv6 exceptions location 0/RP0/CPU0

CEF Exception Statistics
Node: 0/RP0/CPU0
  Slow encap  packets :              0
  Unsupported packets :              0
  Redirect    packets :              0
  Receive     packets :              0
  Broadcast   packets :              0
  IP options  packets :              0
  TTL expired packets :              0
  Fragmented  packets :              0
```

This table describes the significant fields shown in the display.

Table 17: show cef ipv6 exceptions Command Field Descriptions

Field	Description
Slow encap	Number of packets requiring special processing during encapsulation.
Redirect	Number of ICMP[5] redirect messages sent.
Receive	Number of packets destined to the router.
Broadcast	Number of broadcasts received.
IP options	Number of IP option packets.
TTL expired	Number of packets with expired TTLs[6].
Fragmented	Number of packets that have been fragmented.

[5] ICMP = internet control message protocol
[6] TTL = time to live

show cef ipv6 hardware

To display Cisco Express Forwarding (CEF) IPv6 hardware status and configuration information, use the **show cef ipv6 hardware** command in XR EXEC mode.

show cef ipv6 hardware {**egress** | **ingress** [**detail** | **location** *node-id*]}

Syntax Description

egress	Displays information from the egress packet switch exchange (PSE) file.
ingress	Displays information from the ingress packet switch exchange (PSE) file.
detail	(Optional) Displays full details.
location *node-id*	(Optional) Displays detailed CEF information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
cef	read

Examples

The following sample output displays the full details from the **show cef ipv6 hardware** command:

```
RP/0/RP0/CPU0:router# show cef ipv6 hardware egress detail

::/0, version 0, proxy default, default route handler, drop adjacency, internal
 Prefix Len 0, traffic index 0, precedence routine (0)
  gateway array (0x0) reference count 1, flags 0x4000, source 4,
                [0 type 3 flags 0x109000 (0x7895114c) ext 0x0 (0x0)]
  LW-LDI[type=3, refc=1, ptr=0x78a7d0dc, sh-ldi=0x7895114c]
   via point2point, 0 dependencies, weight 0, class 0
    next hop point2point
     drop adjacency


    Load distribution: 0 (refcount 0)

    Hash  OK  Interface                 Address
    0     Y   Unknown                   drop
ff02::/16, version 0, receive
```

```
  Prefix Len 16
ff02::2/128, version 0, receive
  Prefix Len 128
ff02::1:ff00:0/104, version 0, receive
  Prefix Len 104
```

show cef ipv6 interface

To display IPv6 Cisco Express Forwarding (CEF)-related information for an interface, use the **show cef ipv6 interface** command in XR EXEC mode.

show cef ipv6 interface *type interface-path-id* [**detail**] [**location** *node-id*] **[rpf-drop]**

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
detail	(Optional) Displays detailed CEF information for all the interfaces on the node in which the command is issued.
location *node-id*	(Optional) Displays IPv4 CEF-related information for an interface. The *node-id* argument is entered in the *rack/slot/module* notation.
rpf-drop	(Optional) Displays information about the drops due to IPv6 unicast RPF.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, the **show cef ipv6 interface** command displays the CEF-related information for the interface on the route processor.

Task ID

Task ID	Operations
cef	read

Examples

The following sample output is from the **show cef ipv6 interface** command:

```
RP/0/RP0/CPU0:router# show cef ipv6 interface

fib_show_interface
created item name: 1000/protocol/1/vrf/default/interface-info/1/
Bundle-Ether5.2 is down if_handle 0x0800002c if_type IFT_VLAN_SUBIF(0x19)
```

```
     idb info 0x898ecfa0 flags 0x48001 ext 0x8c38b488 flags 0x10
     Vrf Local Info (0x0)
  Interface last modified Dec 15, 2015 16:15:28, modify
  Reference count 1   Next-Hop Count 0
  Forwarding is disabled
  ICMP redirects are never sent
  ICMP unreachables are enabled
  Protocol MTU 9202, TableId 0xe0800000(0x8a1ce6c8)
  Protocol Reference count 1
  Primary IPV6 local address NOT PRESENT
Bundle-Ether5.1 is down if_handle 0x08000024 if_type IFT_VLAN_SUBIF(0x19)
     idb info 0x898ecf20 flags 0x48001 ext 0x8c38b338 flags 0x10
     Vrf Local Info (0x0)
  Interface last modified Dec 15, 2015 16:15:28, modify
  Reference count 1   Next-Hop Count 0
  Forwarding is disabled
  ICMP redirects are never sent
  ICMP unreachables are enabled
  Protocol MTU 9202, TableId 0xe0800000(0x8a1ce6c8)
  Protocol Reference count 1
  Primary IPV6 local address NOT PRESENT
Loopback0 is up if_handle 0x0800001c if_type IFT_LOOPBACK(0x10)
     idb info 0x898ecda0 flags 0x8061 ext 0x0
     Vrf Local Info (0x0)
  Interface last modified Dec 14, 2015 17:24:58, modify
  Interface is marked as point to point interface
  Interface is marked as loopback interface
  Reference count 1   Next-Hop Count 0
  Protocol Reference count 0
  Protocol ipv6 not configured or enabled on this card
  Primary IPV6 local address NOT PRESENT
Bundle-Ether5 is down if_handle 0x08000014 if_type IFT_ETHERBUNDLE(0x1c)
     idb info 0x898ecd20 flags 0x48001 ext 0x8c38b1e8 flags 0x10
     Vrf Local Info (0x0)
  Interface last modified Dec 15, 2015 16:15:28, modify
  Reference count 1   Next-Hop Count 0
  Forwarding is disabled
  ICMP redirects are never sent
  ICMP unreachables are enabled
  Protocol MTU 9202, TableId 0xe0800000(0x8a1ce6c8)
  Protocol Reference count 1
  Primary IPV6 local address NOT PRESENT
TenGigE0/0/0/79 is down if_handle 0x080002b8 if_type IFT_TENGETHERNET(0x1e)
     idb info 0x898ecca0 flags 0x8001 ext 0x0
     Vrf Local Info (0x0)
  Interface last modified Dec 14, 2015 17:24:58, modify
  Reference count 1   Next-Hop Count 0
  Protocol Reference count 0
  Protocol ipv6 not configured or enabled on this card
  Primary IPV6 local address NOT PRESENT
TenGigE0/0/0/78 is down if_handle 0x080002b0 if_type IFT_TENGETHERNET(0x1e)
     idb info 0x898ecc20 flags 0x8001 ext 0x0
     Vrf Local Info (0x0)
  Interface last modified Dec 14, 2015 17:24:58, modify
  Reference count 1   Next-Hop Count 0
  Protocol Reference count 0
  Protocol ipv6 not configured or enabled on this card
  Primary IPV6 local address NOT PRESENT
TenGigE0/0/0/77 is down if_handle 0x080002a8 if_type IFT_TENGETHERNET(0x1e)
     idb info 0x898ecba0 flags 0x8001 ext 0x0
     Vrf Local Info (0x0)
  Interface last modified Dec 14, 2015 17:24:58, modify
  Reference count 1   Next-Hop Count 0
  Protocol Reference count 0
```

```
Protocol ipv6 not configured or enabled on this card
Primary IPV6 local address NOT PRESENT
```

show cef ipv6 resource

To display the IPv6 nonrecursive prefix entries in the IPv6 Cisco Express Forwarding (CEF) table, use the **show cef ipv6 resource** command in XR EXEC mode.

show cef ipv6 resource [**detail**] [**hardware** {**egress** | **ingress**}] [**location** *node-id*]

Syntax Description

detail	(Optional) Displays detailed information resources listed in the IPv6 CEF table.
hardware	(Optional) Displays Cisco Express Forwarding (CEF) IPv6 hardware status and configuration information.
egress	(Optional) Displays information from the egress packet switch exchange (PSE) file.
ingress	(Optional) Displays information from the ingress packet switch exchange (PSE) file.
location *node-id*	(Optional) Displays the IPv6 resource entries in the IPv6 CEF table for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, the output displays the IPv6 CEF nonrecursive routes for the node on which the command is issued.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output from the **show cef ipv6 resource** command:

```
RP/0/RP0/CPU0:router# show cef ipv6 resource

CEF resource availability summary state: GREEN
  ipv4 shared memory resource: GREEN
  ipv6 shared memory resource: GREEN
  mpls shared memory resource: GREEN
  common shared memory resource: GREEN
  TABLE hardware resource: GREEN
  LEAF hardware resource: GREEN
  LOADINFO hardware resource: GREEN
  NHINFO hardware resource: GREEN
  LABEL_INFO hardware resource: GREEN
  IDB hardware resource: GREEN
```

```
FRR_NHINFO hardware resource: GREEN
LDSH_ARRAY hardware resource: GREEN
RSRC_MON hardware resource: GREEN
```

show cef ipv6 summary

To display a summary of the IPv6 Cisco Express Forwarding (CEF) table, use the **show cef ipv6 summary** command in XR EXEC mode.

show cef ipv6 summary [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Displays a summary of the IPv6 CEF table for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, this command displays a summary of the IPv6 CEF table for the node on which the command is issued.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output from the **show cef ipv6 summary** command:

```
RP/0/RP0/CPU0:router# show cef ipv6 summary

IP CEF with switching (Table Version 0)

  Load balancing: L3
  Tableid 0xe0800000, Vrfid 0x60000000, Vrid 0x20000000, Flags 0x301
  Vrfname default, Refcount 12
  4 routes, 0 reresolve, 0 unresolved (0 old, 0 new), 288 bytes
  0 load sharing elements, 0 bytes, 0 references
  0 shared load sharing elements, 0 bytes
  0 exclusive load sharing elements, 0 bytes
  0 CEF route update drops, 0 revisions of existing leaves
  Resolution Timer: 15s
  0 prefixes modified in place
  0 deleted stale prefixes
  0 prefixes with label imposition, 0 prefixes with label information
Adjacency Table has 44 adjacencies
  1 incomplete adjacency
```

This table describes the significant fields shown in the display.

Table 18: show cef ipv6 summary Command Field Descriptions

Field	Description
Load balancing	Current load-balancing mode. The default value is L3.
Table Version	Version of the CEF table.
routes	Total number of routes.
unresolved (*x* old, *x* new)	Number of routes not yet resolved.
load sharing elements	Total number of internal load-sharing data structures.
bytes	Total memory used by internal load sharing data structures.
references	Total reference count of all internal load sharing data structures.
CEF resets	Number of CEF table resets.
revisions of existing leaves	Number of updates to existing prefixes.
Exponential (currently *x*s, peak *x*s)	Currently not used.
prefixes modified in place	Prefixes modified in place.
Router ID	Router identification.
Adjacency Table has *x* adjacencies	Total number of adjacencies.
x incomplete adjacency	Total number of incomplete adjacencies.

show cef ipv6 unresolved

To display the unresolved routes in the IPv6 Cisco Express Forwarding (CEF) table, use the **show cef ipv6 unresolved** command in XR EXEC mode.

show cef ipv6 unresolved [**detail**] [**hardware** {**egress** | **ingress**}] [**location** *node-id*]

Syntax Description

detail	(Optional) Displays full details.
hardware	(Optional) Displays Cisco Express Forwarding (CEF) IPv6 hardware status and configuration information.
egress	Displays information from the egress packet switch exchange (PSE) file.
ingress	Displays information from the ingress packet switch exchange (PSE) file.
location *node-id*	(Optional) Displays detailed CEF information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, this command displays the unresolved routes for the node on which the command is issued.

Task ID

Task ID	Operations
cef	read

Examples

This following is sample output from **show cef ipv6 unresolved** command when an unresolved route is detected:

```
RP/0/RP0/CPU0:router# show cef ipv6 unresolved

9999::/64
  unresolved
```

This table describes the significant fields shown in the display.

Table 19: show cef ipv6 unresolved Command Field Descriptions

Field	Description
xxxx::/*xx*	Detected unresolved route.

show cef mpls adjacency

To display the Multiprotocol Label Switching (MPLS) adjacency table, use the **show cef mpls adjacency** command in XR EXEC mode.

show cef mpls adjacency [*interface-type interface-path-id*] [**detail** | **discard** | **drop** | **glean** | **null** | **punt** | **remote**] [**location** *node-id*]

Syntax Description

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

interface- path-id	(Optional) Either a physical interface instance or a virtual interface instance:
	• Physical interface instance. Naming notation is *rack/slot/module/port* and a slash mark between values is required as part of the notation.
	  • *rack*: Chassis number of the rack.
	  • *slot*: Physical slot number of the line card.
	  • *module*: Module number. A physical layer interface module (PLIM) is always 0.
	  • *port*: Physical port number of the interface.
	Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RSP0) and the module is CPU0. Example: interface MgmtEth0/RSP0 /CPU0/0.
	• Virtual interface instance. Number range varies depending on interface type.
	For more information about the syntax for the router, use the question mark (?) online help function.

detail	(Optional) Displays full details.
discard	(Optional) Displays the discard adjacency information.
drop	(Optional) Displays the drop adjacency information.
glean	(Optional) Displays the glean adjacency information.
null	(Optional) Displays the null adjacency information.
punt	(Optional) Displays the punt adjacency information.
remote	(Optional) Displays the remote adjacency information.
location *node-id*	(Optional) Displays detailed CEF information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, the **show cef mpls adjacency** command displays the MPLS adjacency table for the node in which the command is issued.

Task ID

Task ID	Operations
cef	read

Examples

This following is sample output from **show cef mpls adjacency** command:

```
RP/0/RP0/CPU0:router# show cef mpls adjacency hardware egress

Display protocol is mpls
Interface    Address                                          Type    Refcount

Te0/0/0/11   Prefix: 79.0.0.2/32                              local   5
             Adjacency: PT:0x894d40c0 79.0.0.2/32
             Interface: Te0/0/0/11
             NHID: 0x0
             MAC: 6c.9c.ed.28.8b.71.28.c7.ce.01.f0.4f.88.47
             Interface Type: 0x1e, Base Flags: 0x1 (0x8bec8230)
             Nhinfo PT: 0x8bec8230, Idb PT: 0x899f6a20, If Handle: 0x8000090
             Dependent adj type: remote (0x8be85230)
             Dependent adj intf: Te0/0/0/11
             Ancestor If Handle: 0x0
 Update time Dec 17 09:44:45.779

 Show-data Print at RPLC


TX H/W Result for NP:0 (index: 0x186bc (BE)):

 Next Hop Data
 Next Hop Valid:         YES
 Next Hop Index:         100028
 Egress Next Hop IF:     100028
 Hw Next Hop Intf:       17
 HW Port:                12
 Next Hop Flags:         COMPLETE
 Next Hop MAC:           6c9c.ed28.8b71

NHINDEX H/W Result for NP:0 (index: 0 (BE)):
NhIndex is NOT required on this platform

NHINDEX STATS: pkts 0, bytes 0 (no stats)

RX H/W Result on NP:0 [Adj ptr:0x40 (BE)]:
Rx-Adj is NOT required on this platform
```

show cef mpls adjacency hardware

To display the Multiprotocol Label Switching (MPLS) adjacency hardware status and configuration information, use the **show cef mpls adjacency hardware** command in XR EXEC mode.

show cef mpls adjacency hardware {**egress** | **ingress**} [**detail** | **discard** | **drop** | **glean** | **location** *node-id* | **null** | **punt** | **remote**]

Syntax Description

egress	Displays information from the egress packet switch exchange (PSE) file.
ingress	Displays information from the ingress packet switch exchange (PSE) file.
detail	(Optional) Displays full details.
discard	(Optional) Displays the discard adjacency information.
drop	(Optional) Displays the drop adjacency information.
glean	(Optional) Displays the glean adjacency information.
location *node-id*	(Optional) Displays detailed CEF information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
null	(Optional) Displays the null adjacency information.
punt	(Optional) Displays the punt adjacency information.
remote	(Optional) Displays the remote adjacency information.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
cef	read

Examples

This following is sample output from **show cef mpls adjacency hardware** command:

```
RP/0/RP0/CPU0:router# show cef mpls adjacency hardware egress

Display protocol is mpls
```

```
Interface    Address                                          Type    Refcount

Te0/0/0/11   Prefix: 79.0.0.2/32                             local   5
             Adjacency: PT:0x894d40c0 79.0.0.2/32
             Interface: Te0/0/0/11
             NHID: 0x0
             MAC: 6c.9c.ed.28.8b.71.28.c7.ce.01.f0.4f.88.47
             Interface Type: 0x1e, Base Flags: 0x1 (0x8bec8230)
             Nhinfo PT: 0x8bec8230, Idb PT: 0x899f6a20, If Handle: 0x8000090
             Dependent adj type: remote (0x8be85230)
             Dependent adj intf: Te0/0/0/11
             Ancestor If Handle: 0x0
 Update time Dec 17 09:44:45.779

 Show-data Print at RPLC


TX H/W Result for NP:0 (index: 0x186bc (BE)):

 Next Hop Data
 Next Hop Valid:         YES
 Next Hop Index:         100028
 Egress Next Hop IF:     100028
 Hw Next Hop Intf:       17
 HW Port:                12
 Next Hop Flags:         COMPLETE
 Next Hop MAC:           6c9c.ed28.8b71

NHINDEX H/W Result for NP:0 (index: 0 (BE)):
NhIndex is NOT required on this platform

NHINDEX STATS: pkts 0, bytes 0 (no stats)

RX H/W Result on NP:0 [Adj ptr:0x40 (BE)]:
Rx-Adj is NOT required on this platform
```

show cef mpls interface

To display the Multiprotocol Label Switching (MPLS) Cisco Express Forwarding (CEF)-related information for an interface, use the **show cef mpls interface** command in XR EXEC mode.

show cef mpls interface *type interface-path-id* [**detail**] [**location** *node-id*]

Syntax Description

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

in terface-path-id	Either a physical interface instance or a virtual interface instance as follows:
	• Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation.
	  • *rack*: Chassis number of the rack.
	  • *slot*: Physical slot number of the modular services card or line card.
	  • *module*: Module number. A physical layer interface module (PLIM) is always 0.
	  • *port*: Physical port number of the interface.
	Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RSP0) and the module is CPU0. Example: interface MgmtEth0/ RSP0
	• Virtual interface instance. Number range varies depending on interface type.
	For more information about the syntax for the router, use the question mark (?) online help function.

detail	(Optional) Displays detailed CEF information for all the interfaces on the node in which the command is issued.
location *node-id*	(Optional) Displays IPv4 CEF-related information for an interface. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, the **show cef mpls interface** command displays the CEF-related information for the interface on the route processor.

Task ID

Task ID	Operations
cef	read

Examples

The following sample output is from the **show cef mpls interface** command:

```
RP/0/RP0/CPU0:router# show cef mpls interface

fib_show_interface
Loopback0 is up if_handle 0x08000014 if_type IFT_LOOPBACK(0x10)
     idb info 0x899f78a0 flags 0x8061 ext 0x0
     Vrf Local Info (0x0)
  Interface last modified Dec 17, 2015 09:42:15, create
  Interface is marked as point to point interface
  Interface is marked as loopback interface
  Reference count 1       Next-Hop Count 0
  Protocol Reference count 0
  Protocol mpls not configured or enabled on this card
mpls_v6_item_name: 1000/protocol/1/vrf/default/interface-info/2/8000090
TenGigE0/0/0/11 is up if_handle 0x08000090 if_type IFT_TENGETHERNET(0x1e)
     idb info 0x899f6a20 flags 0x8001 ext 0x8bf0b098 flags 0x50
     Vrf Local Info (0x0)
  Interface last modified Dec 17, 2015 09:42:12, create
  Reference count 1       Next-Hop Count 2
  Forwarding is enabled
  Protocol MTU 1500, TableId 0(0x8a287098)
  Protocol Reference count 2
TenGigE0/0/0/1 is up if_handle 0x08000040 if_type IFT_TENGETHERNET(0x1e)
     idb info 0x899f6520 flags 0x8001 ext 0x0
     Vrf Local Info (0x0)
  Interface last modified Dec 17, 2015 09:42:12, create
  Reference count 1       Next-Hop Count 0
  Protocol Reference count 0
  Protocol mpls not configured or enabled on this card
Null0 is up if_handle 0x0800000c if_type IFT_NULL(0x11)
     idb info 0x899f61a0 flags 0x8061 ext 0x0
     Vrf Local Info (0x0)
  Interface last modified Dec 17, 2015 09:41:51, create
  Interface is marked as point to point interface
  Interface is marked as nullidb
  Reference count 1       Next-Hop Count 0
  Protocol Reference count 0
  Protocol mpls not configured or enabled on this card
FINT0/RP0/CPU0 is up if_handle 0x08000010 if_type IFT_FINT_INTF(0x1b)
     idb info 0x899f6120 flags 0x8021 ext 0x0
     Vrf Local Info (0x0)
  Interface last modified Dec 17, 2015 09:41:51, create
  Interface is marked as point to point interface
  Reference count 1       Next-Hop Count 0
  Protocol Reference count 0
  Protocol mpls not configured or enabled on this card
```

show cef mpls unresolved

To display the Multiprotocol Label Switching (MPLS) unresolved routes, use the **show cef mpls unresolved** command in XR EXEC mode.

show cef mpls unresolved [**detail**] [**location** *node-id*]

Syntax Description

detail	(Optional) Displays detailed adjacency information, including Layer 2 information.
location *node-id*	(Optional) Displays detailed CEF information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
cef	read

Examples

The following sample output is from the **show cef mpls unresolved** command:

```
RP/0/RP0/CPU0:router# show cef mpls unresolved

Label/EOS           Next Hop            Interface
20001/0
20001/1
```

This table describes the significant fields shown in the display.

Table 20: show cef mpls unresolved Command Field Descriptions

Field	Description
Label/EOS	MPLS forwarding label/End of Stack (EOS) bit.
Next Hop	Next hop of the prefix.
Interface	Interface associated with the prefix.

show cef summary

To display summary information for the Cisco Express Forwarding (CEF) table, use the **show cef summary** command in XR EXEC mode.

show cef summary [**location** {*node-id* | **all**}]

Syntax Description

location *node-id*	(Optional) Displays detailed CEF information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
all	(Optional) Displays all locations.

Command Default

The **show cef summary** command assumes the IPv4 CEF table and the active RP node as the location.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
cef	read

Examples

The following sample output is from the **show cef summary** command.

```
RP/0/RP0/CPU0:router# show cef summary location 0/RP0/CPU0

Router ID is 10.1.1.1

IP CEF with switching (Table Version 0) for node0_1_CPU0

  Load balancing: L3
  Tableid 0xe0000000, Vrfid 0x60000000, Vrid 0x20000000, Flags 0x301
  Vrfname default, Refcount 318
  170 routes, 0 reresolve, 0 unresolved (0 old, 0 new), 12240 bytes
  183 load sharing elements, 57292 bytes, 184 references
  19 shared load sharing elements, 7036 bytes
  164 exclusive load sharing elements, 50256 bytes
  0 CEF route update drops, 10 revisions of existing leaves
  Resolution Timer: 15s
  0 prefixes modified in place
  0 deleted stale prefixes
  21 prefixes with label imposition, 60 prefixes with label information
Adjacency Table has 49 adjacencies
  25 incomplete adjacencies
```

This table describes the significant fields shown in the display.

Table 21: show cef summary Command Field Descriptions

Field	Description
Load balancing	Current load-balancing mode. The default value is L3.
Table Version	Version of the CEF table.
tableid	Table identification number.
vrfname	VRF name.
flags	Option value for the table
routes	Total number of routes.
reresolve	Total number of routes being reresolved.
unresolved (*x* old, *x* new)	Number of routes not yet resolved.
load sharing elements	Total number of internal load-sharing data structures.
bytes	Total memory used by internal load sharing data structures.
references	Total reference count of all internal load sharing data structures.
CEF resets	Number of CEF table resets.
revisions of existing leaves	Number of updates to existing prefixes.
Exponential (currently *x*s, peak *x*s)	Currently not used.
prefixes modified in place	Prefixes modified in place.
Adjacency Table has *x* adjacencies	Total number of adjacencies.
x incomplete adjacency	Total number of incomplete adjacencies.



DHCP Commands

This chapter describes the Cisco IOS XR software commands used to configure and monitor Dynamic Host Configuration Protocol (DHCP) features.

For detailed information about DHCP concepts, configuration tasks, and examples, refer to the *IP Addresses and Services Configuration Guide for Cisco NCS 5000 Series Routers*.

- clear dhcp ipv4 client, on page 197
- clear dhcp ipv4 server binding, on page 198
- clear dhcp ipv4 server statistics, on page 199
- clear dhcp ipv6 proxy binding, on page 200
- clear dhcp ipv6 relay binding, on page 201
- clear dhcp ipv6 relay statistics, on page 203
- client-mac-mismatch, on page 204
- database (DHCPv6 Binding), on page 205
- default-router, on page 207
- dhcp ipv4 , on page 208
- dhcp ipv6, on page 209
- dns-server, on page 210
- domain-name, on page 211
- duplicate-mac-allowed, on page 212
- giaddr policy, on page 214
- helper-address, on page 216
- helper-address (ipv6), on page 218
- interface (DHCP), on page 220
- lease (DHCPv4 Server), on page 222
- limit lease, on page 223
- netbios-name-server, on page 224
- netbios-node-type, on page 225
- pool, on page 226
- profile (DHCP), on page 228
- relay information check , on page 230
- relay information option , on page 232
- relay information option allow-untrusted , on page 234
- subnet-mask, on page 236
- show dhcp ipv4 client, on page 237

- show dhcp ipv4 relay profile, on page 239
- show dhcp ipv4 relay profile name, on page 240
- show dhcp ipv4 relay statistics, on page 241
- show dhcp ipv4 server binding, on page 243
- show dhcp ipv4 server profile, on page 245
- show dhcp ipv4 server statistics, on page 246
- show dhcp ipv6 relay binding, on page 248
- show dhcp ipv6 relay statistics, on page 250
- show tech support dhcp ipv4 client, on page 252
- show dhcp vrf ipv4 server statistics, on page 254
- trust relay-reply, on page 256

clear dhcp ipv4 client

To clear the DHCP client binding information configured on a given interface and set the binding information again, use the **clear dhcp ipv4 client** command in XR EXEC mode.

clear dhcp ipv4 client *interface-name interface-number*

Syntax Description

interface-name	Specifies DHCP IPv4 client enabled interface name.
interface-number	Specifies DHCP IPv4 client enabled interface number.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

Use the **clear dhcp ipv4 client** command to clear the DHCP client binding information for the specified interface.

Task ID

Task ID	Operations
IP-Services	Execution

Examples

The following example shows how to clear the DHCP client binding information:

```
Router# clear dhcp ipv4 client mgmtEth 0/0/CPU0/0
Fri Jun  6 08:24:14.558 UTC
RP/0/0/CPU0:ios#show dhcp ipv4 client
Fri Jun  6 08:24:17.377 UTC

    Interface name         IP Address      Binding State         Lease Time Rem
---------------------    ------------    ---------------    ----------------------
MgmtEth0/0/CPU0/0          11.11.11.5       BOUND             3598 secs (00:59:58)

RP/0/0/CPU0:ios#show dhcp ipv4 client mgmtEth 0/0/CPU0/0 statistics
Fri Jun  6 08:24:19.397 UTC

Client Interface name           : MgmtEth0/0/CPU0/0
-------------------------------------------------
     CLIENT COUNTER(s)          |        VALUE
-------------------------------------------------
Num discovers sent              :          1
Num requests sent               :          1
Num releases sent               :          1
Num offers received             :          1
Num acks received               :          1
-------------------------------------------------
```

clear dhcp ipv4 server binding

To clear all client bindings in server, use the **clear dhcp ipv4 server binding** command in XR EXEC mode.

clear dhcp ipv4 server binding [**location** *node-ID*] [**interface** *type interface-path-ID*] [**mac-address** *address*]

Syntax Description

location *node-ID*	Clears detailed client binding information for a specified node.
interface *type interface-path-ID*	Clears client binding by interface. Specifies the interface type. For more information, use the question mark (?) online help function. Physical interface or virtual interface. Use the show interfaces command to see a list of all interfaces currently configured on the router. **Note** For more information about the syntax for the router, use the question mark (?) online help function.
mac-address *address*	Clears detailed client binding information per mac-address.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ip-services	execute

Example

This is a sample output from the **clear dhcp ipv4 server binding** command:

```
Router# clear dhcp ipv4 server binding
```

Related Commands

Command	Description
clear dhcp ipv4 server statistics, on page 199	Clears DHCP server statistics.

clear dhcp ipv4 server statistics

To clear DHCP server statistics, use the **clear dhcp ipv4 server statistics** command in XR EXEC mode.

clear dhcp ipv4 server statistics [[**raw** [**all**] [**location** *node-ID*]]

Syntax Description

raw	Clears debug statistics.
all	Clears debug statistics for base mode.
include-zeroes	Clears debug statistics that are zero.
location *node-ID*	Clears DHCP server statistics information for a specified node.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ip-services	execute
root-system	read, write

Example

This is a sample output from the **clear dhcp ipv4 server statistics** command:

```
Router# clear dhcp ipv4 server statistics
```

Related Commands

Command	Description
clear dhcp ipv4 server binding, on page 198	Clears all client bindings in server.

clear dhcp ipv6 proxy binding

To clear Dynamic Host Configuration Protocol (DHCP) relay bindings for prefix delegation, use the **clear dhcp ipv6 proxy binding** command in XR EXEC mode.

clear dhcp ipv6 proxy binding {*client-duid* | *interface* | *location*}

Syntax Description

client-duid	Specifies the DHCP unique identifier.
interface	Specifies the interface.
location	Specifies the node location.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ip-services	execute

Example

This is a sample output from the **clear dhcp ipv6 proxy binding** command:

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

clear dhcp ipv6 relay binding

To clear DHCPv6 relay binding, use the **clear dhcp ipv6 relay binding** command in XR EXEC mode.

clear dhcp ipv6 relay binding [**client-duid** *client-duid-number*] [**interface** *type interface-path-id*] [**vrf** *vrf-name*] [**location** *node-id*]

Syntax Description

client-duid *client-duid-number*	(Optional) Clears DHCPv6 relay client binding information. The argument *client-duid-number* is the client's DHCP Unique Identifier (DUID) number. **Note** Use the **show dhcp ipv6 relay binding** command to see the client DUID number.
interface *type interfac-path-id*	(Optional) Clears DHCPv6 relay client binding information for an interface. Specifies a physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router.
vrf *vrf-name*	(Optional) Clears DHCPv6 relay client binding information for a VPN routing and forwarding (VRF) instance.
location *node-id*	(Optional) Clears DHCPv6 relay client binding information for a specified node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

None.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ip-services	execute
root-system	read, write

This example shows how to clear DHCPv6 relay binding:

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

clear dhcp ipv6 relay statistics

To clear DHCPv6 relay statistics, use the **clear dhcp ipv6 relay statistics** command in XR EXEC mode.

clear dhcp ipv6 relay statistics [**vrf** *vrf-name* [**location** *node-id*]]

Syntax Description

vrf *vrf-name*	(Optional) Clears DHCPv6 relay statistics information for a VPN routing and forwarding (VRF) instance.
location *node-id*	(Optional) Clears DHCPv6 relay statistics information for a specified node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

None.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ip-services	execute
root-system	read, write

This example shows how to clear DHCPv6 relay statistics:

```
Router# clear dhcp ipv6 relay statistics
```

client-mac-mismatch

To enable DHCP MAC address verification.

client-mac-mismatch action drop

Syntax Description

action	Specifies an action for the router when the DHCP MAC address is a not a match.
drop	Drops the packet with the mismatched DHCP MAC address.

Command Default

None

Command Modes

DHCP Relay Profile Configuration Mode

Command History

Release	Modification
Release 6.3.2	This command was introduced.

Usage Guidelines

Enables MAC address verification. If MAC address in the DHCPv4 protocol header does not match the L2 header source MAC address in the DHCPv4 relay profile, the frame is dropped.

Example

Use the following example to configure DHCP MAC address verification.

```
Router# configure

Router(config)# dhcp ipv4
/* Configures DHCP for IPv4 and enters the DHCPv4 configuration submode. */

Router(config-dhcpv4)# profile client relay
/* Enables DHCP relay profile */

Router(config-dhcpv4)# client-mac-mismatch action drop
/* Enables MAC address verification. If MAC address in the DHCPv4 protocol header does not
 match the L2 header source MAC address in the DHCPv4 relay profile,
 the frame is dropped  */

Router(config-dhcpv4-relay-profile)# commit

Router(config-dhcpv4-relay-profile)# exit
```

database (DHCPv6 Binding)

To enable Dynamic Host Configuration Protocol IPv6 (DHCPv6) binding database write to the system persistent memory, use the **database** command in the DHCP IPv6 configuration mode. To disable the DHCPv6 binding table write and to delete the binding table write files from the file system, use the **no** form of this command.

database [**proxy**] [**relay**] [**full-write-interval** *full-write-interval*] [**incremental-write-interval** *incremental-write-interval*]
no database

Syntax Description

proxy	(Optional) Enables DHCPv6 proxy binding database write to the system file system.
relay	(Optional) Enables DHCPv6 relay binding database write to the system file system.
full-write-interval	Sets the interval for a full file write.
full-write-interval	Full file write interval in minutes. The range is from 0 to 1440. The default value is 10.
incremental-write-interval	Sets the interval for an incremental file write.
incremental-write-interval	Incremental file write interval in minutes. The range is from 0 to 1440. The default value is 1.

Command Default

If the command is executed without the keywords **full-write-interval** or **incremental-write-interval**, then the default values of these write intervals are used.

Command Modes

DHCP IPv6 configuration

DHCP IPv6 profile relay configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

All instances of the previous files are deleted after a full persistent binding file write.

The files are written to the file system even if DHCP has no bindings. The incremental file is written even if no new bindings are found in the binding table.

The incremental file does not track deleted bindings. If a binding is deleted and then a system reload occurs before the next full file write, then that binding may reappear when the binding table is recovered from the file system. In this case, the user has to reapply the command to delete the binding. If the binding was deleted because of lease expiry, then it is again deleted when the binding table is recovered from the file system.

The selection of the file system to be used is fixed and not configurable. The file cannot be stored to an external system. Only one file system is used, and if access to this file system fails, then the DHCP binding table backup to file system does not function and an error is logged.

Task ID

Task ID	Operation
ip-services	read, write

This example shows how to enable DHCPv6 binding database write to the system persistent memory:

```
Router# configure
Router# dhcp ipv6
Router(config-dhcpv6)# database proxy full-write-interval 15 incremental-write-interval 5
```

default-router

To configure the default-router, use the **default-router** command in the DHCPv4 server profile sub-mode. To deconfigure the name of the default-router or the IP address, use the **no** form of this command.

default-router *address1address2...address8*
no default-router *address1address2...address8*

Syntax Description

address1address2...address8	Name of the router or IP address. Upto 8 routers can be configured.

Command Default

None

Command Modes

DHCPv4 Server Profile

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ip-services	read, write

Example

This is a sample output from the **default-router** command:

```
Router# config
Router(config)# dhcp ipv4
Router(config-dhcpv4)# profile DHCP_SERVER_PROFILE server
Router(config-dhcpv4-server-profile)# default-router 10.20.1.2
```

dhcp ipv4

To enable Dynamic Host Configuration Protocol (DHCP) for IPv4 and to enter DHCP IPv4 configuration mode, use the **dhcp ipv4** command in Global Configuration mode. To disable DHCP for IPv4 and exit the DHCP IPv4 configuration mode, use the **no** form of this command.

dhcp ipv4
no dhcp ipv4

Syntax Description

This command has no keywords or arguments.

Command Modes

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

Use the **dhcp ipv4** command to enter DHCP IPv4 configuration mode.

Task ID

Task ID	Operations
ip-services	read, write

Examples

This example shows how to enable DHCP for IPv4:

```
RP0/CPU0:Router# dhcp ipv4
RP0/CPU0:Router# (config-dhcpv4)#
```

dhcp ipv6

To enable Dynamic Host Configuration Protocol (DHCP) for IPv6 and to enter DHCP IPv6 configuration mode, use the **dhcp ipv6** command in XR Config mode. To disable the DHCP for IPv6, use the **no** form of this command.

dhcp ipv6

Syntax Description

This command has no keywords or arguments.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

Use the **dhcp ipv6** command to enter DHCP IPv6 configuration mode.

Task ID

Task ID	Operations
ip-services	read, write

Examples

This example shows how to enable DHCP for IPv6:

```
Router(config)# dhcp ipv6
Router(config-dhcpv6)#
```

dns-server

To configure the Domain Name System (DNS) servers, use the **dns-server** command in DHCPv4 server profile configuration and DHCPv4 server profile class sub-mode. To remove the DNS servers use the no form of this command.

dns-server *address1 address2 .....address8*
no dns-server *address1 address2.....address8*

Syntax Description

address1, address2...address8	Specifies the server IPv4 address. Upto 8 server addresses can be configured. The servers are listed in order of preference *address1* is the most preferred server, *address2* is the next most preferred server, and so on.

Command Default

None.

Command Modes

DHCPv4 Server Profile

DHCPv4 Server Profile Class Sub-mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ip-services	read, write

This example shows how to configure DNS server address:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# dhcp ipv4
RP/0/RP0/CPU0:router(config-dhcpv4)# profile DHCP_SERVER_PROFILE server
RP/0/RP0/CPU0:router(config-dhcpv4-server-profile)# dns-server 192.168.155.9
```

domain-name

To configure domain name that DHCP clients will use to resolve DNS names, use the **domain-name** command in DHCP IPv4 server profile configuration mode.

domain-name *domain-name*

Syntax Description

domain-name	Specify DHCP server domain name for the client.

Command Default

None

Command Modes

DHCP IPv4 Server Profile configuration

DHCP IPv4 Server Profile Class sub-mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ip-services	read, write

This example shows how to define cisco.com as domain name for DHCP server:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# dhcp ipv4
RP/0/RP0/CPU0:router(config-dhcpv4)# profile DHCP_SERVER_PROFILE server
RP/0/RP0/CPU0:router(config-dhcpv4-server-profile)# domain-name cisco.com
```

duplicate-mac-allowed

To allow duplicate client MAC addresses across different VLANs and interfaces, use the **duplicate-mac-allowed** command in the DHCP IPv4 configuration mode. To disallow duplicate client MAC addresses, use the **no** form of this command.

duplicate-mac-allowed [**exclude-vlan** | **include-giaddr**]

Syntax Description

exclude-vlan	Excludes VLANs from the client key; only MAC address and interface form the client key.
include-giaddr	Enables support for duplicate sessions having the same MAC address but different *gi-address* values, mainly in the case of routed sessions.

Command Default

By default, duplicate MAC address support is disabled.

Command Modes

DHCP IPv4 configuration

Command History

Release	Modification
Release 6.3.2	Modified the command to include **include-giaddr** option as part of DHCP L3 snooping feature in BNG.
Release 6.1.2	This command was introduced in BNG, with an addition of **exclude-vlan** option to exclude VLANs from the client key.

Usage Guidelines

You can enable duplicate MAC addresses on relay, proxy, server, and snoop DHCP modes.

Do not enable the **duplicate-mac-allowed** command for mobile subscribers.

With **exclude-vlan** option enabled, both inner and outer VLANs get excluded. You cannot exclude just one of them.

The **include-giaddr** option is used for DHCP L3 snooping feature in BNG. It is supported only on Cisco IOS XR 64-bit operating system.

Task ID

Task ID	Operation
ip-services	read, write

Example

This examples shows how to allow duplicate client MAC addresses across different VLANs and interfaces, using the **duplicate-mac-allowed** command:

```
Router# configure
Router(config)# dhcp ipv4
Router(config-dhcpv4)# duplicate-mac-allowed exclude-vlan
```

This examples shows how to enable support for duplicate sessions having the same MAC address but different *gi-address* values, for DHCP L3 snooping in BNG:

```
Router# configure
Router(config)# dhcp ipv4
Router(config-dhcpv4)# duplicate-mac-allowed include-giaddr
```

Related Commands

Command	Description
dhcp ipv4 , on page 208	Enables Dynamic Host Configuration Protocol (DHCP) for IPv4 and enters DHCP IPv4 configuration mode.

giaddr policy

To configure how Dynamic Host Configuration Protocol (DHCP) IPv4 Relay processes BOOTREQUEST packets that already contain a nonzero giaddr attribute, use the **giaddr policy** command in DHCP IPv4 profile relay configuration submode. To restore the default giaddr policy, use the **no** form of this command.

giaddr policy {**replace** | **drop**}
no giaddr policy {**replace** | **drop**}

Syntax Description

replace	Replaces the existing giaddr value with a value that it generates.
drop	Drops the packet that has an existing nonzero giaddr value.

Command Default

DHCP IPv4 relay retains the existing nonzero giaddr value in the DHCP IPv4 packet received from a client value.

Command Modes

DHCP IPv4 profile relay configuration

DHCP IPv4 profile proxy configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

The **giaddr policy** command affects only the packets that are received from a DHCP IPv4 client that have a nonzero giaddr attribute.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to use the **giaddr policy** command:

```
Router# config
Router(config)# dhcp ipv4
Router(config-dhcpv4)# profile client relay
Router(config-dhcpv4-relay-profile)# giaddr policy drop
```

Related Commands

Command	Description
dhcp ipv4 , on page 208	Enables DHCP for IPv4 and enters DHCP IPv4 configuration mode.

Command	Description
helper-address, on page 216	Configures the DHCP relay agent to relay packets to a specific DHCP Server.
interface (DHCP), on page 220	Configures DHCP profile on an interface.
profile (DHCP), on page 228	Configures a relay profile for the DHCP IPv4 component.
relay information check , on page 230	Configures a DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.
relay information option , on page 232	Enables the system to insert a DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.
relay information option allow-untrusted , on page 234	Configures the DHCP component to not drop BOOTREQUEST messages that have the relay information option set and the giaddr set to zero.
relay information policy	Configures how a relay agent processes BOOTREQUEST messages that already contain a relay information option.

helper-address

To configure the Dynamic Host Configuration Protocol (DHCP) IPv4 relay agent to relay DHCP packets to a specific DHCP server, use the **helper-address** command in an DHCP IPv4 relay profile configuration mode. Use the **no** form of this command to clear the address.

helper-address [**vrf** *vrf-name*] [*address*] [**giaddr** *gateway-address*]
no helper-address [**vrf** *vrf-name*] [*address*] [**giaddr** *gateway-address*]

Syntax Description

vrf-name	(Optional) Specifies the name of a particular VRF.
address	IPv4 in four part, dotted decimal format.
giaddr *gateway-address*	(Optional) Specifies the gateway address to use in packets relayed to server. This keyword is applicable for IPv4 helper address.

Command Default

Helper address is not configured.

Command Modes

DHCP IPv4 relay profile configuration

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

A maximum of upto eight helper addresses can be configured.

Task ID

Task ID	Operations
ip-services	read, write

Examples

This example shows how to set the helper-address for a VRF using the **helper address** command in DHCP IPv4 relay profile class configuration mode:

```
RP/0/CPU0:router(config)#  dhcp ipv4
RP/0/CPU0:router(config-dhcpv4)# profile profile1 relay
RP/0/CPU0:router(config-dhcpv4-relay-profile)# helper-address vrf my-server-vrf 10.1.1.1
```

Related Commands

Command	Description
dhcp ipv4	Enables Dynamic Host Configuration Protocol (DHCP) for IPv4 and enters DHCP IPv4 configuration mode.
relay information check	Configures a DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.

Command	Description
relay information option	Enables the system to insert a DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.
relay information option allow-untrusted	Configures the DHCP component to not drop BOOTREQUEST messages that have the relay information option set and the giaddr set to zero.

helper-address (ipv6)

To configure the Dynamic Host Configuration Protocol (DHCP) IPv6 relay agent for prefix delegation to relay DHCP packets to a specific DHCP server, use the **helper-address** command in the DHCP IPv6 profile configuration submode. Use the **no** form of this command to clear the address.

helper-address *ipv6-address* [**interface** *type* *interface-path-id* *dhcpv6 relay source address*]
no helper-address *ipv6-address* [**interface** *type* *interface-path-id* *dhcpv6 relay source address*]

Syntax Description

ipv6-address	The IPv6 address assigned to the interface. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal format using 16-bit values between colons.
interface *type*	Interface type. For more information, use the question mark (?) online help function.

interface-path-id	(Optional) Either a physical interface instance or a virtual interface instance as follows:
	• Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between value s is required as part of the notation.
	  • *rack*: Chassis number of the rack.
	  • *slot*: Physical slot number of the modular services card or line card.
	  • *module*: Module number. A physical layer interface module (PLIM) is always 0.
	  • *port*: Physical port number of the interface.
	Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RSP0) and the module is CPU0. Example: interface MgmtEth0/RSP0/CPU0/0.
	• Virtual interface instance. Number range varies depending on interface type.
	For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

No default behavior or values

Command Modes

DHCP IPv6 profile configuration

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ip-services	read, write

Example

This is a sample output that shows how to set the helper-address using the **helper-address** command

```
Router# config
Router(config)# dhcp ipv6
Router(config-dhcpv6)# profile p1 proxy
Router(config-dhcpv6-profile)# helper-address 2001:db8::3 GigabitEthernet 0/2/0/0
```

Related Commands

Command	Description
dhcp ipv6, on page 209	Enables Dynamic Host Configuration Protocol (DHCP) for IPv6.

interface (DHCP)

To enable Dynamic Host Configuration Protocol (DHCP) for IPv4 or IPv6 on an interface, use the **interface** command in the appropriate configuration mode. To disable DHCPv4 or DHCPv6 on an interface, use the **no** form of the command.

interface *type* *interface-path-id* { **base** | **proxy** | **relay** | **server** | **snoop** }
profile *profile-name*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
server	Attaches a server profile for the specified interface.
relay	Attaches a relay profile for the specified interface.
snoop	Attaches a snoop profile for the specified interface.
proxy	Attaches the proxy profile to an interface.
base	Attaches a base profile for the specified interface.
profile *profile-name*	Specifies the profile name.

Command Default

None

Command Modes

DHCP IPv6 configuration

DHCP IPv4 configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

The support for **base** profile option for DHCP IPv6 is available in BNG from Release 6.2.1 and later. For more details, refer *PPP Class-based DHCPv6 Mode Selection* feature in *Cisco ASR 9000 Series Aggregation Services Router Broadband Network Gateway Configuration Guide*.

Task ID

Task ID	Operations
ip-services	read, write

Examples

This is an example of attaching a relay profile to an interface:

```
Router(config)# dhcp ipv4
Router(config-dhcpv4)# interface tenGigE 0/4/0/4 relay profile RELAY_PROFILE
```

This is an example of enabling the DHCP interface mode on a Packet over Sonet/SDH (POS) interface using the **interface** command:

```
Router(config)# dhcp ipv6
Router(config-dhcpv6)# interface POS 0/5/0/0 relay
```

This is an example of enabling the DHCP interface mode on a Packet over Sonet/SDH (POS) interface using the **interface** command:

```
Router(config)# dhcp ipv4
Router(config-dhcpv4)# interface POS 0/5/0/0 server profile TEST
```

This example shows how to attach a base profile to an interface, in DHCPv6 mode:

```
Router(config)# dhcp ipv6
Router(config-dhcpv6)# interface Bundle-Ether302.2501 base profile base_TEST
```

lease (DHCPv4 Server)

To configure the lease for an IP address assigned from the pool, use the **lease** command in the DHCPv4 server profile submode. To deconfigure, use the **no** form of this command.

lease { **infinite** | *days* }
no lease { **infinite** | *days* }

Syntax Description

infinite	Configures an infinite lease.
days	Configures lease for the specified number of days. The number of days can range from 0 to 365.

Command Default

None

Command Modes

DHCPv4 Server Profile

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ip-services	read, write

Example

This is a sample output from the **lease** command:

```
Router# config
Router#(config)# dhcp ipv4
Router#(config-dhcpv4)# profile P1 server
Router#(config-dhcpv4-server-profile)# lease infinite
```

limit lease

To configure the limit on a lease per-circuit-id, per-interface, or per-remote-id, use the **limit lease** command in the DHCPv4 server profile submode. To deconfigure, use the **no** form of this command.

limit lease {**per-circuit-id** | **per-interface** | **per-remote-id** } *value*
no limit lease {**per-circuit-id** | **per-interface** | **per-remote-id** } *value*

Syntax Description

per-circuit-id	Inserts the limit lease type circuit-id.
per-interface	Inserts the limit lease type interface.
per-remote-id	Inserts the limit lease type remote-id.
value	Value of limit lease count. Range is from 1 to 240000.

Command Default

None

Command Modes

DHCPv4 Server Profile

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ip-services	read, write

Example

This is a sample output from the **limit lease** command:

```
Router# config
Router(config)# dhcp ipv4
Router(config-dhcpv4)# profile P1 server
Router(config-dhcpv4-server-profile)# limit lease per-circuit-id 23
```

netbios-name-server

To configure net bios name servers, use the **netbios-name-server** command in the DHCPv4 server profile submode. To deconfigure, use the **no** form of this command.

netbios-name server *address1address2...address8*
no netbios-name server *address1address2...address8*

Syntax Description

address1address2...address8	Name of the server or IP address.

Command Default

None

Command Modes

DHCPv4 Server Profile

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ip-services	read, write

Example

This is a sample configuration for the **netbios-name-server** command:

```
Router# config
Router(config)# dhcp ipv4
Router(config-dhcpv4)# profile DHCP_SERVER_PROFILE server
Router(config-dhcpv4-server-profile)# netbios-name-server 10.20.3.5
```

netbios-node-type

To configure the type of net bios node, use the **netbios-node-type** command in the DHCPv4 server profile submode. To deconfigure, use the **no** form of this command.

netbios-node-type {*number* | *b-node* | *h-node* | *m-node* | *p-node* }

Syntax Description

number	Hexadecimal number.
b-node	broadcast node.
h-node	hybrid node.
m-node	mixed node.
p-node	peer-to-peer node.

Command Default

None

Command Modes

DHCPv4 Server Profile

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No manually configured prefix delegations exist.

Task ID

Task ID	Operation
ip-services	read, write

Example

This is a sample output from the **bootfile** command:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# dhcp ipv4
RP/0/RP0/CPU0:router(config-dhcpv4)# profile DHCP_SERVER_PROFILE server
RP/0/RP0/CPU0:router(config-dhcpv4-server-profile)# netbios-node-type p-node
```

pool

To enable distributed address pool service on IPv4 or IPv6 profile and to enter the pool IPv4 or IPv6 configuration submode, use the **pool ipv4** or **pool ipv6** command in the Global Configuration mode. To disable this feature, use the **no** form of this command.

pool {[**ipv4***pool-name* {*address-range* | **exclude** | **network***utilization-mark*}] | [**ipv6** {*address-range* | | **exclude** | | **network** | *prefix-length* | *prefix-range* | *utilization-mark*} | [**vrf** {[**all ipv6** *ipv6-pool-name*] | [*vrf-name* {[**ipv4** *ipv4-pool-name* {*address-range* | **exclude** | **network***utilization-mark*}] | [**ipv6** *ipv6-pool-name* {*address-range* | **exclude** | **network***prefix-lengthprefix-rangeutilization-mark*}}]}]}
no pool ipv4

Syntax Description

address-range	Specifies the address-range of the pool.
exclude	Specifies the address to be excluded from the pool.
network	Specifies the network of the pool.
utilization-mark	Specifies the utilization-mark of the pool.
prefix-length	Specifies the prefix-length to be used for the pool.
prefix-range	Specifies the prefix-range to be used for the pool.

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

Use the **pool ipv4** command to enter IPv4 pool configuration submode.

Task ID

Task ID	Operation
ip-services	read, write

This is an example of configuring the **pool ipv4** command in the Global Configuration mode:

```
Router# configure
Router(config)# pool ipv4 pool1
Router(config-pool-ipv4)# address-range 10.10.10.1 10.10.10.254
```

Related Commands

Commands	Description
pool vrf	Enables distributed address pool service on vrf, ipv4, and ipv6.
exclude	Specifies a range of IP addresses that distributed address pool service should not assign to clients.
address-range	Specifies a range of IP addresses.

profile (DHCP)

To configure a DHCP relay profile, DHCP snooping profile, DHCP base profile or a DHCP proxy profile for the Dynamic Host Configuration Protocol (DHCP) IPv4 or IP6 component and to enter the profile mode, use the **profile** command in DHCP IPv4 or DHCP IPv6 configuration mode. To disable this feature and exit the profile mode, use the **no** form of this command.

profile *name* **relay**
no profile *name* **relay**

Syntax Description

name	Name that uniquely identifies the relay or snoop profile.
relay	Configures a DHCP relay profile. A DHCP relay agent is a host that forwards DHCP packets between clients and servers. When the clients and servers are not on the same physical subnet, the relay agents are used to forward requests and replies between them. A DHCP relay agent is any host that forwards DHCP packets between clients and servers. Relay agents are used to forward requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is distinct from the normal forwarding of an IP router, where IP datagrams are switched between networks rather transparently. By contrast, relay agents receive DHCP messages and then generate a new DHCP message to send out on another interface. The relay agent sets the gateway IP address (giaddr field of the DHCP packet) and, if configured, adds the relay agent information option (option82) in the packet and forwards it to the DHCP server. The reply from the server is forwarded back to the client after removing option 82.

Command Default

None

Command Modes

DHCP IPv4 configuration

DHCP IPv6 configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ip-services	read, write

Examples

This example shows how to use the **profile** command to configure DHCP IPv6 relay profile:

```
RP/0/RP0/CPU0:router(config)# dhcp ipv6
RP/0/RP0/CPU0:router(config-dhcpv6)# profile client relay
RP/0/RP0/CPU0:router(config-dhcpv6-relay-profile)#
```

This example shows how to use the **profile** command to configure DHCP IPv4 relay profile:

```
RP/0/RP0/CPU0:router(config)# dhcp ipv4
RP/0/RP0/CPU0:router(config-dhcpv4)# profile client relay
RP/0/RP0/CPU0:router(config-dhcpv4-relay-profile)#
```

relay information check

To configure a Dynamic Host Configuration Protocol (DHCP) IPv4 Relay to validate the relay agent information option in forwarded BOOTREPLY messages, use the **relay information check** command in DHCP IPv4 relay profile configuration submode. To disable this feature, use the **no** form of this command.

relay information check
no relay information check

Syntax Description

This command has no keywords or arguments.

Command Default

DHCP validates the relay agent information option.

Command Modes

DHCP IPv4 relay profile configuration

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ip-services	read, write
basic-services	read, write

This example shows how to use the **relay information check** command:

```
RP/0/CPU0:router# config
RP/0/CPU0:router(config)# dhcp ipv4
RP/0/CPU0:router(config-dhcpv4)# profile client relay
RP/0/CPU0:router(config-dhcpv4-relay-profile)# relay information check
```

Related Commands

Command	Description
dhcp ipv4	Enables Dynamic Host Configuration Protocol (DHCP) for IPv4 and enters DHCP IPv4 configuration mode.
helper-address	Configures the DHCP relay agent to relay packets to a specific DHCP Server.
relay information check	Configures a DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.
relay information option	Enables the system to insert a DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.

Command	Description
relay information option allow-untrusted	Configures the DHCP component to not drop BOOTREQUEST messages that have the relay information option set and the giaddr set to zero.

relay information option

To configure Dynamic Host Configuration Protocol (DHCP) IPv4 relay to insert relay agent information option in forwarded BOOTREQUEST messages to a DHCP server, use the **relay information option** command in DHCP IPv4 relay profile relay configuration. To disable inserting relay information into forwarded BOOTREQUEST messages, use the **no** form of this command.

relay information option
no relay information option

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

DHCP IPv4

relay

profile

configuration

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

The **relay information option** command automatically adds the circuit identifier suboption and the remote ID suboption to the DHCP relay agent information option.

The **relay information option** command enables a DHCP server to identify the user (for example, cable access router) sending the request and initiate appropriate action based on this information. By default, DHCP does not insert relay information.

The upstream DHCP server or DHCP relay interface must be configured to accept this type of packet using the **relay information option allow-untrusted** configuration. This configuration prevents the server or relay from dropping the DHCP message.

Task ID

Task ID	Operations
ip-services	read, write
basic-services	read, write

This example shows how to use the **relay information option** command:

```
RP/0/CPU0:router# config
RP/0/CPU0:router(config)# dhcp ipv4
RP/0/CPU0:router(config-dhcpv4)# profile client relay
RP/0/CPU0:router(config-dhcpv4-relay-profile)# relay information option
```

Related Commands

Command	Description
dhcp ipv4	Enables DHCP for IPv4 and enters DHCP IPv4 configuration mode.
helper-address	Configures the DHCP relay agent to relay packets to a specific DHCP Server.
relay information check	Configures a DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.
relay information option allow-untrusted	Configures the DHCP component to not drop BOOTREQUEST messages that have the relay information option set and the giaddr set to zero.

relay information option allow-untrusted

To configure the Dynamic Host Configuration Protocol (DHCP) IPv4 relay not to drop discard BOOTREQUEST packets that have the relay information option set and the giaddr set to zero, use the **relay information option allow-untrusted** command in DHCP IPv4 relay profile configuration submode. To restore the default behavior, which is to discard the BOOTREQUEST packets that have the relay information option and set the giaddr set to zero, use the **no** form of this command.

relay information option allow-untrusted
no relay information option allow-untrusted

Syntax Description

This command has no keywords or arguments.

Command Default

The packet is dropped if the relay information is set and the giaddr is set to zero.

Command Modes

DHCP IPv4

relay

profile

configuration

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

According to RFC 3046, relay agent receiving a DHCP packet from an untrusted circuit with giaddr set to zero but with a relay agent information option already present in the packet shall discard the packet and increment an error count. This configuration prevents relay from dropping the DHCP message.

Task ID

Task ID	Operations
ip-services	read, write
basic-services	read, write

Examples

This example shows how to use the **relay information option allow-untrusted** command:

```
RP/0/CPU0:router# config
RP/0/CPU0:router(config)# dhcp ipv4
RP/0/CPU0:router(config-dhcpv4)# profile client relay
RP/0/CPU0:router(config-dhcpv4-relay-profile)# relay information option allow-untrusted
```

Related Commands

Command	Description
dhcp ipv4	Enables Dynamic Host Configuration Protocol (DHCP) for IPv4 and enters DHCP IPv4 configuration mode.
helper-address	Configures the DHCP relay agent to relay packets to a specific DHCP Server.
relay information check	Configures a DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.
relay information option	Enables the system to insert a DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.

subnet-mask

To configure subnet mask that DHCP clients should use, use the **subnet-mask** command in DHCP IPv4 server profile configuration mode.

subnet-mask *number*

Syntax Description

number	Specify DHCP server's subnet mask number.

Command Default

None

Command Modes

DHCP IPv4 Server Profile configuration

DHCP IPv4 Server Profile Class submode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

If subnet-mask is not configured, then the DHCP server will send subnet mask of an access interface to the client.

Task ID

Task ID	Operation
ip-services	read, write

This example shows how to configure subnet mask for DHCP server:

```
Router# config
Router(config)# dhcp ipv4
Router(config-dhcpv4)# profile DHCP_SERVER_PROFILE server
Router(config-dhcpv4-server-profile)# subnet-mask 255.255.255.0
```

show dhcp ipv4 client

To display DHCP client binding information, use the **show dhcp ipv4 client** command in XR EXEC mode.

show dhcp ipv4 client <*interfaceName*> [**detail**] [**debug**]

Syntax Description

interfaceName	Displays the DHCP IPv4 address of the specified interface.
detail	(Optional) Specifies detailed results.
debug	(Optional) Displays internal debugging information.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

Use the **show dhcp ipv4 client** command to display the DHCP IPv4 for the specified client.

Task ID

Task ID	Operations
IP-Services	read

Examples

The following example shows how to display DHCP IPv4 binding information:

```
Router# show dhcp ipv4  client
Mon May  6 16:35:32.581 UTC

    Interface name                    IP Address           Binding State         Lease
Time Rem
----------------------               ------------         ---------------
----------------------
MgmtEth0_0_CPU0_0                   192.168.190.130           BOUND           1688 secs
(00:28:08)

Router#
Router# show dhcp ipv4  client binding ?
  MgmtEth          Ethernet/IEEE 802.3 interface(s)
  detail           Show detailed client binding information
  |                Output Modifiers
  <cr>
Router# show dhcp ipv4  client   detail
Mon May  6 16:35:56.579 UTC

-----------------------------------------------------
Client Interface name         : MgmtEth0_0_CPU0_0
Client Interface handle       : 0x1280
Client Interface VRF name     : default
Client ChAddr                 : 000c.292f.950e
```

```
Client ID                     : MgmtEth0_0_CPU0_0
Client State                  : BOUND
Client IP Address (Dhcp)      : 192.168.190.130
Client IP Address Mask        : 255.255.255.0
Client Lease Time Allocated   : 1800 secs (00:30:00)
Client Lease Time Remaining   : 1664 secs (00:27:44)
Client Selected Server Addr   : 192.168.190.254
-----------------------------------------------------

Router#
Router# show dhcp ipv4  client binding detail ?
  MgmtEth          Ethernet/IEEE 802.3 interface(s)
  debug            Show detailed debug level client binding information
  |                Output Modifiers
  <cr>
Router# show dhcp ipv4  client detail debug
Mon May  6 16:36:43.836 UTC

-----------------------------------------------------
Client Interface name         : MgmtEth0_0_CPU0_0
Client Interface handle       : 0x1280
Client Interface VRF name     : default
Client ChAddr                 : 000c.292f.950e
Client ID                     : MgmtEth0_0_CPU0_0
Client State                  : BOUND
Client IP Address (Dhcp)      : 192.168.190.130
Client IP Address Mask        : 255.255.255.0
Client Lease Time Allocated   : 1800 secs (00:30:00)
Client Lease Time Remaining   : 1617 secs (00:26:57)
Client Selected Server Addr   : 192.168.190.254
Client Interface VRF id       : 0x60000000
Client Interface VRF Table id : 0xe0000000
Client XID                    : 0xa7f
Client Timers Running         : 0x2 (T1_RENEW_TIMER)
Client Renew Time Allocated   : 900 secs (00:15:00)
Client Renew Time Adjusted    : 900 secs (00:15:00)
Client Rebind Time Allocated  : 1575 secs (00:26:15)
Client Rebind Time Adjusted   : 1575 secs (00:26:15)
Client Checkpoint object id   : 0x80002fd8
Client IPv4 MA configured     : TRUE
-----------------------------------------------------

Router#
Router# show dhcp ipv4 client  mgmtEth 0/0/CPU0/0
Mon May  6 16:49:54.382 UTC

    Interface name         IP Address      Binding State         Lease Time Rem
----------------------    ------------    ---------------    ----------------------
MgmtEth0_0_CPU0_0          192.168.190.130  BOUND             1727 secs (00:28:47)
RP/0/0/CPU0:ios#
```

show dhcp ipv4 relay profile

To display Dynamic Host Configuration Protocol (DHCP) relay agent status, use the **show dhcp ipv4 relay profile** command in EXEC mode.

show dhcp ipv4 relay profile

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

This command displays the relay profiles created for DHCP IPv4.

Task ID

Task ID	Operations
ip-services	read

Examples

The following is sample output from the **show dhcp ipv4 relay profile** command:

```
Router# show dhcp ipv4 relay profile

DHCP IPv4 Relay Profiles
------------------------
r1
r2
```

Related Commands

Command	Description
show dhcp ipv4 relay profile name	Displays Dynamic Host Configuration Protocol (DHCP) relay agent status, specific to a relay profile.

show dhcp ipv4 relay profile name

To display Dynamic Host Configuration Protocol (DHCP) relay agent status, specific to a relay profile, use the **show dhcp ipv4 relay profile name** command in EXEC mode.

show dhcp ipv4 relay profile [**name** *profile-name*]

Syntax Description

name *profile-name*	(Optional) Name that uniquely identifies the relay profile.

Command Default

If *name* is not specified, displays a list of configured DHCP profile names.

No default behavior or values

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ip-services	read

Examples

The following is sample output from the **show dhcp ipv4 relay profile name** command:

```
Router# show dhcp ipv4 relay profile name r1

DHCP IPv4 Relay Profile r1:

Helper Addresses:
10.10.10.1, vrf default
Information Option: Disabled
Information Option Allow Untrusted: Disabled
Information Option Policy: Replace
Information Option Check: Disabled
Giaddr Policy: Keep
Broadcast-flag Policy: Ignore

VRF References:
default
Interface References:
FINT0_RP0_CPU0
MgmtEth0_RP0_CPU0_0
```

show dhcp ipv4 relay statistics

To display the Dynamic Host Configuration Protocol (DHCP) IPv4 relay agent packet statistics information for VPN routing and forwarding (VRF) instances, use the **show dhcp ipv4 relay statistics** command in EXEC mode.

show dhcp [**vrf** {*vrf-name* | **default**}] **ipv4 relay statistics**

Syntax Description

vrf *vrf-name*	(Optional) Name that uniquely identifies the VRF.
default	(Optional) Displays the relay statistics information for the default VRF.

Command Default

No default behavior or values

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ip-services	read

Examples

The following is sample output from the **show dhcp ipv4 relay statistics** command when none of the optional keywords or arguments are used command :

```
Router#  show dhcp ipv4 relay statistics

                  VRF                  |       RX       |       TX       |       DR       |
-------------------------------------------------------------------------------------------
                default                |            0   |            0   |            0   |
```

The following is sample output from the show dhcp ipv4 relay statistics command using the **vrf** and **default** keywords:

```
Router#  show dhcp vrf default ipv4 relay statistics
01 Sep 6 07:10:35.873 UTC

DHCP IPv4 Relay Statistics for VRF default:

     TYPE          |    RECEIVE     |    TRANSMIT    |     DROP       |
-------------------------------------------------------------------------
DISCOVER           |             0  |             0  |             0  |
OFFER              |             0  |             0  |             0  |
REQUEST            |             0  |             0  |             0  |
DECLINE            |             0  |             0  |             0  |
ACK                |             0  |             0  |             0  |
NAK                |             0  |             0  |             0  |
```

```
RELEASE           |            0  |            0  |            0  |
INFORM            |            0  |            0  |            0  |
LEASEQUERY        |            0  |            0  |            0  |
LEASEUNASSIGNED   |            0  |            0  |            0  |
LEASEUNKNOWN      |            0  |            0  |            0  |
LEASEACTIVE       |            0  |            0  |            0  |
BOOTP-REQUEST     |            0  |            0  |            0  |
BOOTP-REPLY       |            0  |            0  |            0  |
BOOTP-INVALID     |            0  |            0  |            0  |
```

show dhcp ipv4 server binding

To display DHCP client bindings for server, use the **show dhcp ipv4 server binding** command in EXEC mode.

show dhcp ipv4 server binding { **detail** | **location** *node-ID* | **interface** *type interface-path-ID* | **vrf** *vrf-name* | **ip-address** *address* | **mac-address** *address* | **srg** | **srg-master** | **srg-slave** | **summary**}

Syntax Description

detail	Displays detailed client binding information for all clients.
location *node-ID*	Displays detailed client binding information for a specified node.
interface *type interface-path-ID*	Displays client binding by interface. Specifies the interface type. For more information, use the question mark (?) online help function. Physical interface or virtual interface. Use the show interfaces command to see a list of all interfaces currently configured on the router. **Note** For more information about the syntax for the router, use the question mark (?) online help function.
vrf *vrf-name*	Displays client binding by vrf name.
ip-address *address*	Displays detailed client binding information per IP address or mac-address.
mac-address *address*	Displays detailed client binding information per mac-address.
srg	Displays client binding by SRG group.
srg-master	Displays client binding by SRG master.
srg-slave	Displays client binding by SRG slave.

Command Default

None.

Command Modes

EXEC

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ip-services	read

Example

This is a sample output from the **show dhcp ipv4 server binding** command:

```
Router# show dhcp ipv4 server binding detail

Thu Aug  1 11:37:34.784 IST
MAC Address:                 ca01.4b16.0000
VRF:                         default
IP Address:                  10.10.10.7
Server IP Address:           10.10.10.2
ReceivedCircuit ID:          -
InsertedCircuit ID:          -
ReceivedRemote ID:           -
InsertedRemote ID:           -
ReceivedVSISO:               -
Auth. on received relay info:TRUE
ParamRequestOption:          -
SavedOptions:                -
Profile:                     TEST
Selected Profile:            TEST
State:                       BOUND
Lease:                       1800 secs (00:30:00)
Lease remaining:             1744 secs (00:29:04)
Client ID:
0x00-0x63-0x69-0x73-0x63-0x6F-0x2D-0x63-0x61-0x30-0x31-0x2E-0x34-0x62-0x31-0x36-0x2E-0x30-0x30-0x30-0x30-0x2D-0x50-0x6F-0x31-0x30-0x2E-0x31
Access Interface:            Bundle-Ether10.1
Access VRF:                  default
VLAN Id:                     100
Subscriber Label:            0x41
Subscriber Interface:        Bundle-Ether10.1.ip2
Srg State:                   NONE
Srg Group Id:                0
Event History:
Session Start:               Aug  1 10:38:05.426
PACKET_DISCOVER              :     0.001s
DPM_SUCCESS                  :     0.114s
DAPS_SUCCESS                 :     0.118s
PACKET_REQUEST               :     0.818s
LEASE_DPM_SUCCESS            :     1.181s
OTHER                        :    45.005s
```

Related Commands

Command	Description
show dhcp ipv4 server profile	Displays DHCP server profile information.
show dhcp ipv4 server statistics	Display DHCP server statistics.

show dhcp ipv4 server profile

To display DHCP server profile information with ipv4 binding, use the **show dhcp ipv4 server profile** command in EXEC mode.

show dhcp ipv4 server profile name *profile-name* [**location** *node-ID*]

Syntax Description

profile-name	Name of the profile.
location *node-ID*	Displays detailed DHCP server profile information for a specified node.

Command Default

None.

Command Modes

EXEC

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ip-services	read

Example

This is a sample output from the **show dhcp ipv4 server profile** command:

```
Router# show dhcp ipv4 server profile name foo

Profile:   foo
VRF References:
Interface References: GigabitEthernet0/2/0/0
```

Related Commands

Command	Description
show dhcp ipv4 server binding	Displays DHCP client bindings for server.
show dhcp ipv4 server statistics	Displays DHCP server statistics.
show dhcp ipv4 server interface	Displays DHCP client bindings for server with respect to interfaces.
show dhcp ipv4 server disconnect-history	

show dhcp ipv4 server statistics

To display DHCP server statistics, use the **show dhcp ipv4 server statistics** command in EXEC mode.

show dhcp ipv4 server statistics [[**raw** {[| **all**] [| **include-zeroes**] [| **location** *node-ID*]]}

Syntax Description

raw	Displays debug statistics.
all	Displays debug statistics for base mode.
include-zeroes	Displays debug statistics that are zero.
location *node-ID*	Displays DHCP server statistics information for a specified node.

Command Default

None.

Command Modes

EXEC

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ip-services	read

Example

This is a sample output from the **show dhcp ipv4 server statistics** command:

```
Router# show dhcp ipv4 server statistics
              VRF         |       RX       |      TX       |       DR       |
-------------------------------------------------------------------------------------
             default      |        0       |       0       |        0       |
```

Related Commands

Command	Description
show dhcp ipv4 server binding	Displays DHCP client bindings for server.
show dhcp ipv4 server profile	Displays DHCP server profile information.
show dhcp ipv4 server interface	Displays DHCP server profile information for interface.

Command	Description
show dhcp ipv4 server disconnect-history	Displays DHCP server profile information with respect to disconnect-history.

show dhcp ipv6 relay binding

To display DHCPv6 client bindings for relay, use the **show dhcp ipv6 relay binding** command in XR EXEC mode.

show dhcp ipv6 relay binding [**client-duid** *client-duid-number*] [**detail**] [**interface** *type interface-path-id*] [**location** *node-id*] [**summary**] [**vrf** *vrf-name*]

Syntax Description

client-duid *client-duid-number*	(Optional) Displays DHCPv6 relay client binding information. The argument *client-duid-number* is the client's DHCP Unique Identifier (DUID) number. **Note** Use the **show dhcp ipv6 relay binding** command to see the client DUID number.
detail	(Optional) Displays detailed DHCPv6 relay client binding information for all clients.
interface *type interfac-path-id*	(Optional) Displays DHCPv6 relay client binding by interface. Specifies a physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router.
location *node-id*	(Optional) Displays detailed DHCPv6 relay client binding information for a specified node. The *node-id* argument is entered in the *rack/slot/module* notation.
summary	(Optional) Displays the summary of DHCPv6 relay client binding.
vrf *vrf-name*	(Optional) Displays DHCPv6 relay client binding information for a VPN routing and forwarding (VRF) instance.

Command Default

None.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ip-services	read

This is the sample output for show dhcp ipv6 relay binding command:

```
Router# show dhcp ipv6 relay binding
Summary:
Total number of clients: 1

IPv6 Address: fc00:35:0:ef5c:a932:239f:1b0e:e4ed/128 (BVI3500)
    Client DUID: 000100011b626e6f0000cae2da26
    IAID: 0x0
    VRF: default
    Lifetime: 172800 secs (2d00h)
    Expiration: 172766 secs (1d23h)
```

show dhcp ipv6 relay statistics

To display DHCPv6 relay statistics, use the **show dhcp ipv6 relay statistics** command in XR EXEC mode.

show dhcp ipv6 relay statistics [**debug** [**all** | **include-zeroes** | **location** *node-id*]] [**vrf** *vrf-name*] [**location** *nide-id*]

Syntax Description

debug	(Optional) Displays DHCPv6 relay debug statistics information.
all	(Optional) Displays DHCPv6 relay debug statistics information for all location.
include-zeroes	(Optional) Displays DHCPv6 relay debug statistics information that are zero.
location *node-id*	(Optional) Displays DHCPv6 relay debug statistics information for for a specified node. The *node-id* argument is entered in the *rack/slot/module* notation.
vrf *vrf-name*	(Optional) Displays DHCPv6 relay statistics information for a VPN routing and forwarding (VRF) instance.
location *node-id*	(Optional) Displays detailed DHCPv6 relay statistics information for a specified node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

None.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ip-services	read

This is the sample output for **show dhcp ipv6 relay statistics** command:

```
Router# show dhcp ipv6 relay statistics
                  VRF                       |       RX        |       TX        |        DR
|
-------------------------------------------------------------------------------------------------
default                                     |          241  |             5  |          236  |
**nVSatellite                               |            0  |             0  |            0  |
red4                                        |            0  |             0  |            0  |
red6                                        |            0  |             0  |            0  |
**eint                                      |            0  |             0  |            0  |
```

show tech support dhcp ipv4 client

To retrieve the DHCP client show tech support information, use the **show tech dhcp ipv4 client** command in XR EXEC mode.

show tech-support dhcp ipv4 client <show-tech-options>

Syntax Description

show-tech-options	Displays the DHCP IPv4 client show tech-support options.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

Use the **show tech-support dhcp ipv4 client** command to retrieve the DHCP show-tech options for the specified interface.

Task ID

Task ID	Operations
IP-Services	Execution

Examples

The following example shows how to clear the DHCP client binding statistics information:

```
Router# show tech-support dhcp ipv4 client ?
  file      Specify a valid file name (e.g. disk0:tmp.log)(cisco-support)
  terminal  Send output to terminal(cisco-support)
Router# show tech-support dhcp ipv4 client file ?
  WORD        Send to file
  bootflash:  Send to bootflash: file system(cisco-support)
  disk0:      Send to disk0: file system(cisco-support)
  disk0a:     Send to disk0a: file system(cisco-support)
  disk1:      Send to disk1: file system(cisco-support)
  disk1a:     Send to disk1a: file system(cisco-support)
  ftp:        Send to ftp: file system(cisco-support)
  nvram:      Send to nvram: file system(cisco-support)
  rcp:        Send to rcp: file system(cisco-support)
  tftp:       Send to tftp: file system(cisco-support)
Router# show tech-support dhcp ipv4 client file disk0?
WORD  disk0:  disk0a:
Router# show tech-support dhcp ipv4 client file disk0:/dhcpv4-client-showtech.tgz
Fri Jun  6 08:25:24.793 UTC
Router# dir disk0:
Fri Jun  6 08:25:47.321 UTC

Directory of disk0:

2           drwx  1024        Thu Mar 13 06:12:03 2014  .boot
…
```

```
3           -rw-  83337       Fri Jun  6 08:25:26 2014  dhcpv4-client-showtech.tgz

1911537664 bytes total (1838081024 bytes free)
Router#
```

Related Commands

show dhcp ipv4 client statistics	Displays the statistics of the DHCP client.
show tech support dhcp ipv4 server	Displays the tech support for DHCP ipv4 server profile.
show tech support dhcp ipv4 proxy	Displays the tech support for DHCP ipv4 proxy profile.
show tech support dhcp ipv4 relay	Displays the tech support for DHCP ipv4 relay profile.
show tech support dhcp ipv6 server	Displays the tech support for DHCP ipv6 server profile.
show tech support dhcp ipv6 proxy	Displays the tech support for DHCP ipv6 proxy profile.
show tech support dhcp ipv6 relay	Displays the tech support for DHCP ipv6 relay profile.

show dhcp vrf ipv4 server statistics

To display DHCP server statistics for the default vrf or a specific vrf, use the **show dhcp vrf ipv4 server statistics** command in XR EXEC mode.

show dhcp vrf { **default** | *vrf-name* } [**location** *node-ID*]

Syntax Description

default	Display DHCP server statistics for the default vrf.
vrf-name	Display DHCP server statistics for a specific vrf.
location *node-ID*	Displays DHCP server statistics information for a specified node.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ip-services	read

Example

This is a sample output from the **show dhcp vrf default ipv4 server statistics** command:

```
Router# show dhcp vrf default ipv4 server statistics
Thu Aug  1 11:41:48.255 IST

DHCP IPv4 Proxy/Server Statistics for VRF default:

     TYPE          |    RECEIVE    |    TRANSMIT   |     DROP      |
-------------------------------------------------------------------
 DISCOVER          |             5  |             0  |             0  |
 OFFER             |             0  |             3  |             0  |
 REQUEST           |            15  |             0  |             0  |
 DECLINE           |             0  |             0  |             0  |
 ACK               |             0  |            15  |             0  |
 NAK               |             0  |             0  |             0  |
 RELEASE           |             0  |             0  |             0  |
 INFORM            |             0  |             0  |             0  |
```

```
 LEASEQUERY       |            0  |            0  |            0  |
 LEASEUNASSIGNED  |            0  |            0  |            0  |
 LEASEUNKNOWN     |            0  |            0  |            0  |
 LEASEACTIVE      |            0  |            0  |            0  |
 BOOTP-REQUEST    |            0  |            0  |            0  |
 BOOTP-REPLY      |            0  |            0  |            0  |
RP/0/0/CPU0:server#
```

trust relay-reply

To configure a DHCP IPv6 profile to enable processing relay-replies, use the **trust relay-reply** command in DCHP IPv6 profile configuration mode. To restore the interface to the default behavior, use the **no** form of the command.

trust relay-reply
no trust relay-reply

This command has no keywords or arguments.

Command Default

By default, all interfaces are trusted.

Command Modes

DHCP IPv6 profile configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ip-services	read, write

Example

```
Router# configure
Router(config)# dhcp ipv6
Router(config-dhcpv6)# profile downstream proxy
Router(config-dhcpv6-profile)# helper-address ff05::1:3
Router(config-dhcpv6-profile)# exit
Router(config-dhcpv6)# profile upstream proxy
Router(config-dhcpv6-profile)# trust relay-reply
```

Related Commands

Command	Description
helper-address (ipv6), on page 218	Configures the Dynamic Host Configuration Protocol (DHCP) IPv6 relay agent for prefix delegation.



Host Services and Applications Commands

This chapter describes the commands used to configure and monitor host services and applications, such as Domain Name System (DNS), Telnet, File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), and Remote Copy Protocol (RCP).

For detailed information about host services and applications concepts, configuration tasks, and examples, refer to the *IP Addresses and Services Configuration Guide for Cisco NCS 5000 Series Routers*.

- cinetd rate-limit, on page 258
- clear host, on page 259
- destination address(ipsla), on page 260
- domain ipv4 host, on page 261
- domain ipv6 host, on page 262
- domain list, on page 263
- domain lookup disable, on page 264
- domain name (IPAddr), on page 265
- domain name-server, on page 266
- ftp client anonymous-password, on page 267
- ftp client passive, on page 268
- ftp client password, on page 269
- ftp client source-interface, on page 270
- ftp client username, on page 271
- logging source-interface , on page 272
- ping (network), on page 273
- ping bulk (network), on page 276
- scp, on page 278
- show cinetd services, on page 280
- show hosts, on page 282
- telnet, on page 284
- telnet client source-interface, on page 287
- telnet dscp, on page 288
- telnet server, on page 289
- telnet transparent, on page 291
- tftp client source-interface, on page 292
- tftp server, on page 293
- traceroute, on page 294

cinetd rate-limit

To configure the rate limit at which service requests are accepted by Cisco inetd (Cinetd), use the **cinetd rate-limit** command in XR Config mode. To restore the default, use the **no** form of this command.

cinetd rate-limit *value*
no cinetd rate-limit *value*

Syntax Description

value	Number of service requests that are accepted per second. Range is 1 to 100. Default is 1.

Command Default

One service request per second is accepted.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Any service request that exceeds the rate limit is rejected. The rate limit is applied to individual applications.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows the **cinetd rate-limit** being set to 10:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# cinetd rate-limit 10
```

clear host

To delete temporary entries from the hostname-to-address cache, use the **clear host** command in XR EXEC mode.

clear host {*host-name* | *****}

Syntax Description

host-name	Name of host to be deleted.
*	Specifies that all entries in the local cache be deleted.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The dynamic host entries in the cache are cleared.

The temporary entries in the cache are cleared; the permanent entries that were entered with the domain ipv4 host, on page 261 or the domain ipv6 host, on page 262 command are not cleared.

By default, no static mapping is configured.

Task ID

Task ID	Operations
ip-services	execute

Examples

The following example shows how to clear all temporary entries from the hostname-and-address cache:

```
RP/0/RP0/CPU0:router# clear host *
```

destination address(ipsla)

To configure the address of the destination device, use the **destination address** command in the ipsla echo configuration mode. To restore the default, use the **no** form of this command.

destination address *address*
no destination address *address*

Syntax Description

address	IPv4/IPv6 address of the destination device.

Command Default

None

Command Modes

ipsla echo configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
monitor	read, write

Example

This example shows how to configure 10.10.10.20 as the destination address of a device.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 500
RP/0/RP0/CPU0:router(config-ipsla-op)# type icmp echo
RP/0/RP0/CPU0:router(config-ipsla-echo)# timeout 5000
RP/0/RP0/CPU0:router(config-ipsla-echo)# destination address 10.10.10.20
```

domain ipv4 host

To define a static hostname-to-address mapping in the host cache using IPv4, use the **domain ipv4 host** command in XR Config mode. To remove the **domain ipv4 host** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

domain ipv4 host *host-name v4address2.....v4address8*
no domain ipv4 host *host-name v4address1*

Syntax Description

host-name	Name of the host. The first character can be either a letter or a number.
v4address1	Associated IP address.
v4address2...v4address8	(Optional) Additional associated IP address. You can bind up to eight addresses to a hostname.

Command Default

No static mapping is configured.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The first character can be either a letter or a number. If you use a number, the operations you can perform (such as **ping**) are limited.

Task ID

Task ID	Operations
ip-services	read, write
basic-services	read, write

Examples

The following example shows how to define two IPv4 static mappings:

```
RP/0/RP0/CPU0:router(config)# domain ipv4 host host1 192.168.7.18
RP/0/RP0/CPU0:router(config)# domain ipv4 host bost2 10.2.0.2 192.168.7.33
```

domain ipv6 host

To define a static hostname-to-address mapping in the host cache using IPv6, use the **domain ipv6 host** command in XR Config mode. To remove the **domain ipv6 host** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

domain ipv6 host *host-name v6address1 [v6address2 .....v6address4]*
no domain ipv6 host *host-name v6address1*

Syntax Description

host-name	Name of the host. The first character can be either a letter or a number.
v6address1	Associated IP address.
v6address2...v6address4	(Optional) Additional associated IP address. You can bind up to four addresses to a hostname.

Command Default

No static mapping is configured. IPv6 address prefixes are not enabled.

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The first character can be either a letter or a number. If you use a number, the operations you can perform (such as **ping**) are limited.

Task ID

Task ID	Operations
ip services	read, write

Examples

The following example shows how to define two IPv6 static mappings:

```
RP/0/RP0/CPU0:router(config)# domain ipv6 host host1 ff02::2
RP/0/RP0/CPU0:router(config)# domain ipv6 host host2 ff02::1
```

domain list

To define a list of default domain names to complete unqualified hostnames, use the **domain list** command in XR Config mode. To delete a name from a list, use the **no** form of this command.

domain list *domain-name*
no domain list *domain-name*

Syntax Description

domain-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

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

If there is no domain list, the domain name that you specified with the domain name (IPAddr), on page 265 command is used to complete unqualified hostnames. If there is a domain list, the default domain name is not used. The **domain list** command is similar to the domain name (IPAddr), on page 265 command, except that you can use the **domain list** command to define a list of domains, each to be tried in turn.

Task ID

Task ID	Operations
ip-service	read, write

Examples

The following example shows how to add several domain names to a list:

```
RP/0/RP0/CPU0:router(config)# domain list domain1.com
RP/0/RP0/CPU0:router(config)# domain list domain2.edu
```

The following example shows how to add a name to and then delete a name from the list:

```
RP/0/RP0/CPU0:router(config)# domain list domain3.edu
RP/0/RP0/CPU0:router(config)# no domain list domain2.edu
```

domain lookup disable

To disable the IP Domain Name System (DNS)-based hostname-to-address translation, use the **domain lookup disable** command in XR Config mode. To remove the specified command from the configuration file and restore the system to its default condition, use the **no** form of this command.

domain lookup disable
no domain lookup disable

Syntax Description

This command has no keywords or arguments.

Command Default

The IP DNS-based host-to-address translation is enabled.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Using the **no** command removes the specified command from the configuration file and restores the system to its default condition. The **no** form of this command is not stored in the configuration file.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to enable the IP DNS-based hostname-to-address translation:

```
RP/0/RP0/CPU0:router(config)# domain lookup disable
```

domain name (IPAddr)

To define a default domain name that the software uses to complete unqualified hostnames, use the **domain name** command in the appropriate mode. To remove the name, use the **no** form of this command.

domain name *domain-name*
no domain name *domain-name*

Syntax Description

domain-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

There is no default domain name.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

If a hostname does not contain a domain name, then a dot and the domain name configured by the **domain name** command are appended to the hostname before it is added to the host table.

If no domain name is configured by the **domain name** command and the user provides only the hostname, then the request is not looked up.

Task ID

Task ID	Operations
ip-services	read, write

domain name-server

To specify the address of one or more name servers to use for name and address resolution, use the **domain name-server** command in XR Config mode. To remove the address specified, use the **no** form of this command.

domain name-server *server-address*
no domain name-server *server-address*

Syntax Description

server-address	IP address of a name server.

Command Default

If no name server address is specified, the default name server is 255.255.255.255. IPv4 and IPv6 address prefixes are not enabled.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

You can enter up to six addresses, but only one for each command.

If no name server address is specified, the default name server is 255.255.255.255 so that the DNS lookup can be broadcast to the local network segment. If a DNS server is in the local network, it replies. If not, there might be a server that knows how to forward the DNS request to the correct DNS server.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to specify host 192.168.1.111 as the primary name server and host 192.168.1.2 as the secondary server:

```
RP/0/RP0/CPU0:router(config)# domain name-server 192.168.1.111
RP/0/RP0/CPU0:router(config)# domain name-server 192.168.1.2
```

ftp client anonymous-password

To assign a password for anonymous users, use the **ftp client anonymous-password** command in XR Config mode. To remove the **ftp client anonymous-password** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

ftp client anonymous-password *password*
no ftp client anonymous-password

Syntax Description

password	Password for the anonymous user.

Command Default

No default behavior or values

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **ftp client anonymous-password** command is File Transfer Protocol (FTP) server dependent.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to set the anonymous password to *xxxx*:

```
RP/0/RP0/CPU0:router(config)# ftp client anonymous-password xxxx
```

ftp client passive

To configure the software to use only passive File Transfer Protocol (FTP) connections, use the **ftp client passive** command in XR Config mode. To remove the **ftp client passive** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

ftp client passive
no ftp client passive

Syntax Description

This command has no keywords or arguments.

Command Default

FTP data connections are active.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Using the **ftp client passive** command allows you to make only passive-mode FTP connections. To specify the source IP address for FTP connections, use the **ftp client source-interface** command.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to configure the networking device to use only passive FTP connections:

```
RP/0/RP0/CPU0:router(config)# ftp client passive

1d:3h:54:47: ftp_fs[16437]: FTP: verifying tuple passive (SET).
1d:3h:54:47: ftp_fs[16437]: FTP: applying tuple passive (SET).
1d:3h:54:47: ftp_fs[16437]: FTP: passive mode has been enabled.
```

ftp client password

To specify the password for the File Transfer Protocol (FTP) connections, use the **ftp client password** command in XR Config mode. To disable this feature, use the **no** form of this command.

ftp client password {*clear-text-password* | **clear** *clear-text password* | **encrypted** *encrypted-text password*}
no ftp client password {*clear-text-password* | **clear** *clear-text password* | **encrypted** *encrypted-text password*}

Syntax Description

clear-text-password	Specifies an unencrypted (cleartext) user password
clear *clear-text password*	Specifies an unencrypted (cleartext) shared password.
encrypted *encrypted-text password*	Specifies an encrypted shared password.

Command Default

No default behavior or values

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to specify the password for the File Transfer Protocol (FTP) connections:

```
RP/0/RP0/CPU0:router(config)# ftp client password lab
```

ftp client source-interface

To specify the source IP address for File Transfer Protocol (FTP) connections, use the **ftp client source-interface** command in XR Config mode . To remove the **ftp client source-interface** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

ftp client source-interface *type interface-path-id*
no ftp client source-interface *type interface-path-id*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the show interfaces command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

The FTP source address is the IP address of the interface used by the FTP packets to leave the networking device.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use this command to set the same source address for all FTP connections. To configure the software to use only passive FTP connections, use the **ftp client passive** command.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to configure the IP address associated with tenGigE interface 0/1/2/1 as the source address on all FTP packets, regardless of which interface is actually used to send the packet:

```
RP/0/RP0/CPU0:router(config)# ftp client source-interface tenGigE0/1/2/1
```

ftp client username

To specify the username for File Transfer Protocol (FTP) connections, use the **ftp client username** command in XR Config mode. To disable this feature, use the **no** form of this command.

ftp client username *username*
no ftp client username *username*

Syntax Description

username	Name for FTP user.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to specify the username for FTP connections:

```
Router(config)# ftp client username fox
```

logging source-interface

To configure the logging source interface in order to identify the syslog traffic that originates from a particular router, as coming from a single device, use the **logging source-interface** command in XR Config mode. To remove the source-interface logging configuration, use the **no** form of this command.

logging source-interface *interface*
no logging source-interface *interface*

Syntax Description

interface	Interface number of the source

Command Default

If *vrf-name* is not specified, the source interface is configured for the default VRF.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Normally, a syslog message contains the IPv4 or IPv6 address of the interface used to exit the router. The **logging source-interface** command configures the syslog packets to contain the IPv4 or IPv6 address of a particular interface , regardless of which interface the packet uses to exit the router.

Task ID

Task ID	Operation
logging	read, write

Example

This example shows how to configure interface loopback 0 to be the logging source interface for VRF vrf1.

```
RP/0/RP0/CPU0:router#logging source-interface loopback 0 vrf vrf1
RP/0/RP0/CPU0:router#logging source-interface loopback 1 vrf default
```

This sample output shows a logging source interface that is correctly configured for the VRF.

```
RP/0/RP0/CPU0:router#show running configuration logging

logging trap debugging
logging 223.255.254.249 vrf vrf1
logging 223.255.254.248 vrf default
logging source-interface Loopback0 vrf vrf1
logging source-interface Loopback1
```

ping (network)

To check host reachability and network connectivity on IP networks, use the **ping** command in XR EXEC mode.

ping [**ipv4** | **ipv6**] [*host-nameip-address*] [**count** *number*] [**size** *number*] [**source** {*ip-addressinterface-name* | **type** *number*}] [**timeout** *seconds*] [**pattern** *number*] [**type** *number*] [**priority** *number*][**verbose**] [**donnotfrag**] [**validate**] [**sweep**]

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.
A.B.C.D	Target end address of the pseudowire.
host-name	(Optional) Hostname of the system to ping.
ip-address	(Optional) IP address of the system to ping.
count *number*	(Optional) Sets the repeat count. Range is 0 to 2147483647.
size *number*	(Optional) Sets the datagram size. Range is 36 to 18024
source	(Optional) Identifies the source address or source interface.
type *number*	(Optional) Sets the type of service. Range is 0 to 255. Available when the **ipv4** keyword is specified.
timeout *seconds*	(Optional) Sets the timeout in seconds. Range is 0 to 3600.
priority *number*	(Optional) Sets the packet priority. Range is 0 to 15. Available when the **ipv6** keyword is specified.
pattern *number*	(Optional) Sets the data pattern. Range is 0 to 65535.
verbose	(Optional) Sets verbose output.
donnotfrag	(Optional) Sets the Don't Fragment (DF) bit in the IP header.
validate	(Optional) Validates the return packet.
sweep	(Optional) Sets the sweep ping.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The default value for the **ping** command refers only to the target IP address. No default value is available for the target IP address.

The ping program sends an echo request packet to an address and then waits for a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

Note The **ping** (EXEC) command is supported only on IP networks.

If you enter the command without specifying either a hostname or an IP address, the system prompts you to specify the target IP address and several other command parameters. After specifying the target IP address, you can specify alternate values for the remaining parameters or accept the displayed default for each parameter.

If the system cannot map an address for a hostname, it returns an "%Unrecognized host or address, or protocol not running" error message.

To abnormally terminate a ping session, enter the escape sequence, which is, by default, Ctrl-C. Simultaneously press and release the Ctrl and C keys.

This table describes the test characters sent by the ping facility.

Table 22: ping Test Characters

Character	Description
!	Each exclamation point indicates receipt of a reply.
.	Each period indicates that the network server timed out while waiting for a reply.
?	Unknown packet type.
U	A "destination unreachable" error protocol data unit (PDU) was received.
C	A "congestion experienced" packet was received.
M	Fragmentation is needed, but the "don't fragment" bit in the IP header is set. When this bit is set, the IP layer does not fragment the packet and returns an Internet Control Message Protocol (ICMP) error message to the source if the packet size is larger than the maximum transmission size. When this bit is not set, the IP layer fragments the packet to forward it to the next hop.
Q	A source quench packet was received.

Task ID

Task ID	Operations
basic-services	read, write, execute

Examples

Although the precise dialog varies somewhat between IPv4 and IPv6, all are similar to the ping session, using default values shown in the following output:

```
RP/0/RP0/CPU0:router# ping

Protocol [ipv4]:
Target IP address: 10.0.0.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
```

```
Extended commands? [no]: yes
Source address or interface: 10.0.0.2
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]: yes
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes? [no]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.25.58.21, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/11/49 ms
```

If you enter a hostname or an address on the same line as the **ping** command, the command performs the default actions appropriate for the protocol type of that hostname or address, as shown in the following output:

```
RP/0/RP0/CPU0:router# ping server01

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.27, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/9 ms
```

ping bulk (network)

To check reachability and network connectivity to multiple hosts on IP networks, use the **ping bulk** command in XR EXEC mode.

ping bulk ipv4 [**input cli** [**batch** | **inline**]]

Syntax Description

ipv4	Specifies IPv4 address prefixes.
input	Specifies input mode.
cli	Specifies input via CLI.
batch	Pings after all destinations are input.
inline	Pings after each destination is input.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

You must hit the Enter button and then specify one destination address per line.

Maximum number of destinations you can specify in the cli or batch mode is 2000.

Task ID

Task ID	Operation
basic-services	read, write, execute

Example

The following example shows how to ping many hosts by the input via CLI method:

```
RP/0/RP0/CPU0:router# ping bulk ipv4 input cli batch

Please enter input via CLI with one destination per line and when done Ctrl-D/(exit)
to initiate pings:
1: vrf myvrf1 10.2.1.16
2:
Starting pings...
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.1.16, vrf is myvrf1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/7/9 ms
```

```
RP/0/RP0/CPU0:router# ping bulk ipv4 input cli

Please enter input via CLI with one destination per line:
vrf myvrf1 1.1.1.1
vrf myvrf2 2.2.2.2
vrf myvrf1 myvrf1.cisco.com
vrf myvrf2 myvrf2.cisco.com

Starting pings...
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 1.1.1.1, vrf is myvrf1:
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 1/1/1 ms
Sending 2, 100-byte ICMP Echos to 2.2.2.2, vrf is myvrf2:
!!
Success rate is 100 percent (2/2), round-trip min/avg/max = 1/1/1 ms
Sending 1, 100-byte ICMP Echos to 1.1.1.1, vrf is myvrf1:
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 1/4/1 ms
Sending 2, 100-byte ICMP Echos to 2.2.2.2, vrf is myvrf2:
!!
Success rate is 100 percent (2/2), round-trip min/avg/max = 1/3/1 ms
```

scp

To securely transfer a file from a local directory to a remote directory or from a remote directory to a local directory, use the **scp** command in XR EXEC mode.

scp {*local-directory username@location/directory*} */ filename* {*username@location/directory local-directory* } */ filename*

Syntax Description

local-directory	Specifies the local directory on the device.
username@location/directory	Specifies the remote directory where *location* is the IP address of the remote device.
filename	Specifies the file name to be transferred.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Secure Copy Protocol (SCP) is a file transfer protocol which provides a secure and authenticated method for transferring files. SCP relies on SSHv2 to transfer files from a remote location to a local location or from local location to a remote location.

Use the **scp** command to copy a file from the local device to a destination device or from a destination device to the local device.

Using SCP, you can only transfer individual files. You cannot transfer a file from a remote device to another remote device.

SSH server process must be running on the remote device.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to copy a file using the **scp** command from a local directory to a remote directory:

```
RP/0/RP0/CPU0:router# scp /usr/file1.txt root@209.165.200.1:/root/file3.txt

Connecting to 209.165.200.1...
Password:
  Transferred 553065 Bytes
  553065 bytes copied in 0 sec (7576232)bytes/sec
```

The following example shows how to copy a file using the **scp** command from a remote directory to a local directory:

```
RP/0/RP0/CPU0:router# scp root@209.165.200.1:/root/file4.txt /usr/file.txt

Connecting to 209.165.200.1...
Password:
  Transferred 553065 Bytes
  553065 bytes copied in 0 sec (7576232)bytes/sec
```

show cinetd services

To display the services whose processes are spawned by Cinetd when a request is received, use the **show cinetd services** command in XR EXEC mode.

show cinetd services

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ip-services	read

Examples

The following is sample is output from the **show cinetd services** command:

```
RP/0/RP0/CPU0:router# show cinetd services

Vrf Name          Family Service Proto Port ACL max_cnt curr_cnt wait Program Client Option

context-management v4    telnet   tcp   23       100       0    nowait telnetd sysdb
default            v4    telnet   tcp   23       100       2    nowait telnetd sysdb
```

This table describes the significant fields shown in the display.

Table 23: show cinetd services Command Field Descriptions

Field	Description
Family	Version of the network layer (IPv4 or IPv6).
Service	Network service (for example, FTP, Telnet, and so on).
Proto	Transport protocol used by the service (tcp or udp).
Port	Port number used by the service.
ACL	Access list used to limit the service from some hosts.
max_cnt	Maximum number of concurrent servers allowed for a service.
curr_cnt	Current number of concurrent servers for a service.

Field	Description
wait	Status of whether Cinetd has to wait for a service to finish before serving the next request.
Program	Name of the program for a service.
Option	Service-specific options.

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, use the **show hosts** command in XR EXEC mode.

show hosts [*host-name*]

Syntax Description

host-name	(Optional) Name of the host about which to display information. If omitted, all entries in the local cache are displayed.

Command Default

Unicast address prefixes are the default when IPv4 address prefixes are configured.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ip-services	read

Examples

The following is sample output from the **show hosts** command:

```
RP/0/RP0/CPU0:router# show hosts

Default domain is cisco.com
Name/address lookup uses domain service
Name servers are 255.255.255.255
Host              Flags        Age(hr)    Type        Address(es)
host1.cisco.com    (temp, OK)     1          IP          192.168.4.10
abc               (perm, OK)     0          IP          10.0.0.0 10.0.0.2 10.0.0.3
```

This table describes the significant fields shown in the display.

Table 24: show hosts Command Field Descriptions

Field	Description
Default domain	Default domain used to complete the unqualified hostnames.
Name/address lookup	Lookup is disabled or uses domain services.
Name servers	List of configured name servers.
Host	Hostname.

Field	Description
Flags	Indicates the status of an entry. • temp—Temporary entry entered by a name server; the software removes the entry after 72 hours of inactivity. • perm—Permanent entry entered by a configuration command; does not time out. • OK—Entry is believed to be valid. • ??—Entry is considered suspect and subject to revalidation. • EX—Entry has expired.
Age(hr)	Number of hours since the software most recently referred to the cache entry.
Type	Type of address (IPv4 or IPv6).
Address(es)	Address of the host. One host may have up to eight addresses.

telnet

To log in to a host that supports Telnet, use the **telnet** command in XR EXEC mode.

telnet {*ip-addresshost-name*} [*options*]

Syntax Description

ip-address	IP address of a specific host on a network. • IPv4 address format—Must be entered in the (*x.x.x.x*) format. • IPv6 address format— Must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
host-name	Name of a specific host on a network.
options	(Optional) Telnet connection options. See Table 25: Telnet Connection Options, on page 284for a list of supported options.

Command Default

Telnet client is in Telnet connection options nostream mode.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

If the Telnet server is enabled, you should be able to start a Telnet session as long as you have a valid username and password.

This table lists the supported Telnet connection options.

Table 25: Telnet Connection Options

Option	Description
/stream	Turns on stream processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running UNIX-to-UNIX copy program (UUCP) and other non-Telnet protocols.
/nostream	Turns off stream processing.

Option	Description
port number	Port number. Range is 0 to 65535.
/source-interface	Specifies source interface.

To display a list of the available hosts, use the **show hosts** command. To display the status of all TCP connections, use the **show tcp** command.

The software assigns a logical name to each connection, and several commands use these names to identify connections. The logical name is the same as the hostname, unless that name is already in use or you change the connection name with the **name-connection** EXEC command. If the name is already in use, the software assigns a null name to the connection.

The Telnet software supports special Telnet commands in the form of Telnet sequences that map generic terminal control functions to operating system-specific functions. To issue a special Telnet command, enter the escape sequence and then a command character. The default escape sequence is Ctrl-^ (press and hold the Control and Shift keys and the 6 key). You can enter the command character as you hold down Ctrl or with Ctrl released; you can use either uppercase or lowercase letters. Table 26: Special Telnet Escape Sequences, on page 285 lists the special Telnet escape sequences.

Table 26: Special Telnet Escape Sequences

Escape Sequence[7]	Purpose
Ctrl-^ c	Interrupt Process (IP).
Ctrl-^ o	Terminate Output (AO).
Ctrl-^ u	Erase Line (EL).

[7] The caret (^) symbol refers to Shift-6 on your keyboard.

At any time during an active Telnet session, you can list the Telnet commands by pressing the escape sequence keys followed by a question mark at the system prompt:

ctrl-^?

A sample of this list follows. In this sample output, the first caret (^) symbol represents the Control key, and the second caret represents Shift-6 on your keyboard:

```
RP/0/RP0/CPU0:router# ^^?

[Special telnet escape help]
^^B  sends telnet BREAK
^^C  sends telnet IP
^^H  sends telnet EC
^^O  sends telnet AO
^^T  sends telnet AYT
^^U  sends telnet EL
```

You can have several concurrent Telnet sessions open and switch among them. To open a subsequent session, first suspend the current connection by pressing the escape sequence (Ctrl-Shift-6 and then x [Ctrl^x] by default) to return to the system command prompt. Then open a new connection with the **telnet** command.

To terminate an active Telnet session, issue any of the following commands at the prompt of the device to which you are connecting:

- close
- disconnect
- exit
- logout
- quit

Task ID

Task ID	Operations
basic-services	read, write, execute

Examples

The following example shows how to establish a Telnet session to a remote host named host1:

```
RP/0/RP0/CPU0:router# telnet host1
```

telnet client source-interface

To specify the source IP address for a Telnet connection, use the **telnet client source-interface** command in XR Config mode. To remove the **telnet client source-interface** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

telnet {**ipv4** | **ipv6**} **client source-interface** *type interface-path-id*
no telnet client source-interface *type interface-path-id*

Syntax Description

ipv4	Specifies IPv4 address prefixes.
ipv6	Specifies IPv6 address prefixes.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the show interfaces command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

The IP address of the best route to the destination is used as the source IP address.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **telnet client source-interface** command to set the IP address of an interface as the source for all Telnet connections.

Task ID

Task ID	Operations
ipv4	read, write
ip-services	read, write

Examples

The following example shows how to set the IP address for tenGigEinterface 1/0/2/1 as the source address for Telnet connections:

```
RP/0/RP0/CPU0:router(config)# telnet ipv4 client source-interface tengige1/0/2/1
```

telnet dscp

To define the differentiated services code point (DSCP) value and IPv4 precedence to specifically set the quality-of-service (QoS) marking for Telnet traffic on a networking device, use the **telnet dscp** command in XR Config mode. To disable DSCP, use the **no** form of this command.

telnet ipv4 dscp *dscp-value*
no telnet ipv4 dscp *dscp-value*

Syntax Description

ipv4	Specifies IPv4 address prefixes.
dscp-value	Value for DSCP. The range is from 0 to 63. The default value is 0.

Command Default

If DSCP is disabled or not configured, the following default values are listed:

- The default value for the server 16.
- The default value for the client is 0.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

IPv4 is the supported protocol for defining a DSCP value for locally originated Telnet traffic.

Task ID

Task ID	Operations
ipv4	read, write
ip-services	read, write

Examples

The following example shows how to define the DSCP value and IPv4 precedence:

```
RP/0/RP0/CPU0:router(config)# telnet ipv4 dscp 40
RP/0/RP0/CPU0:router(config)# telnet ipv4 dscp 10
```

telnet server

To enable Telnet services on a networking device, use the **telnet server** command in XR Config mode. To disable Telnet services, use the **no** form of this command.

telnet [**vrf** {*vrf-name* | **default**}] {**ipv4** | **ipv6**} **server max-servers** {**no-limit***limit*} [**access-list** *list-name*]
no telnet [**vrf** {*vrf-name* | **default**}] {**ipv4** | **ipv6**} **server max-servers** {**no-limit***limit*} [**access-list** *list-name*]

Syntax Description

vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) VRF name of the system to ping.
default	(Optional) Specifies the default VRF instance.
ipv4	Specifies IPv4 address prefixes.
ipv6	Specifies IPv6 address prefixes.
max-servers	Sets the number of allowable Telnet servers.
no-limit	Specifies that there is no maximum number of allowable Telnet servers.
limit	Specifies the maximum number of allowable Telnet servers. Range is 1 to 200.
access-list	(Optional) Specifies an access list.
list-name	(Optional) Access list name.

Command Default

Telnet services are disabled.

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Disable Telnet services to prevent inbound Telnet connections from being accepted into a networking device using the **telnet** command. After Telnet services are disabled, no new inbound connections are accepted, and the Cisco Internet services daemon (Cinetd) stops listening on the Telnet port.

Enable Telnet services by setting the **max-servers** keyword to a value of one or greater. This allows inbound Telnet connections into a networking device.

This command affects only inbound Telnet connections to a networking device. Outgoing Telnet connections can be made regardless of whether Telnet services are enabled.

Using the **no** form of the command disables the Telnet connection and restores the system to its default condition.



Note Before establishing communications with the router through a Telnet session, configure the telnet server and vty-pool functions (see the *Cisco ASR 9000 Series Aggregation Services Router* System Management Command *Reference* , the *Cisco ASR 9000 Series Aggregation Services Router* System Management Configuration Guide, and *Cisco ASR 9000 Series Aggregation Services Router* IP Addresses and Services Configuration Guide).

Task ID

Task ID	Operations
ipv4	read, write
ip-services	read, write

Examples

The following example shows how to enable Telnet services for one server:

```
RP/0/RP0/CPU0:router(config)# telnet ipv4 server max-servers 1
```

telnet transparent

To send a Carriage Return (CR) as a CR-NULL rather than a Carriage Return-Line Feed (CR-LF) for virtual terminal sessions, use the **telnet transparent** command in line template submode. To remove the **telnet transparent** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

telnet transparent
no telnet transparent

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

Line console

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **telnet transparent** command is useful for coping with different interpretations of end-of-line handling in the Telnet protocol specification.

Task ID

Task ID	Operations
tty-access	read, write

Examples

The following example shows how to configure the vty line to operate in Telnet transparent mode so that when the carriage return key is pressed the system sends the signal as a CR-NULL key combination rather than a CR-LF key combination:

```
RP/0/RP0/CPU0:router(config)# line console
RP/0/RP0/CPU0:router(config-line)# telnet transparent
```

tftp client source-interface

To specify the source IP address for a TFTP connection, use the **tftp client source-interface** command in XR Config mode. To remove the **tftp client source-interface** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

tftp client source-interface *type interface-path-id*
no tftp client source-interface *type interface-path-id*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the show interfaces command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

The IP address of the best route to the destination is used as the source IP address.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **tftp client source-interface** command to set the IP address of an interface as the source for all TFTP connections.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to set the IP address for tenGigE interface 1/0/2/1 as the source address for TFTP connections:

```
RP/0/RP0/CPU0:router(config)# tftp client source-interface tengige1/0/2/1
```

tftp server

To enable or disable the TFTP server or a feature running on the TFTP server, use the **tftp server** command in XR Config mode. To restore the system to its default condition, use the **no** form of this command.

tftp {**ipv4** | **ipv6**} **server homedir** *tftp-home-directory* [**max-servers** [*number* | **no-limit**]] [**access-list** *name*]
no tftp {**ipv4** | **ipv6**} **server homedir** *tftp-home-directory* [**max-servers** [*number* | **no-limit**]] [**access-list** *name*]

Syntax Description

ipv4	Specifies IPv4 address prefixes.
ipv6	Specifies IPv6 address prefixes.
homedir *tftp-home-directory*	Specifies the home directory.
max-servers *number*	(Optional) Sets the maximum number of concurrent TFTP servers. The range is from 1 to 2147483647.
max-servers no-limit	(Optional) Sets no limit to process a number of allowable TFTP server.
access-list *name*	(Optional) Specifies the name of the access list associated with the TFTP server.

Command Default

The TFTP server is disabled by default. When not specified, the default value for the **max-servers** keyword is unlimited.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Using the **no** form of the **tftp server** command removes the specified command from the configuration file and restores the system to its default condition. The **no** form of the command is not stored in the configuration file.

Task ID

Task ID	Operations
ipv4	read, write
ip-services	read, write

Examples

The following example shows that the TFTP server is enabled for the access list named test:

```
RP/0/RP0/CPU0:router(config)# tftp ipv4 server homedir disk0 access-list test
```

traceroute

To discover the routes that packets actually take when traveling to their destination across an IP network, use the **traceroute** command in XR EXEC mode.

traceroute [**ipv4** | **ipv6**] [*host-nameip-address*] [{**source***ip-address-nameinterface-name*}] [**numeric**] [**timeout** *seconds*] [**probe** *count*] [**minttl** *seconds*] [**maxttl** *seconds*] [**port** *number*] [**priority** *number*] [**verbose**]

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.
ipv6	(Optional) Specifies IPv6 address prefixes.
host-name	(Optional) Hostname of system to use as the destination of the trace attempt.
ip-address	(Optional) Address of system to use as the destination of the trace attempt.
source	(Optional) Source address.
ip-address-name	(Optional) IP address A.B.C.D or hostname.
numeric	(Optional) Numeric display only.
timeout *seconds*	(Optional) Timeout value. Range is 0 to 3600.
probe *count*	(Optional) Probe count. Range is 0 to 65535.
minttl *seconds*	(Optional) Minimum time to live. Range is 0 to 255.
maxttl *seconds*	(Optional) Maximum time to live. Range is 0 to 255.
port *number*	(Optional) Port number. Range is 0 to 65535.
priority *number*	(Optional) Packet priority. Range is 0 to 15. Available when the **ipv6** keyword is specified.
verbose	(Optional) Verbose output.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The default value for the **traceroute** command refers only to the destination. No default value is available for the destination address.

The **traceroute** command works by taking advantage of the error messages generated by networking devices when a datagram exceeds its time-to-live (TTL) value.

The **traceroute** command starts by sending probe datagrams with a TTL value of 1, which causes the first networking device to discard the probe datagram and send back an error message. The **traceroute** command sends several probes at each TTL level and displays the round-trip time for each.

The **traceroute** command sends out one probe at a time. Each outgoing packet may result in one or two error messages. A "time-exceeded" error message indicates that an intermediate networking device has seen and discarded the probe. A "destination-unreachable" error message indicates that the destination node has received the probe and discarded it because it could not deliver the packet. If the timer goes off before a response comes in, the **traceroute** command prints an asterisk (*).

The **traceroute** command terminates when the destination responds, when the maximum TTL is exceeded, or when the user interrupts the trace with the escape sequence, which is, by default, Ctrl-C. Simultaneously press and release the Ctrl and C keys.

To use nondefault parameters and invoke an extended **traceroute** test, enter the command without a *host-name* or *ip- address* argument. You are stepped through a dialog to select the desired parameter values for the **traceroute** test.

Because of how IP is implemented on various networking devices, the IP **traceroute** command may behave in unexpected ways.

Not all destinations respond correctly to a probe message by sending back an "ICMP port unreachable" message. A long sequence of TTL levels with only asterisks, terminating only when the maximum TTL has been reached, may indicate this problem.

There is a known problem with the way some hosts handle an "ICMP TTL exceeded" message. Some hosts generate an "ICMP" message, but they reuse the TTL of the incoming packet. Because this value is zero, the ICMP packets do not succeed in returning. When you trace the path to such a host, you may see a set of TTL values with asterisks (*). Eventually the TTL is raised high enough that the "ICMP" message can get back. For example, if the host is six hops away, the **traceroute** command times out on responses 6 through 11.

Task ID

Task ID	Operations
basic-services	read, write, execute

Examples

The following output shows a sample **traceroute** session when a destination hostname has been specified:

```
RP/0/RP0/CPU0:router# traceroute host8-sun

Type escape sequence to abort.
Tracing the route to 192.168.0.73
 1 192.168.1.6 (192.168.1.6) 10 msec 0 msec 10 msec
 2 gateway01-gw.gateway.cisco.com (192.168.16.2) 0 msec 10 msec 0 msec
 3 host8-sun.cisco.com (192.168.0.73) 10 msec * 0 msec
```

The following display shows a sample extended **traceroute** session when a destination hostname is not specified:

```
traceroute# traceroute

Protocol [ipv4]:
Target IP address: ena-view3
Source address: 10.0.58.29
Numeric display? [no]:
Timeout in seconds [3]:
```

```
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:

Type escape sequence to abort.
Tracing the route to 171.71.164.199
 1  sjc-jpxlnock-vpn.cisco.com (10.25.0.1) 30 msec  4 msec  4 msec
 2  15lab-vlan725-gx1.cisco.com (173.19.72.2) 7 msec  5 msec  5 msec
 3  stc15-00lab-gw1.cisco.com (173.24.114.33) 5 msec  6 msec  6 msec
 4  stc5-lab4-gw1.cisco.com (173.24.114.89) 5 msec  5 msec  5 msec
 5  stc5-sbb4-gw1.cisco.com (172.71.241.162) 5 msec  6 msec  6 msec
 6  stc5-dc5-gw1.cisco.com (172.71.241.10) 6 msec  6 msec  5 msec
 7  stc5-dc1-gw1.cisco.com (172.71.243.2) 7 msec  8 msec  8 msec
 8  ena-view3.cisco.com (172.71.164.199) 6 msec  *  8 msec
```

This table describes the characters that can appear in traceroute output.

Table 27: traceroute Text Characters

Character	Description
xx msec	For each node, the round-trip time in milliseconds for the specified number of probes.
*	Probe time out.
?	Unknown packet type.
A	Administratively unreachable. This output usually indicates that an access list is blocking traffic.
H	Host unreachable.
N	Network unreachable.
P	Protocol unreachable.
Q	Source quench.
U	Port unreachable.



HSRP Commands

This chapter describes the Cisco IOS XR software commands used to configure and monitor the Hot Standby Router Protocol (HSRP) features.

For detailed information about HSRP concepts, configuration tasks, and examples, refer to the *IP Addresses and Services Configuration Guide for Cisco NCS 5000 Series Routers*.

- address (hsrp), on page 299
- address global (HSRP), on page 301
- address global subordinate (HSRP), on page 303
- address linklocal(HSRP), on page 305
- address secondary (hsrp), on page 307
- authentication (hsrp), on page 309
- clear hsrp statistics, on page 311
- hsrp authentication, on page 312
- hsrp delay, on page 314
- hsrp ipv4, on page 316
- mac-address (hsrp), on page 318
- hsrp priority, on page 320
- hsrp redirects, on page 322
- hsrp timers, on page 323
- hsrp track, on page 325
- hsrp use-bia, on page 327
- interface (HSRP), on page 328
- preempt (hsrp), on page 330
- priority (hsrp), on page 332
- router hsrp, on page 334
- session name, on page 335
- show hsrp, on page 337
- show hsrp mgo, on page 340
- show hsrp statistics, on page 342
- show hsrp summary, on page 344
- hsrp slave follow, on page 346
- subordinate primary virtual IPv4 address, on page 347
- subordinate secondary virtual IPv4 address, on page 348
- subordinate virtual mac address, on page 349

- timers (hsrp), on page 350
- track (hsrp), on page 352
- track(object), on page 354

address (hsrp)

To enable hot standby protocol for IP, use the **address (hsrp)** command in the HSRP group submode. To disable hot standby protocol for IP, use the **no** form of this command.

address { **learn** *address* }
no address { **learn** *address* }

Syntax Description

learn	Learns virtual IP address from peer.
address	Hot standby IP address.

Command Default

None

Command Modes

HSRP Group Submode

Command History

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
hsrp	read, write

Example

This example shows how to enable a group to learn the primary virtual IPv4 address from received HSRP control packets:

```
Router# configure
Router(config)# router hsrp
Router(config-hsrp)# interface tenGigE hundredgige 0/4/0/4
Router(config-hsrp-if)# address-family ipv4
Router(config-hsrp-ipv4)# hsrp 1 version 2
Router(config-hsrp-gp)# address learn
Router(config-hsrp-gp)#
```



Note

- The **version** keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families.
- The HSRP version 2 extended group range must be restricted to 0-255, even though the configuration up to 0-4095 is accepted.



Note Starting with IOS XR Release 7.4.1, the HSRP version 2 extended group range configurable in the router is restricted to 0-255.

Related Commands

Command	Description
address secondary (hsrp), on page 307	Configures the secondary virtual IPv4 address for a virtual router.

address global (HSRP)

To configure the global virtual IPv6 address for the HSRP group, use the **address global** command in the virtual router submode. To deconfigure the global virtual IPv6 address for the HSRP group, use the **no** form of this command.

address global *ipv6-address*

no address global *ipv6-address*

Syntax Description

ipv6-address	Global HSRP IPv6 address.

Command Default

None

Command Modes

HSRP Group Submode, under the IPv6 address-family

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
hsrp	read,write

Example

This example shows how to add a global virtual IPv6 address for the HSRP group:

```
Router# configure
Router(config)# router hsrp
Router(config-hsrp)# interface tenGigE 0/4/0/4
Router(config-hsrp-if)# address-family ipv6
Router(config-hsrp-address-family)# hsrp 3
Router(config-hsrp-virtual-router)# address global 4000::1000
Router(config-hsrp-virtual-router)#
```

Note

- The **version** keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families.
- The HSRP version 2 extended group range must be restricted to 0-255, even though the configuration up to 0-4095 is accepted.



Note Starting with IOS XR Release 7.4.1, the HSRP version 2 extended group range configurable in the router is restricted to 0-255.

address global subordinate (HSRP)

To configure the global virtual IPv6 address for the subordinate group, use the **address global** command in the HSRP slave submode. To deconfigure the global virtual IPv6 address for the subordinate group, use the **no** form of this command.

address global *ipv6-address*

no address global *ipv6-address*

Syntax Description

ipv6-address	Global VRRP IPv6 address.

Command Default

None

Command Modes

HSRP Slave Submode, under the IPv6 address-family

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
hsrp	read,write

Example

This example shows how to add a global virtual IPv6 address for the subordinate group:

```
Router# configure
Router(config)# router hsrp
Router(config-hsrp)# interface tenGigE 0/4/0/4
Router(config-hsrp-if)# address-family ipv6
Router(config-hsrp-address-family)# hsrp 3 slave
Router(config-hsrp-virtual-router)# address global 4000::1000
Router(config-hsrp-virtual-router)#
```



Note

- The **version** keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families.
- The HSRP version 2 extended group range must be restricted to 0-255, even though the configuration up to 0-4095 is accepted.



Note Starting with IOS XR Release 7.4.1, the HSRP version 2 extended group range configurable in the router is restricted to 0-255.

address linklocal(HSRP)

To either configure the virtual link-local IPv6 address for the HSRP group or to specify that the virtual link-local IPv6 address should be enabled and calculated automatically from the virtual router virtual Media Access Control (MAC) address, use the **address linklocal** command in the HSRP group submode, under the IPv6 address-family. To deconfigure the virtual link-local IPv6 address forthe HSRP group, use the **no** form of this command.

address linklocal
ipv6-address | **autoconfig**

no address linklocal
ipv6-address | **autoconfig**

Syntax Description

ipv6-address	HSRP IPv6 link-local address.
autoconfig	Autoconfigures the HSRP IPv6 link-local address.

Command Default

None

Command Modes

HSRP Group Submode, under the IPv6 address-family

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

When you configure HSRP for IPv6, you must also configure the linklocal IPv6 address using either the *ipv6-address* argument or the **autoconfig** keyword. If you configure only the global IPv6 address and commit the changes using the **commit** keyword, the router does not accept the configuration and displays an error message.

Task ID

Task ID	Operation
hsrp	read, write

Example

This example shows how to autoconfigure the HSRP IPv6 link-local address:

```
Router# configure
Router(config)# router hsrp
Router(config-hsrp)# interface tenGigE 0/4/0/4
Router(config-hsrp-if)# address-family ipv6
Router(config-hsrp-address-family)# hsrp 3 version 2
Router(config-hsrp-virtual-router)# address linklocal autoconfig
```

```
Router(config-hsrp-virtual-router)#
```

This example shows how to configure the virtual link-local IPv6 address for the HSRP group:

```
Router# configure
Router(config)# router hsrp
Router(config-hsrp)# interface tenGigE 0/4/0/4
Router(config-hsrp-if)# address-family ipv6
Router(config-hsrp-address-family)# hsrp 3
Router(config-hsrp-virtual-router)# address linklocal FE80::260:3EFF:FE11:6770
Router(config-hsrp-virtual-router)#
```



Note

- The **version** keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families.
- The HSRP version 2 extended group range must be restricted to 0-255, even though the configuration up to 0-4095 is accepted.



Note Starting with IOS XR Release 7.4.1, the HSRP version 2 extended group range configurable in the router is restricted to 0-255.

address secondary (hsrp)

To configure the secondary virtual IPv4 address for a virtual router, use the **address secondary** command in the Hot Standby Router Protocol (HSRP) virtual router submode. To deconfigure the secondary virtual IPv4 address for a virtual router, use the **no** form of this command.

address *address* **secondary**
no address *address* **secondary**

Syntax Description

secondary	Sets the secondary HSRP IP address.
address	HSRP IPv4 address.

Command Default

None

Command Modes

HSRP virtual router

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
hsrp	read, write

Example

This example shows how to set the secondary virtual IPv4 address for the virtual router:

```
Router# configure
Router(config)# router hsrp
Router(config-hsrp)# interface tenGigE 0/4/0/4
Router(config-hsrp-if)# address-family ipv4
Router(config-hsrp-ipv4)# hsrp 3 version 2
Router(config-hsrp-gp)# address 10.20.30.1 secondary
Router(config-hsrp-gp)#
```

Note

- The **version** keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families.
- The HSRP version 2 extended group range must be restricted to 0-255, even though the configuration up to 0-4095 is accepted.



Note Starting with IOS XR Release 7.4.1, the HSRP version 2 extended group range configurable in the router is restricted to 0-255.

authentication (hsrp)

To configure an authentication string for the Hot Standby Router Protocol (HSRP), use the **hsrp authentication** command in HSRP group submode. To delete an authentication string, use the **no** form of this command.

authentication *string*
no authentication [*string*]

Syntax Description

string	Authentication string. It can be up to eight characters long. The default is 'cisco'.

Command Default

The default authentication string is cisco.

Command Modes

HSRP Group Submode

Command History

Release	Modification
Release 7.1.1	This command was introduced. This command replaces the **hsrp authentication** command.

Usage Guidelines

The authentication string is sent unencrypted in all HSRP messages. The same authentication string must be configured on all routers and access servers on a LAN to ensure interoperation. Authentication mismatch prevents a device from learning the designated Hot Standby IP address and the Hot Standby timer values from other routers configured with HSRP.

The **hsrp authentication** command is available for version 1 groups only

Task ID

Task ID	Operations
hsrp	read, write

Examples

This example shows how to configure “company1” as the authentication string required to allow Hot Standby routers in group 1 on tengige hundredgige interface 0/4/0/4 to interoperate:

```
Router# configure
Router(config)# router hsrp
Router(config-hsrp)# interface tenGigE 0/4/0/4
Router(config-hsrp-if)# address-family ipv4
Router(config-hsrp-ipv4)# hsrp 1 version 1
Router(config-hsrp-gp)# authentication company1
Router(config-hsrp-gp)#
```

Note The **version** keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families.

Related Commands

Command	Description
show hsrp, on page 337	Displays HSRP information.

clear hsrp statistics

To reset the Hot Standby Routing Protocol Statistics (HSRP) statistics to zero, use the **clear hsrp statistics** command in XR EXEC mode.

clear hsrp statistics [**interface** *interface-type interface-path-id group*]

Syntax Description

interface *interface-path-id*	Physical interface or virtual interface. **Note** Use the show interfaces command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
group	(Optional) Group number.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
hsrp	read, write

Example

This sample output is from the **clear hsrp statistics** command:

```
Router# clear hsrp statistics
```

Related Commands

Command	Description
show hsrp, on page 337	Displays HSRP information.

hsrp authentication

To configure an authentication string for the Hot Standby Router Protocol (HSRP), use the **hsrp authentication** command in HSRP interface configuration mode. To delete an authentication string, use the **no** form of this command.

hsrp [*group-number*] **authentication** *string*
no hsrp [*group-number*] **authentication** [*string*]

Syntax Description

group-number	(Optional) Group number on the interface to which this authentication string applies. Default is 0.
string	Authentication string. It can be up to eight characters long. The default is 'cisco'.

Command Default

The default group number is 0.

The default authentication string is cisco.

Command Modes

HSRP interface configuration

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

The authentication string is sent unencrypted in all HSRP messages. The same authentication string must be configured on all routers and access servers on a LAN to ensure interoperation. Authentication mismatch prevents a device from learning the designated Hot Standby IP address and the Hot Standby timer values from other routers configured with HSRP.

Task ID

Task ID	Operations
hsrp	read, write

Examples

This example shows how to configure “company1” as the authentication string required to allow Hot Standby routers in group 1 on Ten Gigabit Ethernet interface 0/2/0/1 to interoperate:

```
Router(config)# router hsrp
Router(config-hsrp)# interface TenGigE 0/2/0/1
Router(config-hsrp-if)# hsrp 1 authentication company1
```

Related Commands

Command	Description
show hsrp, on page 337	Displays HSRP information.

hsrp delay

To configure the activation delay for the Hot Standby Router Protocol (HSRP), use the **hsrp delay** command in HSRP interface configuration mode. To delete the activation delay, use the **no** form of this command.

hsrp delay minimum *value* **reload** *value*
no hsrp delay

Syntax Description

minimum *value*	Sets the minimum delay in seconds for every interface up event. Range is 0 to 10000.
reload *value*	Sets the reload delay in seconds for first interface up event. Range is 0 to 10000.

Command Default

minimum *value* : 1

reload *value* : 5

Command Modes

HSRP interface configuration

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

The **hsrp delay** command delays the start of the HSRP finite state machine (FSM) on an interface up event to ensure that the interface is ready to pass traffic. This ensures that there are no mistaken state changes due to loss of hello packets. The minimum delay is applied on all interface up events and the reload delay is applied on the first interface event.

The values of zero must be explicitly configured to turn this feature off.

Task ID

Task ID	Operations
hsrp	read, write

Examples

The following example shows how to configure a minimum delay of 10 seconds with a reload delay of 100 seconds:

```
Router(config)# router hsrp
Router(config-hsrp)# interface tenGigE 0/RP0/CPU0/0
Router(config-hsrp-if)# hsrp delay minimum 10 reload 100
```

Related Commands

Command	Description
show hsrp, on page 337	Displays HSRP information.

hsrp ipv4

To activate the Hot Standby Router Protocol (HSRP), use the **hsrp ipv4** command in HSRP interface configuration mode. To disable HSRP, use the **no** form of this command.

hsrp ipv4 [*ip-address* [**secondary**]]
no hsrp *group-number* **ipv4** [*ip-address* [**secondary**]]

Syntax Description

group-number	(Optional) Group number on the interface for which HSRP is being activated. Range is 0 to 255. Default is 0.
ip-address	(Optional) IP address of the Hot Standby router interface.
secondary	(Optional) Indicates that the IP address is a secondary Hot Standby router interface. Useful on interfaces with primary and secondary addresses; you can configure primary and secondary HSRP addresses.

Command Default

group-number : 0

HSRP is disabled by default.

Command Modes

HSRP interface configuration

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

The **hsrp ipv4** command activates HSRP on the configured interface. If an IP address is specified, that address is used as the designated address for the Hot Standby group. If no IP address is specified, the virtual address is learned from the active router. For HSRP to elect a designated router, at least one router in the Hot Standby group must have been configured with, or must have learned, the designated address. Configuring the designated address on the active router always overrides a designated address that is currently in use.

When the **hsrp ipv4** command is enabled on an interface, the handling of proxy Address Resolution Protocol (ARP) requests is changed (unless proxy ARP was disabled). If the Hot Standby state group has been configured with or has learned the designated address, the proxy ARP requests are answered using the MAC address of the Hot Standby group. Otherwise, proxy ARP responses are suppressed.

Configuring secondary Hot Standby router IP addresses is necessary when the interface has secondary IP addresses configured and redundancy must be provided for the networks of these addresses also.

A primary address must be configured before a secondary address. Likewise, a secondary address must be unconfigured before unconfiguring a primary address. All IP addresses can be unconfigured using the **no hsrp ipv4** command.

Task ID

Task ID	Operations
hsrp	read, write

Examples

The following example shows how to activate HSRP for group 1 on tengige interface 0/2/0/1. The IP address used by the Hot Standby group is learned using HSRP.

```
Router(config)# router hsrp
Routerrouter(config-hsrp)# interface tenGigE 0/2/0/1
Router(config-hsrp-if)# hsrp 1 ipv4
```

Related Commands

Command	Description
hsrp redirects, on page 322	Configures ICMP redirect messages to be sent when the HSRP is configured on an interface.
show hsrp, on page 337	Displays HSRP information.

mac-address (hsrp)

To specify a virtual MAC address for the Hot Standby Router Protocol (HSRP), use the **hsrp mac-address** command in HSRP group submode. To revert to the standard virtual MAC address (0000.0C07.AC*n)*, use the **no** form of this command.

mac-address *address*
no mac-address

Syntax Description

address	MAC address.

Command Default

If this command is not configured, and the **hsrp use-bia** command is not configured, the standard virtual MAC address is used: 0000.0C07.AC*n*, where *n* is the group number in hexadecimal. This address is specified in RFC 2281, *Cisco Hot Standby Router Protocol (HSRP)*.

Command Modes

HSRP group submode

Command History

Release	Modification
Release 6.1.2	This command was introduced. This command replaces the **hsrp mac-address** command

Usage Guidelines

The **hsrp mac-address** command is not recommended except for IBM networking environments in which first-hop redundancy is based on being able to use a virtual MAC address and in which you cannot change the first-hop addresses in the PCs that are connected to an Ethernet switch.

HSRP is used to help end stations locate the first-hop gateway for IP routing. The end stations are configured with a default gateway. However, HSRP can provide first-hop redundancy for other protocols. Some protocols, such as Advanced Peer-to-Peer Networking (APPN), use the MAC address to identify the first-hop for routing purposes. In this case, it is often necessary to specify the virtual MAC address; the virtual IP address is unimportant for these protocols.

Use the **hsrp mac-address** command to specify the virtual MAC address. The MAC address specified is used as the virtual MAC address when the router is active. This command is intended for certain APPN configurations.

This table shows the parallel terms between APPN and IP.

Table 28: APPN and IP Parallel Terms

APPN	IP
end node	host
network node	router or gateway

Note In an APPN network, an end node is typically configured with the MAC address of the adjacent network node. Use the **hsrp mac-address** command in the routers to set the virtual MAC address to the value used in the end nodes.

Task ID

Task ID	Operations
hsrp	read, write

Examples

If the end nodes are configured to use 4000.1000.1060 as the MAC address of the network node, the command to configure the virtual MAC address is as follows:

```
Router# configure
Router(config)# router hsrp
Router(config-hsrp)# interface HundredGigE 0/4/0/4
Router(config-hsrp-if)# address-family ipv4
Router(config-hsrp-ipv4)# hsrp 1 version 2
Router(config-hsrp-gp)# mac-address 4000.1000.1060
Router(config-hsrp-gp)#
```

Note
- The **version** keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families.
- HSRP version 2 provides an extended group range of 0-4095.

Related Commands

Command	Description
show hsrp, on page 337	Displays HSRP information.

hsrp priority

To configure Hot Standby Router Protocol (HSRP) priority, use the **hsrp priority** command in HSRP interface configuration mode. To restore the default values, use the **no** form of this command.

hsrp [*group-number*] **priority** *priority*
no hsrp [*group-number*] **priority** *priority*

Syntax Description

group-number	(Optional) Group number on the interface to which the priority applies. Default is 0.
priority	Priority value that prioritizes a potential Hot Standby router. Range is 1 to 255. Default is 100.

Command Default

group-number: 0

priority: 100

Command Modes

HSRP interface configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

The assigned priority is used to help select the active and standby routers. Assuming that preemption is enabled, the router with the highest priority becomes the designated active router. In case of ties, the interface IP addresses are compared, and the interface with the higher IP address has priority.

The priority of the device can change dynamically if an interface is configured with the **hsrp track** command and another interface on the device goes down.

If preemption is not enabled, the router may not become active even though it might have a higher priority than other HSRP routers.

Task ID

Task ID	Operations
hsrp	read, write

Examples

In the following example, the router has a priority of 120:

```
Router(config)# router hsrp
Router(config-hsrp)# interface TenGigE 0/2/0/1
Router(config-hsrp-if)# hsrp ipv4 192.168.18.1
Router(config-hsrp-if)# hsrp priority 120
```

Related Commands

Command	Description
hsrp preempt	Configures HSRP preemption and preemption delay.
hsrp track	Configures an interface so that the Hot Standby priority changes based on the availability of other interfaces.
show hsrp, on page 337	Displays HSRP information.

hsrp redirects

To configure Internet Control Message Protocol (ICMP) redirect messages to be sent when the Hot Standby Router Protocol (HSRP) is configured on an interface, use the **hsrp redirects** command in HSRP interface configuration mode. To revert to the default, which is that ICMP messages are enabled, use the **no** form of this command.

hsrp redirects disable
no hsrp redirects disable

Syntax Description

disable	Disables the filtering of ICMP redirect messages on interfaces configured with HSRP.

Command Default

HSRP ICMP redirects are enabled by default.

Command Modes

HSRP interface configuration

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

The **hsrp redirects** command can be configured on a per-interface basis. When HSRP is first configured on an interface, the setting for that interface inherits the global value. With the **hsrp redirects** command is enabled, ICMP redirects messages are filtered by replacing the real IP address in the next-hop address of the redirect packet with a virtual IP address if it is known to HSRP.

Task ID

Task ID	Operations
hsrp	read, write

Examples

The following example shows how to allow HSRP to filter redirect messages on tengige interface 0/2/0/1:

```
Router(config)# router hsrp
Router(config-hsrp)# interface tenGigE 0/2/0/1
Router(config-hsrp-if)# hsrp 1 ipv4 192.168.18.1
Router(config-hsrp-if)# hsrp redirects disable
```

Related Commands

Command	Description
show hsrp, on page 337	Displays HSRP information.

hsrp timers

To configure the time between hello packets and the time before other routers declare the active Hot Standby or standby router to be down, use the **hsrp timers** command in HSRP interface configuration mode. To restore the timers to their default values, use the **no** form of this command.

hsrp [*group-number*] **timers** { *hello-seconds* | **msec** *hello-milliseconds* } { *hold-seconds* | **msec** *hold-milliseconds* }
no hsrp [*group-number*] **timers**

Syntax Description

group-number	(Optional) Group number on the interface to which the timers apply. Default is 0.
hello-seconds	Hello interval in seconds. Range is 1 to 255. Default is 3 seconds.
msec *hello-milliseconds*	Hello interval in milliseconds. Range is 100 to 3000 milliseconds.
hold-seconds	Time in seconds before the active or standby router is declared to be down. Range is 1 to 255. Default is 10 seconds.
msec *hold-milliseconds*	Time in milliseconds before the active or standby router is declared to be down. Range is 100 to 3000 milliseconds.

Command Default

group-number: 0

hello-seconds: 3 seconds (If the **msec** keyword is specified, there is no default value.)

hold-seconds: 10 seconds (If the **msec** keyword is specified, there is no default value.)

Command Modes

HSRP interface configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

Nonactive routers learn timer values from the active router, unless millisecond timer values are being used. If millisecond timer values are being used, all routers must be configured with the millisecond timer values. This rule applies if either the hello time or the hold time is specified in milliseconds.

The timers configured on the active router always override any other timer settings. All routers in a Hot Standby group should use the same timer values. Normally, the hold time is greater than or equal to three times the hello time (holdtime > 3 * hellotime).

You must specify either the *hello-seconds* argument or the **msec** keyword and *hello-milliseconds* argument, depending on whether you want the hello time in seconds or milliseconds. You must also specify either the *hold-seconds* argument or **msec** keyword and *hold-milliseconds* argument, depending on whether you want the hold time in seconds or milliseconds.

Task ID

Task ID	Operations
hsrp	read, write

Examples

The following example shows how to set, for group number 1 on Ten Gigabit Ethernet interface 0/2/0/1, the time between hello packets to 5 seconds and the time after which a router is considered to be down to 15 seconds. The configured timer values are used only if the router is active (or before they have been learned).

```
Router(config)# router hsrp
Router(config-hsrp)# interface TenGigE 0/2/0/1
Router(config-hsrp-if)# hsrp 1 ipv4
Router(config-hsrp-if)# hsrp 1 timers 5 15
```

The following example shows how to set, for group number 1 on Ten Gigabit Ethernet interface 0/2/0/1, the time between hello packets to 200 milliseconds and the time after which a router is considered to be down to 1000 milliseconds. The configured timer values are always used because milliseconds have been specified.

```
Router(config)# router hsrp
Router(config-hsrp)# interface TenGigE 0/2/0/1
Router(config-hsrp-if)# hsrp 1 ipv4
Router(config-hsrp-if)# hsrp 1 timers msec 200 msec 1000
```

Related Commands

Command	Description
show hsrp, on page 337	Displays HSRP information.

hsrp track

To configure an interface so that the Hot Standby priority changes on the basis of the availability of other interfaces, use the **hsrp track** command in HSRP interface configuration mode. To remove the tracking, use the **no** form of this command.

hsrp [*group-number*] **track** *type interface-path-id* [*priority-decrement*]
no hsrp [*group-number*] **track** *type interface-path-id* [*priority-decrement*]

Syntax Description

group-number	(Optional) Group number on the interface to which the tracking applies. Default is 0.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the show interfaces command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
priority-decrement	(Optional) Amount by which the Hot Standby priority for the router is decremented (or incremented) when the interface goes down (or comes back up). Range is 1 to 255.

Command Default

group-number: 0

priority-decrement: 10

Command Modes

HSRP interface configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

The **hsrp track** command ties the Hot Standby priority of the router to the availability of its interfaces. It is useful for tracking interfaces that are not configured for the Hot Standby Router Protocol (HSRP). Only IP interfaces are tracked. A tracked interface is up if IP on that interface is up. Otherwise, the tracked interface is down.

When a tracked interface goes down, the Hot Standby priority decreases by 10. If an interface is not tracked, its state changes do not affect the Hot Standby priority. For each group configured for Hot Standby, you can configure a separate list of interfaces to be tracked.

The optional *priority-decrement* argument specifies by how much to decrement the Hot Standby priority when a tracked interface goes down. When the tracked interface comes back up, the priority is incremented by the same amount.

When multiple tracked interfaces are down and *priority-decrement* values have been configured, these configured priority decrements are cumulative. If tracked interfaces are down, but none of them were configured with priority decrements, the default decrement is 10 and it is cumulative.

The **hsrp preempt** command must be used in conjunction with this command on all routers in the group whenever the best available router should be used to forward packets. If the **hsrp preempt** command is not used, then the active router stays active, regardless of the current priorities of the other HSRP routers.

Task ID

Task ID	Operations
hsrp	read, write

Examples

In the following example, Ten Gigabit Ethernet interface 0/2/0/1 tracks interface 0/1/0/1 and 0/3/0/1. If one or both of these two interfaces go down, the Hot Standby priority of the router decreases by 10. Because the default Hot Standby priority is 100, the priority becomes 90 when one of the tracked interfaces goes down and the priority becomes 80 when both go down.

```
Router(config)# router hsrp
Router(config-hsrp)# interface TenGigE 0/2/0/1
Router(config-hsrp-if)# hsrp track TenGigE 0/1/0/1
Router(config-hsrp-if)# hsrp track TenGigE 0/3/0/1
Router(config-hsrp-if)# hsrp preempt
Router(config-hsrp-if)# hsrp ipv4 192.92.72.46
```

Related Commands

Command	Description
hsrp preempt	Configures HSRP preemption and preemption delay.
hsrp priority	Configures HSRP priority.
show hsrp, on page 337	Displays HSRP information.

hsrp use-bia

To configure the Hot Standby Router Protocol (HSRP) to use the burned-in address of the interface as its virtual MAC address, instead of the preassigned MAC address or the functional address, use the **hsrp use-bia** command in HSRP interface configuration mode. To restore the default virtual MAC address, use the **no** form of this command.

hsrp use-bia
no hsrp use-bia

Command Default

HSRP uses the preassigned MAC address on Ethernet.

Command Modes

HSRP interface configuration

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

It is desirable to configure the **hsrp use-bia** command on an interface if there are devices that reject Address Resolution Protocol (ARP) replies with source hardware addresses set to a functional address.

Task ID

Task ID	Operations
hsrp	read, write

Examples

In the following example, the burned-in address of tengige interface 0/2/0/1 will be the virtual MAC address mapped to the virtual IP address for all Hot Standby groups configured on tengige interface 0/1/0/1:

```
Router(config)# router hsrp
Router(config-hsrp)# interface tenGigE 0/2/0/1
Router(config-hsrp-if)# hsrp use-bia
```

Related Commands

Command	Description
show hsrp, on page 337	Displays HSRP information.

interface (HSRP)

To enable Hot Standby Router Protocol (HSRP) interface configuration command mode, use the **interface** command in router configuration mode. To terminate interface mode, use the **no** form of this command.

interface *type interface-path-id*
no interface *type interface-path-id*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the show interfaces command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

HSRP is disabled.

Command Modes

Router HSRP configuration

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

All the commands used to configure HSRP are used in HSRP interface configuration mode.

Task ID

Task ID	Operations
hsrp	read, write

Examples

The following example show how to enable HSRP interface configuration mode on tengige 0/2/0/1:

```
Router(config)# router hsrp
Router(config-hsrp)# interface tenGigE 0/2/0/1
Router(config-hsrp-if)#
```

Related Commands

Command	Description
router hsrp, on page 334	Enables HSRP.

preempt (hsrp)

To configure Hot Standby Router Protocol (HSRP) preemption and preemption delay, use the **hsrp preempt** command in HSRP interface configuration mode. To restore the default values, use the **no** form of this command.

hsrp [*group-number*] **preempt** [**delay** *seconds*]
no hsrp [*group-number*] **preempt** [**delay** *seconds*]

Syntax Description

group-number	(Optional) Group number on the interface to which the other arguments in this command apply. Default is 0.
delay *seconds*	(Optional) Time in seconds. The *seconds* argument causes the local router to postpone taking over the active role for the specified preempt delay *seconds* value. Range is 0 to 3600 seconds (1 hour). Default is 0 seconds (no delay).

Command Default

group-number: 0

seconds: 0 seconds (if the router wants to preempt, it does immediately)

Command Modes

HSRP interface configuration

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

When the **hsrp preempt** command is configured, the local router should attempt to assume control as the active router if it has a hot standby priority higher than the current active router. If the hsrp preempt command is not configured, the local router assumes control as the active router only if no other router is currently in the active state.

When a router first comes up, it does not have a complete routing table. If HSRP is configured to preempt, the local HSRP group may become the active router, yet it is unable to provide adequate routing services. This problem can be solved by configuring a delay before the preempting router actually preempts the currently active router.

The preempt delay *seconds* value does not apply if there is no router currently in the active state. In this case, the local router becomes active after the appropriate timeouts (see the **hsrp timers** command), regardless of the preempt *delay seconds* value.

Task ID

Task ID	Operations
hsrp	read, write

Examples

In the following example, the router waits for 300 seconds (5 minutes) after having determined that it should preempt before attempting to preempt the active router. The router might become the active

router in a shorter span of time despite the configured delay if no active router is present. Only preempting the active router is delayed.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router hsrpi
RP/0/RSP0/CPU0:router(config-hsrp)# interface tenGigE 0/4/0/4
RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4
RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp 1 version 2
RP/0/RSP0/CPU0:router(config-hsrp-gp)# preempt delay 300
RP/0/RSP0/CPU0:router(config-hsrp-gp)#
```

Related Commands

Command	Description
priority (hsrp), on page 332	Configures HSRP priority.
track(object), on page 354	Configures an interface so that the Hot Standby priority changes based on the availability of other interfaces.
show hsrp, on page 337	Displays HSRP information.

priority (hsrp)

To configure Hot Standby Router Protocol (HSRP) priority, use the **priority** command in HSRP group submode. To restore the default values, use the **no** form of this command.

priority *priority*
no priority *priority*

Syntax Description

priority	Priority value that prioritizes a potential Hot Standby router. Range is from 1 to 255. Default is 100.

Command Default

The default priority is 100.

Command Modes

HSRP interface configuration

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

The assigned priority is used to help select the active and standby routers. Assuming that preemption is enabled, the router with the highest priority becomes the designated active router. In case of ties, the interface IP addresses are compared, and the interface with the higher IP address has priority.

The priority of the device can change dynamically if an interface is configured with the **hsrp track** command and another interface on the device goes down.

If preemption is not enabled, the router may not become active even though it might have a higher priority than other HSRP routers.

Task ID

Task ID	Operations
hsrp	read, write

Examples

In this example, the router has a priority of 120:

```
Router# configure
Router(config)# router hsrp
Router(config-hsrp)# interface tengige 0/4/0/4
Router(config-hsrp-if)# address-family ipv4
Router(config-hsrp-ipv4)# hsrp 1 version 2
Router(config-hsrp-gp)# priority 120
Router(config-hsrp-gp)#
```

Note

- The **version** keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families.
- The HSRP version 2 extended group range must be restricted to 0-255, even though the configuration up to 0-4095 is accepted.

Note Starting with IOS XR Release 7.4.1, the HSRP version 2 extended group range configurable in the router is restricted to 0-255.

Related Commands

Command	Description
preempt (hsrp), on page 330	Configures HSRP preemption and preemption delay.
track(object), on page 354	Configures an interface so that the Hot Standby priority changes based on the availability of other interfaces.
show hsrp, on page 337	Displays HSRP information.

router hsrp

To enable the Hot Standby Router Protocol (HSRP), use the **router hsrp** command in XR Config mode. To disable HSRP, use the **no** form of this command.

router hsrp
no router hsrp

Syntax Description

This command has no keywords or arguments.

Command Default

HSRP is disabled.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

HSRP configuration commands must be configured in the HSRP interface configuration mode.

Task ID

Task ID	Operations
hsrp	read, write

Examples

The following example shows how to configure an HSRP redundancy process that contains a virtual router group 1 on tengige 0/2/0/1:

```
Router(config)# router hsrp
Router(config-hsrp)# interface tenGigE 0/2/0/1
Router(config-hsrp-if)# hsrp 1 priority 254
```

session name

To configure an HSRP session name, use the **session name** command in the HSRP group submode. To deconfigure an HSRP session name, use the **no** form of this command.

name *name*

Syntax Description

name	MGO session name

Command Default

None

Command Modes

HSRP Group Submode

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
hsrp	read

Example

This example shows how to configure an HSRP session name.

```
Router# configure
Router(config)# router hsrp
Router(config-hsrp)# interface tenGigE 0/4/0/4
Router(config-hsrp-if)# address-family ipv4
Router(config-hsrp-ipv4)# hsrp 1 version 2
Router(config-hsrp-gp)# name s1
Router(config-hsrp-gp)#
```

Note

- The **version** keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families.
- The HSRP version 2 extended group range must be restricted to 0-255, even though the configuration up to 0-4095 is accepted.



Note Starting with IOS XR Release 7.4.1, the HSRP version 2 extended group range configurable in the router is restricted to 0-255.

show hsrp

To display Hot Standby Router Protocol (HSRP) information, use the **show hsrp** command in XR EXEC mode mode.

show hsrp [**interface** *interface-type* *interface-path-id*] [*group-number*] [**brief** | **detail**]

Syntax Description

interface*interface-type*	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the show interfaces command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
group-number	(Optional) Group number on the interface for which output is displayed.
brief	(Optional) A single line of output summarizes each standby group. The **brief** keyword is the default if **detail** is not specified.
detail	(Optional) This keyword has the same effect as not specifying **brief**; more output is provided.
	(Optional) After this vertical bar (|), specify one of these output modifiers and a keyword from the output: • **begin** —Begins the output from the word that you specify. • **exclude** —Excludes lines that match the word that you specify. • **include** —Includes lines that match the word that you specify.

Command Default

By default, a single line of output summarizing each standby group is displayed.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

Use the **show hsrp** command to display HSRP information.

If you want to specify a value for the *group-number* argument, you must also specify an interface *type* and *number*.

Task ID

Task ID	Operations
hsrp	read

Examples

This is sample output from the **show hsrp detail** command:

```
Router# show hsrp detail

tengige 0/4/0/0 - Group 1
  Local state is Active, priority 100
  Hellotime 3 sec holdtime 10 sec
  Next hello sent in 0.539
  Minimum delay 1 sec, reload delay 5 sec
BFD enabled: state none, interval 15 ms multiplier 3
  Hot standby IP address is 4.0.0.100 configured
  Active router is local
  Standby router is unknown expired
  Standby virtual mac address is 0000.0c07.ac01
  2 state changes, last state change 00:05:20
```

This table describes the significant fields shown in the display.

Table 29: show hsrp Command Field Descriptions

Field	Description
tengige E0/2/0/4	Interface type and number and Hot Standby group number for the interface.
Local state is	State of local networking device; can be one of the following: • Active—Current Hot Standby router. • Standby—Router next in line to be the Hot Standby router. • Speak—Router is sending packets to claim the active or standby role. • Listen—Router is neither active nor standby, but if no messages are received from the active or standby router, it will start to “speak.” • Learn—Router is neither active nor standby, nor does it have enough information to attempt to claim the active or standby roles. • Init—Router is not yet ready to participate in HSRP, possibly because the associated interface is not up.
Hellotime	Current time (in seconds) between sending of hello packets, learned dynamically from the hello packets received from the active Hot Standby router.
holdtime	Current time (in seconds) before other routers declare the active or standby router to be down, learned dynamically from the hello packets received from the active Hot Standby router.
Next hello sent in	Time in which the software will send the next hello packet (in hours:minutes:seconds).

Field	Description
BFD enabled	Displays BFD related information (with multiplier and minimum interval details)
Hot standby IP address is configured	IP address of the current Hot Standby router. The word "configured" indicates that this address is known through the **hsrp ip** command. Otherwise, the address was learned dynamically through HSRP hello packets from other routers that do have the HSRP IP address configured.
Active router is	Value can be "local" or an IP address. Address of the current active Hot Standby router.
Standby router is	Value can be "local" or an IP address of the standby router (the router that is next in line to be the Hot Standby router).
Standby virtual mac address is	MAC address associated with the standby group address.
state changes	Number of times the router changed the standby state.
last state change	Time (in hours:minutes:seconds) expired since the last state change.
Tracking interface states for	List of interfaces that are being tracked and their corresponding states. Based on the **hsrp track** command.
Priority decrement	Value by which the standby priority is decremented or incremented when the tracked interface goes down or up, respectively. Default is 10.

Related Commands

Command	Description
authentication (hsrp), on page 309	Configures an authentication string for HSRP.
hsrp ipv4, on page 316	Activates the HSRP.
preempt (hsrp), on page 330	Configures HSRP preemption and preemption delay.
priority (hsrp), on page 332	Configures HSRP priority.
timers (hsrp), on page 350	Configures the time between hello packets and the time before other routers declare the active Hot Standby or standby router to be down.
track(object), on page 354	Configures an interface so that the Hot Standby priority changes based on the availability of other interfaces.

show hsrp mgo

To display Hot Standby Router Protocol (HSRP) mgo information across all interfaces, use the **show hsrp mgo** command in XR EXEC mode.

show hsrp mgo [**brief** *session-name*]

Syntax Description

brief	(Optional) Displays information in a brief format.
session-name	(Optional) Display information for a single MGO Session.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
hsrp	read

Example

This example shows Hot Standby Router Protocol (HSRP) mgo information for interface HSRP3.

```
Router# show hsrp mgo HSRP3

HSRP3
  Primary group Bundle-Ether1.1 IPv4 group 1
  State is Active
  Slave groups:
    Interface                Grp
    Bundle-Ether1.2            2
    Bundle-Ether1.3            3
    Bundle-Ether1.4            4
    Bundle-Ether1.5            5
```

This example shows Hot Standby Router Protocol (HSRP) mgo information across all interfaces in a brief format.

```
Router# show hsrp mgo brief
```

```
Name            Interface      AF   Grp    State Slaves
HSRP1           Gi0/0/0/1       IPv4   1   Active    100
HSRP2           Te0/1/0/0.1     IPv4   2  Standby     50
HSRP3           BE1             IPv4   1   Active      4
HSRP4           BE1             IPv6  10   Active     11
```

Related Commands

Command	Description
show hsrp, on page 337	Displays HSRP information.

show hsrp statistics

To display Hot Standby Router Protocol (HSRP) statistics information across all interfaces, use the **show hsrp statistics** command in XR EXEC mode.

show hsrp [*interface-type interface-path-id group-number*] **statistics**

Syntax Description

interface-type interface-path-id	Physical interface or virtual interface. **Note** Use the show interfaces command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
group-number	(Optional) Group number of the interface.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
hsrp	read

Example

This sample output is from the **show hsrp statistics** command:

```
 Router# show hsrp statistics
Protocol:
  Transitions to Active                2
  Transitions to Standby               2
  Transitions to Speak                 0
  Transitions to Listen                2
  Transitions to Learn                 0
  Transitions to Init                  0

Packets Sent:                         12
  Hello:                               7
  Resign:                              0
  Coup:                                2
  Adver:                               3
```

```
Valid Packets Received:                 13
  Hello:                                8
  Resign:                               2
  Coup:                                 0
  Adver:                                3

Invalid packets received:               0
  Too long:                             0
  Too short:                            0
  Mismatching/unsupported versions:     0
  Invalid opcode:                       0
  Unknown group:                        0
  Inoperational group:                  0
  Conflicting Source IP:                0
  Failed Authentication:                2
  Invalid Hello Time:                   0
  Mismatching Virtual IP:               0
```

Related Commands

Command	Description
show hsrp, on page 337	Displays HSRP information.

show hsrp summary

To display Hot Standby Router Protocol (HSRP) summary information across all interfaces, use the **show hsrp summary** command in XR EXEC mode mode.

show hsrp summary

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
hsrp	read

Example

This sample output is from the **show hsrp summary** command:

```
Router# show hsrp summary
                Groups                VIPs
State  Sessions Slaves Total     Up  Down  Total
-----   ---------------------   -----------------
ALL          60    900    960    860  2020   2880

ACTIVE       10    190    200    200   300    500
STANDBY      15    235    250    250   600    850
SPEAK        10    190    200    200   400    600
LISTEN       10    190    200    200   400    600
LEARN         5      5     10     10    20     30
INIT         10     90    100      0   300    300

48   HSRP IPv4 interfaces    (43   up, 5   down)
5   Tracked IPv4 interfaces (4    up, 1    down)
5    BFD sessions       (3    up, 2    down)
```

Related Commands

Command	Description
show hsrp, on page 337	Displays HSRP information.

hsrp slave follow

To instruct the subordinate group to inherit its state from a specified group, use the **hsrp slave follow** command in HSRP slave submode.

follow *mgo-session-name*

Syntax Description

mgo-session-name	Name of the MGO session from which the subordinate group will inherit the state.

Command Default

None

Command Modes

HSRP Slave Submode

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
hsrp	read, write

Example

This example shows how to instruct the subordinate group to inherit its state from a specified group.

```
Router# configure
Router(config)# router hsrp
Router(config-hsrp)# interface tenGigE 0/4/0/4
Router(config-hsrp-if)# address-family ipv4
Router(config-hsrp-ipv4)# hsrp slave
Router(config-hsrp-slave)# follow m1
```

subordinate primary virtual IPv4 address

To configure the primary virtual IPv4 address for the subordinate group, use the subordinate primary virtual IPv4 address command in the HSRP slave submode.

address *ip-address*

Syntax Description

ip-address	IP address of the Hot Standby router interface.

Command Default

None

Command Modes

HSRP Slave Submode

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
hsrp	read, write

Example

This example shows how to configure the primary virtual IPv4 address for the subordinate group.

```
Router# configure
Router(config)# router hsrp
Router(config-hsrp)# interface tenGigE 0/4/0/4
Router(config-hsrp-if)# address-family ipv4
Router(config-hsrp-ipv4)# hsrp slave
Router(config-hsrp-slave)# address 10.2.1.4
```

Related Commands

Command	Description
hsrp slave follow, on page 346	Instructs the subordinate group to inherit its state from a specified group.

subordinate secondary virtual IPv4 address

To configure the secondary virtual IPv4 address for the subordinate group, use the **subordinate secondary virtual IPv4 address** command in the HSRP slave submode.

address *ip-address* **secondary**

Syntax Description

ip-address	IP address of the Hot Standby router interface.
secondary	Sets the secondary hot standby IP address.

Command Default

None

Command Modes

HSRP Slave Submode

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
hsrp	read, write

Example

This example shows how to configure the secondary virtual IPv4 address for the subordinate group.

```
Router# configure
Router(config)# router hsrp
Router(config-hsrp)# interface tengige 0/4/0/4
Router(config-hsrp-if)# address-family ipv4
Router(config-hsrp-ipv4)# hsrp slave
Router(config-hsrp-slave)# address 10.2.1.4 secondary
```

Related Commands

Command	Description
hsrp slave follow, on page 346	Instructs the subordinate group to inherit its state from a specified group.

subordinate virtual mac address

To configure the virtual MAC address for the subordinate group, use the **subordinate virtual mac address** command in the HSRP slave submode.

mac-address *address*

Syntax Description

address	48-bit hardware address of ARP entry.

Command Default

None

Command Modes

HSRP Slave Submode

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
hsrp	read, write

Example

This example shows how to configure the virtual MAC address for the subordinate group.

```
Router# configure
Router(config)# router hsrp
Router(config-hsrp)# interface tenGigE 0/4/0/4
Router(config-hsrp-if)# address-family ipv4
Router(config-hsrp-ipv4)# hsrp slave
Router(config-hsrp-slave)# mac-address 10.2.4
```

Related Commands

Command	Description
hsrp slave follow, on page 346	Instructs the subordinate group to inherit its state from a specified group.

timers (hsrp)

To configure the time between hello packets and the time before other routers declare the active Hot Standby or standby router to be down, use the **hsrp timers** command in HSRP group submode. To restore the timers to their default values, use the **no** form of this command.

timers { *hello-seconds* | **msec** *hello-milliseconds* } { *hold-seconds* | **msec** *hold-milliseconds* }
no timers

Syntax Description

hello-seconds	Hello interval in seconds. Range is from 1 to 255. Default is 3.
msec *hello-milliseconds*	Hello interval in milliseconds. Range is from 100 to 3000.
hold-seconds	Time in seconds before the active or standby router is declared to be down. Range is from 1 to 255. Default is 10.
msec *hold-milliseconds*	Time in milliseconds before the active or standby router is declared to be down. Range is from 100 to 3000.

Command Default

The default hello-seconds is 3. (If the **msec** keyword is specified, there is no default value.)

The default hold-seconds is 10. (If the **msec** keyword is specified, there is no default value.)

Command Modes

HSRP Group Submode

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

Nonactive routers learn timer values from the active router, unless millisecond timer values are being used. If millisecond timer values are being used, all routers must be configured with the millisecond timer values. This rule applies if either the hello time or the hold time is specified in milliseconds.

The timers configured on the active router always override any other timer settings. All routers in a Hot Standby group should use the same timer values. Normally, the hold time is greater than or equal to three times the hello time (holdtime > 3 * hellotime).

You must specify either the *hello-seconds* argument or the **msec** keyword and *hello-milliseconds* argument, depending on whether you want the hello time in seconds or milliseconds. You must also specify either the *hold-seconds* argument or **msec** keyword and *hold-milliseconds* argument, depending on whether you want the hold time in seconds or milliseconds.

Task ID

Task ID	Operations
hsrp	read, write

Examples

This example shows how to set, for group number 1 on Ten Gigabit Ethernet interface 0/2/0/1, the time between hello packets to 5 seconds and the time after which a router is considered to be down to 15 seconds. The configured timer values are used only if the router is active (or before they have been learned).

```
Router# configure
Router(config)# router hsrp
Router(config-hsrp)# interface tengige 0/4/0/4
Router(config-hsrp-if)# address-family ipv4
Router(config-hsrp-ipv4)# hsrp 1
Router(config-hsrp-gp)# timers 5 15
Router(config-hsrp-gp)#
```

This example shows how to set, for group number 1 on Ten Gigabit Ethernet interface 0/2/0/1, the time between hello packets to 200 milliseconds and the time after which a router is considered to be down to 1000 milliseconds. The configured timer values are always used because milliseconds have been specified.

```
Router# configure
Router(config)# router hsrp
Router(config-hsrp)# interface tenGigE 0/4/0/4
Router(config-hsrp-if)# address-family ipv4
Router(config-hsrp-ipv4)# hsrp 1 version 2
Router(config-hsrp-gp)# timers msec 200 msec 1000
Router(config-hsrp-gp)#
```

Note

- The **version** keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families.
- The HSRP version 2 extended group range must be restricted to 0-255, even though the configuration up to 0-4095 is accepted.

Note Starting with IOS XR Release 7.4.1, the HSRP version 2 extended group range configurable in the router is restricted to 0-255.

Related Commands

Command	Description
show hsrp, on page 337	Displays HSRP information.

track (hsrp)

To configure an interface so that the Hot Standby priority changes on the basis of the availability of other interfaces, use the **hsrp track** command in HSRP group submode. To remove the tracking, use the **no** form of this command.

track *type* *interface-path-id* [*priority-decrement*]
no track *type* *interface-path-id* [*priority-decrement*]

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the show interfaces command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
priority-decrement	(Optional) Amount by which the Hot Standby priority for the router is decremented (or incremented) when the interface goes down (or comes back up). Range is 1 to 255.

Command Default

The default priority-decrement is 10.

Command Modes

HSRP Group Submode

Command History

Release	Modification
Release 7.1.1	This command was introduced. This command replaced the **hsrp track** command.

Usage Guidelines

The **hsrp track** command ties the Hot Standby priority of the router to the availability of its interfaces. It is useful for tracking interfaces that are not configured for the Hot Standby Router Protocol (HSRP). Only IP interfaces are tracked. A tracked interface is up if IP on that interface is up. Otherwise, the tracked interface is down.

When a tracked interface goes down, the Hot Standby priority decreases by 10. If an interface is not tracked, its state changes do not affect the Hot Standby priority. For each group configured for Hot Standby, you can configure a separate list of interfaces to be tracked.

The optional *priority-decrement* argument specifies by how much to decrement the Hot Standby priority when a tracked interface goes down. When the tracked interface comes back up, the priority is incremented by the same amount.

When multiple tracked interfaces are down and *priority-decrement* values have been configured, these configured priority decrements are cumulative. If tracked interfaces are down, but none of them were configured with priority decrements, the default decrement is 10 and it is cumulative.

The **hsrp preempt** command must be used in conjunction with this command on all routers in the group whenever the best available router should be used to forward packets. If the **hsrp preempt** command is not used, then the active router stays active, regardless of the current priorities of the other HSRP routers.

Task ID

Task ID	Operations
hsrp	read, write

Examples

This example shows how to configure an interface so that the Hot Standby priority changes on the basis of the availability of other interfaces.

```
Router# configure
Router(config)# router hsrp
Router(config-hsrp)# interface tenGigE 0/4/0/4
Router(config-hsrp-if)# address-family ipv4
Router(config-hsrp-ipv4)# hsrp 1 version 2
Router(config-hsrp-gp)# track tenGigE 0/4/0/4 2
Router(config-hsrp-gp)#
```

Note

- The **version** keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families.
- The HSRP version 2 extended group range must be restricted to 0-255, even though the configuration up to 0-4095 is accepted.

Note Starting with IOS XR Release 7.4.1, the HSRP version 2 extended group range configurable in the router is restricted to 0-255.

Related Commands

Command	Description
preempt (hsrp), on page 330	Configures HSRP preemption and preemption delay.
priority (hsrp), on page 332	Configures HSRP priority.
show hsrp, on page 337	Displays HSRP information.

track(object)

To enable tracking of a named object with the specified decrement, use the **track (object)** command in HSRP group submode. To remove the tracking, use the **no** form of this command.

track object *name* [*priority-decrement*]
no track object *name* [*priority-decrement*]

Syntax Description

object *name*	Object tracking. Name of the object to be tracked.
priority-decrement	(Optional) Amount by which the Hot Standby priority for the router is decremented (or incremented) when the interface goes down (or comes back up). Range is 1 to 255.

Command Default

The default priority-decrement is 10.

Command Modes

HSRP Group Submode

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
hsrp	read, write

Examples

This example shows how to configure object tracking under the HSRP group submode.

```
Router# configure
Router(config)# router hsrp
Router(config-hsrp)# interface tenGigE 0/4/0/4
Router(config-hsrp-if)# address-family ipv4
Router(config-hsrp-ipv4)# hsrp 1 version 2
Router(config-hsrp-gp)# track object t1 2
Router(config-hsrp-gp)#
```

Note

- The **version** keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families.
- The HSRP version 2 extended group range must be restricted to 0-255, even though the configuration up to 0-4095 is accepted.



Note Starting with IOS XR Release 7.4.1, the HSRP version 2 extended group range configurable in the router is restricted to 0-255.

Related Commands

Command	Description
preempt (hsrp), on page 330	Configures HSRP preemption and preemption delay.
priority (hsrp), on page 332	Configures HSRP priority.
show hsrp, on page 337	Displays HSRP information.



LPTS Commands

This chapter describes the Cisco IOS XR software commands used to monitor Local Packet Transport Services on NCS 5000 routers.

For detailed information about LPTS concepts, configuration tasks, and examples, refer to the *IP Addresses and Services Configuration Guide for Cisco NCS 5000 Series Routers*.

- clear lpts ifib statistics, on page 358
- clear lpts pifib statistics , on page 359
- show lpts bindings, on page 360
- show lpts clients, on page 364
- show lpts flows, on page 366
- show lpts ifib , on page 369
- show lpts ifib slices, on page 372
- show lpts ifib statistics, on page 375
- show lpts ifib times, on page 377
- show lpts pifib, on page 379
- show lpts pifib hardware police, on page 384
- show lpts pifib hardware usage, on page 387
- show lpts pifib statistics, on page 389
- show lpts port-arbitrator statistics, on page 390

clear lpts ifib statistics

To clear the Internal Forwarding Information Base (IFIB) statistics, use the **clear lpts ifib statistics** command in XR EXEC mode.

clear lpts ifib statistics [**location** *node-id*]

Syntax Description

location *node-id*	Clears the IFIB statistics for the designated node. The *node-id* argument is entered in standard *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
lpts	execute

Examples

The following example shows how to clear the IFIB statistics for the RP:

```
RP/0/RP0/CPU0:router# clear lpts ifib statistics
```

clear lpts pifib statistics

To clear the Pre-Internal Forwarding Information Base (Pre-IFIB) statistics, use the **clear lpts pifib statistics** command in XR EXEC mode.

clear lpts pifib statistics [**location** *node-id*]

Syntax Description

location *node-id*	Clears the Pre-IFIB statistics for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
lpts	execute

Examples

The following example shows how to clear the Pre-IFIB statistics for the RP:

```
RP/0/RP0/CPU0:router# clear lpts pifib statistics location 0/RP0/CPU0
```

show lpts bindings

To display the binding information in the Port Arbitrator, use the **show lpts bindings** command in XR EXEC mode.

show lpts bindings [**location** *node-id*] [**client-id** {**clnl** | **ipsec** | **ipv4-io** | **ipv6-io** | **mpa** | **tcp** | **test** | **udp** | **raw**}] [**brief**] [**vrf** *vrf-name*]

Syntax Description

location *node-id*	(Optional) Displays information for the specified node. The *node-id* argument is entered in the *rack/slot/module* notation.
client-id	(Optional) Type of client. It can be one of the following values: • **clnl** —ISO connectionless protocol (used by IS-IS) • **ipsec** —Secure IP • **ipv4-io** —Traffic processed by the IPv4 stack • **ipv6-io** —Traffic processed by the IPv6 stack • **mpa** —Multicast Port Arbitrator (multicast group joins) • **tcp** —Transmission Control Protocol • **test** —Test applications • **udp** —User Datagram Protocol • **raw** —Raw IP
brief	(Optional) Displays summary output.
vrf *vrf-name*	(Optional) Name of assigned VRF.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **show lpts bindings** command displays the Local Packet Transport Services (LPTS) bindings (requests to receive traffic of a particular type). Bindings are aggregated into flows by the LPTS Port Arbitrator; flows are then programmed into the Internal Forwarding Information Base (IFIB) and Pre-IFIB to direct packets to applications.

If you specify the optional **client-id** keyword and type of client, only bindings from that client are shown. If you specify the optional **location** keyword and *node-id* argument, only bindings from clients on that node are displayed.

Task ID

Task ID	Operations
lpts	read

Examples

The following sample output is from the **show lpts bindings** command, displaying bindings for all client ID types:

```
RP/0/RP0/CPU0:router# show lpts bindings

@ - Indirect binding; Sc - Scope

-----------------------------------------
Location   :0/1/CPU0
Client ID  :IPV4_IO
Cookie     :0x00000001
Clnt Flags :
Layer 3    :IPV4
Layer 4    :ICMP
Local Addr :any
Remote Addr:any
Local Port :any
Remote Port:any
Filters    :Type / Intf or Pkt Type / Source Addr / Location
 INCLUDE_TYPE / type 8
 INCLUDE_TYPE / type 13
 INCLUDE_TYPE / type 17
-----------------------------------------
Location   :0/2/CPU0
Client ID  :IPV4_IO
Cookie     :0x00000001
Clnt Flags :
Layer 3    :IPV4
Layer 4    :ICMP
Local Addr :any
Remote Addr:any
Local Port :any
Remote Port:any
Filters    :Type / Intf or Pkt Type / Source Addr / Location
 INCLUDE_TYPE / type 8
 INCLUDE_TYPE / type 13
 INCLUDE_TYPE / type 17
-----------------------------------------
Location   :0/RP1/CPU0
Client ID  :TCP
Cookie     :0x4826f1f8
Clnt Flags :REUSEPORT
Layer 3    :IPV4
Layer 4    :TCP
Local Addr :any
Remote Addr:any
Local Port :7
Remote Port:any
-----------------------------------------
Location   :0/RP1/CPU0
Client ID  :TCP
Cookie     :0x4826fa0c
Clnt Flags :REUSEPORT
Layer 3    :IPV4
Layer 4    :TCP
```

```
Local Addr :any
Remote Addr:any
Local Port :9
Remote Port:any
---------------------------------------
Location   :0/RP1/CPU0
Client ID  :TCP
Cookie     :0x482700d0
Clnt Flags :REUSEPORT
Layer 3    :IPV4
Layer 4    :TCP
Local Addr :any
Remote Addr:any
Local Port :19
Remote Port:any
---------------------------------------
Location   :0/RP1/CPU0
Client ID  :IPV4_IO
Cookie     :0x00000001
Clnt Flags :
Layer 3    :IPV4
Layer 4    :ICMP
Local Addr :any
Remote Addr:any
Local Port :any
Remote Port:any
Filters    :Type / Intf or Pkt Type / Source Addr / Location
 INCLUDE_TYPE / type 8
 INCLUDE_TYPE / type 13
 INCLUDE_TYPE / type 17
```

This table describes the significant fields shown in the display.

Table 30: show lpts bindings Command Field Descriptions

Field	Description
Location	Node location, in the format of *rack/slot/module*.
Client ID	LPTS client type.
Cookie	Client's unique tag for the binding.
Clnt Flags	REUSEPORT -- client has set the SO_REUSEPORT or SO_REUSEADDR socket option.
Layer 3	Layer 3 protocol (IPv4, IPv6, CLNL).
Layer 4	Layer 4 protocol (TCP, UDP).
Local Addr	Local (destination) address.
Remote Addr	Remote (source) address.
Local Port	Local (destination) TCP or UDP port, or ICMP/IGMP packet type, or IPsec SPI.
Remote Port	Remote (source) TCP or UDP port.

The following sample output is from the **show lpts bindings brief** command:

```
RP/0/RP0/CPU0:router# show lpts bindings brief

@ - Indirect binding; Sc - Scope

 Location   Clnt Sc L3   L4    VRF-ID   Local,Remote Address.Port  Interface
 ---------- ---- -- ---- ----- -------- -------------------------- ------------
 0/1/CPU0   IPV4 LO IPV4 ICMP  *        any.ECHO any               any
 0/1/CPU0   IPV4 LO IPV4 ICMP  *        any.TSTAMP any             any
 0/1/CPU0   IPV4 LO IPV4 ICMP  *        any.MASKREQ any            any
 0/1/CPU0   IPV6 LO IPV6 ICMP6 *        any.ECHOREQ any            any
 0/3/CPU0   IPV4 LO IPV4 ICMP  *        any.ECHO any               any
 0/3/CPU0   IPV4 LO IPV4 ICMP  *        any.TSTAMP any             any
```

This table describes the significant fields shown in the display.

Table 31: show lpts bindings brief Command Field Descriptions

Field	Description
Location	Node location, in the format of *rack/slot/module*.
Clnt ID	LPTS client type.
Sc	Scope (LR = Logical-Router, LO = Local).
Layer 3	Layer 3 protocol.
Layer 4	Layer 4 protocol.
VRF-ID	VPN routing and forwarding (VRF) identification (vrfid) number.
Local,Remote Address.Port	Local (destination) and Remote (source) addresses and ports or packet types.
Interface	Inbound interface.

show lpts clients

To display the client information for the Port Arbitrator, use the **show lpts clients** command in XR EXEC mode.

show lpts clients [**times**]

Syntax Description

times	(Optional) Displays information about binding request rates and service times.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **show lpts clients** command displays the clients connected to the local packet transport services (LPTS) port arbitrator (PA).

Task ID

Task ID	Operations
lpts	read

Examples

The following sample output is from the **show lpts clients** command:

```
RP/0/RP0/CPU0:router# show lpts clients

o_flgs - open flags ; clid - client id
clid            loc             flags   o_flgs
RAW(3)          0/RP1/CPU0      0x1     0x2
TCP(1)          0/RP1/CPU0      0x1     0x2
IPV4_IO(5)      0/1/CPU0        0x3     0x2
IPV4_IO(5)      0/2/CPU0        0x3     0x2
IPV4_IO(5)      0/RP1/CPU0      0x3     0x2
MPA(7)          0/RP1/CPU0      0x3     0x0
```

This table describes the significant fields shown in the display.

Table 32: show lpts clients Command Field Descriptions

Field	Description
Clid	LPTS client ID.
Loc	Node location, in the format *rack/slot/module*.

Field	Description
Flags	Client flags. **Note** The client flags are used only for debugging purposes.
o_flags	Open flags. **Note** The open flags are used only for debugging purposes.

The following sample output is from the **show lpts clients times** command. The output shows samples for the last 30 seconds, 1 minute, 5 minutes, 10 minutes, and a total (if nonzero). The number of transactions, number of updates, and the minimum/average/maximum time in milliseconds to process each transaction is shown.

```
RP/0/RP0/CPU0:router# show lpts clients times

o_flgs - open flags ; clid - client id
clid            loc     flags   o_flgs
RAW(3)          0/RP1/CPU0      0x1     0x2
   30s:2 tx 2 upd 2/2/3ms/tx
    1m:2 tx 2 upd 2/2/3ms/tx
    5m:2 tx 2 upd 2/2/3ms/tx
   10m:2 tx 2 upd 2/2/3ms/tx
 total:2 tx 2 upd 2/-/3ms/tx
TCP(1)          0/RP1/CPU0      0x1     0x2
 total:3 tx 3 upd 1/-/1ms/tx
IPV4_IO(5)      0/1/CPU0        0x3     0x2
 total:1 tx 1 upd 0/-/0ms/tx
IPV4_IO(5)      0/2/CPU0        0x3     0x2
 total:1 tx 1 upd 1/-/1ms/tx
IPV4_IO(5)      0/RP1/CPU0      0x3     0x2
 total:1 tx 1 upd 3/-/3ms/tx
MPA(7)          0/RP1/CPU0      0x3     0x0
```

show lpts flows

To display information about Local Packet Transport Services (LPTS) flows, use the **show lpts flows** command in XR EXEC mode.

show lpts flows [**brief**]

Syntax Description

brief	(Optional) Displays summary output.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **show lpts flows** command is used to display LPTS flows, which are aggregations of identical binding requests from multiple clients and are used to program the LPTS Internal Forwarding Information Base (IFIB) and Pre-IFIB.

Task ID

Task ID	Operations
lpts	read

Examples

The following sample output is from the **show lpts flows** command:

```
RP/0/RP0/CPU0:router# show lpts flows

-----------------------------------------
L3-proto    : IPV4(2)
L4-proto    : ICMP(1)
VRF-ID      : * (000000000)
Local-IP    : any
Remote-IP   : any
Pkt-Type    : 8
Remote-Port : any
Interface   : any (0x0)
Flow-type   : ICMP-local
Min-TTL     : 0
Slice       : RAWIP4_FM
Flags       : 0x20 (in Pre-IFIB)
Location    : (drop)
Element References
location / count / scope
* / 3 / LOCAL
```

This table describes the significant fields shown in the display.

Table 33: show lpts flows Command Field Descriptions

Field	Description
L3-proto	Layer 3 protocol (IPv4, IPv6, CLNL).
L4-proto	Layer 4 protocol (TCP, UDP, and so on).
VRF-ID	VPN routing and forwarding (VRF) identification (vrfid) number.
Local-IP	Local (destination) IP address.
Remote-IP	Remote (source) IP address.
Pkt-Type	ICMP or IGMP packet type.
Remote-Port	Remote (source) TCP or UDP port.
Interface	Ingress interface.
Flow-type	Flow classification for hardware packet policing.
Min-TTL	Minimum time-to-live value expected from in the incoming packet. Any packet received with a lower TTL value will be dropped.
Slice	IFIB slice.
Flags	• Has FGID: Delivered to multiple destinations. • No IFIB entry: IFIB entry suppressed. • Retrying FGID allocation. • In Pre-IFIB: Entry is in Pre-IFIB as well. • Deliver to one: If multiple bindings, will deliver to only one.
Location	*rack/slot/module* to deliver to.
Element References	• location: *rack/slot/module* of client. • count: number of clients at that location. • scope: binding scope (LR:Logical Router, LOCAL:Local).

The following sample output is from the **show lpts flows brief** command:

```
RP/0/RP0/CPU0:router# show lpts flows brief

+ - Additional delivery destination; L - Local interest; P - In Pre-IFIB

 L3   L4    VRF-ID   Local, Remote Address.Port      Interface    Location    LP
 ---- ----- -------- ------------------------------- ------------ ----------- --
 IPV4 ICMP  *        any.ECHO any                    any          (drop)      LP
 IPV4 ICMP  *        any.TSTAMP any                  any          (drop)      LP
 IPV4 ICMP  *        any.MASKREQ any                 any          (drop)      LP
 IPV6 ICMP6 *        any.ECHOREQ any                 any          (drop)      LP
 IPV4 any   default  224.0.0.2 any                   Gi0/1/0/1    0/5/CPU0     P
```

This table describes the significant fields shown in the display.

Table 34: show lpts flows brief Command Field Descriptions

Field	Description
L3	Layer 3 protocol (IPv4, IPv6, CLNL).
L4	Layer 4 protocol.
VRF-ID	VPN routing and forwarding (VRF) identification (vrfid) number.
Local, Remote Address.Port	Local (destination) and remote (source) IP addresses and TCP or UDP ports, or ICMP/IGMP packet types, or IPSec Security Parameters Indices.
Interface	Ingress interface.
Location	Delivery location: • *rack/slot/module*—Individual location. • [0xNNNNN]—Multiple locations (platform-dependent value). • (drop)—Do not deliver to any application.
LP	Local interest (to be processed by IPv4 or IPv6 stack directly) or entry is resident in Pre-IFIB.

show lpts ifib

To display the entries in the Internal Forwarding Information Base (IFIB), use the **show lpts ifib** command in XR EXEC mode.

show lpts ifib [**entry**] [**type** {**bgp4** | **bgp6** | **isis** | **mcast4** | **mcast6** | **ospf-mc4** | **ospf-mc6** | **ospf4** | **ospf6** | **raw4** | **raw6** | **tcp4** | **tcp6** | **udp4** | **udp6**} | **all**] [**brief** [**statistics**]] [**slices**] [**times**] [**location** *node-id*]

Syntax Description

entry	(Optional) Displays the IFIB entries.
type	(Optional) Displays the following protocol types. • **bgp4** —IPv4 Border Gateway Protocol (BGP) slice • **bgp6** —IPv6 BGP slice • **isis** —Intermediate System-to-Intermediate System (IS-IS) slice • **mcast4** —IPv4 multicast slice • **mcast6** —IPv6 multicast slice • **ospf-mc4** —IPv4 Open Shortest Path First (OSPF) multicast slice • **ospf-mc6** —IPv6 OSPF multicast slice • **ospf4** —IPv4 OSPF slice • **ospf6** —IPv6 OSPF slice • **raw4** —IPv4 raw IP • **raw6** —IPv6 raw IP • **tcp4** —IPv4 Transmission Control Protocol (TCP) slice • **tcp6** —IPv6 TCP slice • **udp4** —IPv4 UDP slice • **udp6** —IPv6 UDP slice
all	Displays all IFIB types.
brief	(Optional) Displays the IFIB entries in brief format.
statistics	(Optional) Displays the IFIB table with statistics information.
slices	(Optional) Displays IFIB slices.
times	(Optional) Displays the IFIB update transaction times.
location *node-id*	(Optional) Specifies the location of the Flow Manager. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use this command to display detailed information about the entries in an IFIB slice. This command is useful for debugging problems with delivering packets to applications.

When the **statistics** keyword is used, detailed statistics are displayed for packet count, number of entries in each slice, and a total entries count.

Task ID

Task ID	Operations
lpts	read

Examples

The following sample output is from the **show lpts ifib** command:

```
RP/0/RP0/CPU0:router# show lpts ifib

O - Opcode; A - Accept Counter; D - Drop Counter; F - Flow Type; L - Listener Tag;
I - Local Flag; Y - SYN; T - Min TTL; DV - Deliver; DP - Drop; RE - Reassemble; na - Not
Applicable
-----------------------------------------------------
VRF-ID           : default (0x60000000)
Port/Type        : any
Source Port      : any
Dest IP          : any
Source IP        : any
Layer 4          : 88 (88)
Interface        : any (0x0)
O/A/D/F/L/I/Y/T  : DELIVER/0/0/IPv4_STACK/0/0/0
Deliver List     : 0/5/CPU0
-----------------------------------------------------
```

This table describes the significant fields shown in the display.

Table 35: show lpts ifib entries Command Field Descriptions

Field	Description
VRF-ID	VPN routing and forwarding (VRF) identification (vrfid) number.
Port/Type	Destination (local) TCP or UDP port number, or ICMP/IGMP packet type, or IPSec Security Parameters Index.t2222
Source Port	Source (remote) TCP or UDP port.
Dest IP	Destination (local) IP address.
Source IP	Source (remote) IP address.
Layer 4	Layer 4 protocol number (6 = TCP). **Note** Only the common Layer 4 protocol names are displayed.
Interface	Ingress interface name.

Field	Description
O/S/P/R/L/I/Y	• O: Opcode (DELIVER, DROP, or REASSEMBLE • S: Stats counter • P: Packet forwarding priority (LO, MED, or HIGH) • R: Rate limit (LO, MED, or HIGH) • L: Listener tag (IPv4_STACK, IPv6_STACK, or CLNL_STACK) • I: Local-interest flag (0 or 1) • Y: TCP SYN flag (0 or 1)
Deliver List	• (drop)—Drop packet • *rack/slot/module*—Deliver to single destination • [0xNNNN]—Deliver to multiple destinations (platform-dependent format)

The following sample output is from the **show lpts ifib brief** command:

```
RP/0/RP0/CPU0:router# show lpts ifib brief

 Slice    Local, Remote Address.Port            L4    Interface    Dlvr
 -------- ------------------------------------ ----- ------------ -----------
 TCP4     any.7 any                            TCP   any          0/RP1/CPU0
 TCP4     any.9 any                            TCP   any          0/RP1/CPU0
```

The following sample output is from the **show lpts ifib brief statistics** command:

```
RP/0/RP0/CPU0:router# show lpts ifib brief statistics

 Slice    Local, Remote Address.Port            L4    Interface    Accept/Drop
 -------- ------------------------------------ ----- ------------ -----------
 TCP4     any.7 any                            TCP   any          0/0
 TCP4     any.9 any                            TCP   any          0/0
 TCP4     any.19 any                           TCP   any          0/0

 Slice    Num. Entries Accepts/Drops
 -------- ------------ -------------
TCP4     3            0/0
Total    3            0/0
```

show lpts ifib slices

To display Internal Forwarding Information Base (IFIB) slice information, use the **show lpts ifib slices** command in XR EXEC mode.

show lpts ifib slices [**type** {**bgp4** | **bgp6** | **isis** | **mcast4** | **mcast6** | **ospf-mc4** | **ospf-mc6** | **ospf4** | **ospf6** | **raw4** | **raw6** | **tcp4** | **tcp6** | **udp4** | **udp6**}] [**all**] [**statistics**] [**times**]

Syntax Description

type	(Optional) Enter protocol types. • **bgp4** —IPv4 Border Gateway Protocol (BGP) slice • **bgp6** —IPv6 BGP slice • **isis** —Intermediate System-to-Intermediate System (IS-IS) slice • **mcast4** —IPv4 multicast slice • **mcast6** —IPv6 multicast slice • **ospf-mc4** —IPv4 Open Shortest Path First (OSPF) multicast slice • **ospf-mc6** —IPv6 OSPF multicast slice • **ospf4** —IPv4 OSPF slice • **ospf6** —IPv6 OSPF slice • **raw4** —IPv4 raw IP • **raw6** —IPv6 raw IP • **tcp4** —IPv4 Transmission Control Protocol (TCP) slice • **tcp6** —IPv6 TCP slice • **udp4** —IPv4 UDP slice • **udp6** —IPv6 UDP slice
all	(Optional) Displays all entries.
statistics	(Optional) Displays the statistics for slice lookups.
times	(Optional) Displays the IFIB update transaction times.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **show lpts ifib slices** command when troubleshooting IFIB entries and slice assignments. This command is especially useful when troubleshooting problems with delivering packets to applications.

Task ID

Task ID	Operations
lpts	read

Examples

The following sample output is from the **show lpts ifib slices** command:

```
RP/0/RP0/CPU0:router# show lpts ifib slices

Slice    L3   L4     Port  Location
-------- ---- ------ ----- --------
RAWIP4   IPV4 any    any   0/RP0/CPU0
RAWIP6   IPV6 any    any   0/RP0/CPU0
OSPF4    IPV4 OSPF   any   0/RP0/CPU0
OSPF6    IPV6 OSPF   any   0/RP0/CPU0
OSPF_MC4 IPV4 any    any   0/RP0/CPU0
OSPF_MC6 IPV6 any    any   0/RP0/CPU0
BGP4     IPV4 TCP    179   0/RP0/CPU0
BGP6     IPV6 TCP    179   0/RP0/CPU0

UDP4     IPV4 UDP    any   0/RP0/CPU0
UDP6     IPV6 UDP    any   0/RP0/CPU0
TCP4     IPV4 TCP    any   0/RP0/CPU0
TCP6     IPV6 TCP    any   0/RP0/CPU0
ISIS     CLNS -      any   0/RP0/CPU0
MCAST4   IPV4 any    any   0/RP0/CPU0
MCAST6   IPV6 any    any   0/RP0/CPU0
```

The following sample output is from the **show lpts ifib slices times** command:

```
RP/0/RP0/CPU0:router# show lpts ifib slices times

Slice    L3   L4     Port  Location
-------- ---- ------ ----- --------
RAWIP4   IPV4 any    any   0/RP0/CPU0
RAWIP6   IPV6 any    any   0/RP0/CPU0
OSPF4    IPV4 OSPF   any   0/RP0/CPU0
OSPF6    IPV6 OSPF   any   0/RP0/CPU0
OSPF_MC4 IPV4 any    any   0/RP0/CPU0
OSPF_MC6 IPV6 any    any   0/RP0/CPU0
BGP4     IPV4 TCP    179   0/RP0/CPU0
BGP6     IPV6 TCP    179   0/RP0/CPU0

UDP4     IPV4 UDP    any   0/RP0/CPU0
UDP6     IPV6 UDP    any   0/RP0/CPU0
TCP4     IPV4 TCP    any   0/RP0/CPU0
TCP6     IPV6 TCP    any   0/RP0/CPU0
ISIS     CLNS -      any   0/RP0/CPU0
MCAST4   IPV4 any    any   0/RP0/CPU0
MCAST6   IPV6 any    any   0/RP0/CPU0
  Flow Manager 0/RP0/CPU0:
   total:5 tx 13 upd 1/-/1ms/tx
```

The following sample output is from the **show lpts ifib slices statistics** command:

```
RP/0/RP0/CPU0:router# show lpts ifib slices all statistics

Slice    L3   L4     Port  Location   Lookups RmtDlvr Rejects RLDrops NoEntry
```

```
-------- ---- ------ ----- ---------- ------- ------- ------- ------- -------
RAWIP4   IPV4 any    any   0/0/CPU0   5       0       0       0       0
RAWIP6   IPV6 any    any   0/0/CPU0   0       0       0       0       0
OSPF4    IPV4 OSPF   any   0/0/CPU0   0       0       0       0       0
OSPF6    IPV6 OSPF   any   0/0/CPU0   0       0       0       0       0
OSPF_MC4 IPV4 any    any   0/0/CPU0   0       0       0       0       0
OSPF_MC6 IPV6 any    any   0/0/CPU0   0       0       0       0       0
BGP4     IPV4 TCP    179   0/0/CPU0   0       0       0       0       0
BGP6     IPV6 TCP    179   0/0/CPU0   0       0       0       0       0

UDP4     IPV4 UDP    any   0/0/CPU0   3704    0       979     0       0
UDP6     IPV6 UDP    any   0/0/CPU0   0       0       0       0       0
TCP4     IPV4 TCP    any   0/0/CPU0   0       0       0       0       0
TCP6     IPV6 TCP    any   0/0/CPU0   0       0       0       0       0
ISIS     CLNS -      any   0/0/CPU0   0       0       0       0       0
MCAST4   IPV4 any    any   0/0/CPU0   0       0       0       0       0
MCAST6   IPV6 any    any   0/0/CPU0   0       0       0       0       0
  Flow Manager 0/0/CPU0:
   Packets in: 3792
   Packets delivered locally without lookups: 83
   Slice lookups: 3709
     Rejects: 979
```

This table describes the significant fields shown in the display.

Table 36: show lpts ifib slices statistics Command Field Descriptions

Field	Description
Slice	Slice number.
L3-proto	Layer 3 protocol (IPv4, IPv6, CLNL).
L4-proto	Layer 4 protocol (TCP, UDP, and others).
Port	Local (destination) TCP or UDP port.
Location	Node location, in the format *rack/slot/module*.

show lpts ifib statistics

To display Internal Forwarding Information Base (IFIB) statistics, use the **show lpts ifib statistics** command in .

show lpts ifib statistics [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Displays IFIB statistics for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
lpts	read

Examples

The following sample output is from the **show lpts ifib statistics** command:

```
RP/0/# show lpts ifib statistics

Flow Manager 0/RP0/CPU0:
   Packets in:254
   Packets delivered locally without lookups:0
   Slice lookups:254
     Post-lookup error drops:
      Failed ipv4_netio_input:1
     Rejects:254
    Packets delivered locally:0
    Packets delivered remotely:0
```

This table describes the significant fields shown in the display.

Table 37: show lpts ifib statistics Command Field Descriptions

Field	Description
Packets in	Packets presented to the LPTS decaps node in netio.
Packets delivered locally without lookups	Packets previously resolved on a LC delivered directly to L3.
Slice lookups	Packets requiring slice lookups.

Field	Description
Post-lookup error drops	Packets dropped after a slice lookup.
Rejects	Packets that caused a TCP RST or ICMP Port/Protocol Unreachable.
Packets delivered locally	Packets delivered to local applications after slice lookups.
Packets delivered remotely	Packets delivered to applications on remote RPs.



Note The sample output is an example only and displays only those fields showing a value. No display exists for nonzero values. This command may show other values depending on your router configuration.

show lpts ifib times

To display Internal Forwarding Information Base (IFIB) update transaction times, use the **show lpts ifib times** command in XR EXEC mode.

show lpts ifib times [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Displays IFIB update transaction times for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
lpts	read

Examples

The following sample output is from the **show lpts ifib times** command:

```
RP/0/RP0/CPU0:router# show lpts ifib times

Slice    L3   L4     Port  Location
-------- ---- ------ ----- --------
RAWIP4   IPV4 any    any   0/RP1/CPU0
RAWIP6   IPV6 any    any   0/RP1/CPU0
OSPF4    IPV4 OSPF   any   0/RP1/CPU0
OSPF6    IPV6 OSPF   any   0/RP1/CPU0
OSPF_MC4 IPV4 any    any   0/RP1/CPU0
OSPF_MC6 IPV6 any    any   0/RP1/CPU0
BGP4     IPV4 TCP    179   0/RP1/CPU0
BGP6     IPV6 TCP    179   0/RP1/CPU0
UDP4     IPV4 UDP    any   0/RP1/CPU0
UDP6     IPV6 UDP    any   0/RP1/CPU0
TCP4     IPV4 TCP    any   0/RP1/CPU0
TCP6     IPV6 TCP    any   0/RP1/CPU0
ISIS     CLNS -      any   0/RP1/CPU0
MCAST4   IPV4 any    any   0/RP1/CPU0
MCAST6   IPV6 any    any   0/RP1/CPU0
Flow Manager 0/RP0/CPU0:
 total:5 tx 13 upd 1/-/1ms/tx
```

This table describes the significant fields shown in the display.

Table 38: show lpts ifib times Command Field Descriptions

Field	Description
Slice	Slice number.
L3 Protocol	Layer 3 protocol (IPv4, IPV6, CLNL).
L4 Protocol	Layer 4 protocol (TCP, UDP, and so on).
Port	Local (destination) TCP or UDP port.
Location	Node location, in the format *rack/slot/module*.

show lpts pifib

To display Pre-Internal Forwarding Information Base (Pre-IFIB) entries, use the **show lpts pifib** command in XR EXEC mode.

show lpts pifib [entry] [hardware {**entry | police**}**[type {isis | ipv4 | ipv6}** {**any** } [**brief**] **[statistics] [location** *node-id*]

Syntax Description

entry	(Optional) Pre-IFIB entry.
hardware	(Optional) Displays hardware for Pre-IFIB.
entry	(Optional) Displays the entries for Pre-IFIB.
police	(Optional) Displays the policer values that are being use.
type	(Optional) Protocol type.
isis	(Optional) Intermediate System-to-Intermediate System (IS-IS) sub Pre-IFIB type.
ipv4	(Optional) IPv4 sub Pre-IFIB type. Possible values include **frag** , **ixmp** , **mcast** , **tcp** , **udp** , **ipsec** , and **raw** .
ipv6	(Optional) IPv6 sub Pre-IFIB type. Possible values include **frag** , **icmp** , **ixmp** , **mcast** , **tcp** , **udp** , **ipsec, and raw** .
any	Any IPv4 or IPv6 protocol.
brief	(Optional) Pre-IFIB entries in brief format.
statistics	(Optional) Pre-IFIB table with statistics information.
location *node-id*	(Optional) The *node-id* argument is entered in the *rack/slot/module* notation (for example, 0/7/CPU0).

Command Default

By default, all entries are displayed.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **show lpts pifib** command with the **brief** keyword to perform the following functions:

- Display entries of all or part of a Pre-IFIB.
- Display a short description of each entry in the LPTS Pre-IFIB, optionally displaying packet counts for each entry.

Note These statistics are used only for packets that are processed by a line card, route processor, or distributed route processor.

Pre-IFIB statistics for packets processed by line card hardware are counted separately.

By default, all the defaults are displayed.

Task ID

Task ID	Operations
lpts	read

Examples

The following is sample output for the **show lpts pifib** command:

```
RP/0/RP0/CPU0:router# show lpts pifib

O - Opcode; F - Flow Type; L - Listener Tag; I - Local Flag; T - Min TTL;
na - Not Applicable
-----------------------------------------------------
L3 Protocol       : CLNS
L4 Protocol       : -
VRF-ID            : default (0x60000000)
Destination IP    : any
Source IP         : any
Port/Type         : any
Source Port       : any
Is Fragment       : 0
Is SYN            : 0
Interface         : any (0x0)
O/F/L/I/T         : DELIVER/ISIS-default/CLNS_STACK/0/0
Deliver List      : FGID 11935
Accepts/Drops     : 0/0
Is Stale          : 0
```

The following is sample output for the **show lpts pifib type** command using the **ipv4** and **tcp** keywords.

```
RP/0/RP0/CPU0:router# show lpts pifib type ipv4 tcp

O - Opcode; F - Flow Type; L - Listener Tag; I - Local Flag; T - Min TTL;
na - Not Applicable
-----------------------------------------------------
L3 Protocol       : IPV4
L4 Protocol       : TCP
VRF-ID            : default (0x60000000)
Destination IP    : any
Source IP         : any
Port/Type         : Port:23
Source Port       : any
Is Fragment       : 0
Is SYN            : 0
Interface         : any (0x0)
O/F/L/I/T         : DELIVER/TELNET-default/IPv4_LISTENER/0/0
Deliver List      : 0/RP0
```

```
/CPU0
Accepts/Drops     : 0/0
Is Stale          : 0
-----------------------------------------------------
```

The following is sample output from the **show lpts pifib** command with the **entry** and **brief** keywords added command:

```
RP/0/RP0/CPU0:router# show lpts pifib entry brief

* - Critical Flow; I - Local Interest;
X - Drop; R - Reassemble;

 Type       VRF-ID   Local, Remote Address.Port L4    Interface    Deliver
 ---------- -------- -------------------------- ----- ------------ -------------

 ISIS       *        - -                        -     any          0/0/CPU0
 IPv4_frag  *        any any                    any   any          R
 IPv4_IXMP  *        any.ECHO any               ICMP  any          XI
 IPv4_IXMP  *        any.TSTAMP any             ICMP  any          XI
 IPv4_IXMP  *        any.MASKREQ any            ICMP  any          XI
 IPv4_IXMP  *        any any                    ICMP  any          0/0/CPU0
 IPv4_IXMP  *        any any                    IGMP  any          0/0/CPU0
 IPv4_mcast *        224.0.0.5 any              any   any          0/0/CPU0
 IPv4_mcast *        224.0.0.6 any              any   any          0/0/CPU0
 IPv4_mcast *        224.0.0.0/4 any            any   any          0/0/CPU0

 IPv4_TCP   *        any.179 any                TCP   any          0/0/CPU0
 IPv4_TCP   *        any any.179                TCP   any          0/0/CPU0
 IPv4_TCP   *        any any                    TCP   any          0/0/CPU0
 IPv4_UDP   *        any any                    UDP   any          0/0/CPU0
 IPv4_IPsec *        any any                    ESP   any          0/0/CPU0
 IPv4_IPsec *        any any                    AH    any          0/0/CPU0
 IPv4_rawIP *        any any                    OSPF  any          0/0/CPU0
 IPv4_rawIP *        any any                    any   any          0/0/CPU0
 IPv6_frag  *        any any                    any   any          R
 IPv6_ICMP  *        any.na any                 ICMP6 any          XI
 IPv6_ICMP  *        any any                    ICMP6 any          0/0/CPU0
 IPv6_mcast *        ff02::5 any                any   any          0/0/CPU0
 IPv6_mcast *        ff02::6 any                any   any          0/0/CPU0
 IPv6_mcast *        ff00::/8 any               any   any          0/0/CPU0
 IPv6_TCP   *        any.179 any                TCP   any          0/0/CPU0
 IPv6_TCP   *        any any.179                TCP   any          0/0/CPU0
 IPv6_TCP   *        any any                    TCP   any          0/0/CPU0
 IPv6_UDP   *        any any                    UDP   any          0/0/CPU0
 IPv6_IPsec *        any any                    ESP   any          0/0/CPU0
 IPv6_IPsec *        any any                    AH    any          0/0/CPU0
 IPv6_rawIP *        any any                    OSPF  any          0/0/CPU0
 IPv6_rawIP *        any any                    any   any          0/0/CPU0
```

The following sample output is from the **show lpts pifib** command with the **entry, brief,** and **entry brief statistics** keywords added:

```
RP/0/RP0/CPU0:router# show lpts pifib entry brief statistics

* - Critical Flow; I - Local Interest;
X - Drop; R - Reassemble;

 Type       VRF-ID   Local, Remote Address.Port L4    Interface    Accepts/Drops
```

```
---------- -------- -------------------------- ----- ------------ -------------

ISIS       *        - -                        -     any          0/0
IPv4_frag  *        any any                    any   any          0/0
IPv4_IXMP  *        any.ECHO any               ICMP  any          0/0
IPv4_IXMP  *        any.TSTAMP any             ICMP  any          0/0
IPv4_IXMP  *        any.MASKREQ any            ICMP  any          0/0
IPv4_IXMP  *        any any                    ICMP  any          5/0
IPv4_IXMP  *        any any                    IGMP  any          0/0
IPv4_mcast *        224.0.0.5 any              any   any          0/0
IPv4_mcast *        224.0.0.6 any              any   any          0/0
IPv4_mcast *        224.0.0.0/4 any            any   any          0/0
IPv4_TCP   *        any.179 any                TCP   any          0/0
IPv4_TCP   *        any any.179                TCP   any          0/0
IPv4_TCP   *        any any                    TCP   any          0/0
IPv4_UDP   *        any any                    UDP   any          4152/0
IPv4_IPsec *        any any                    ESP   any          0/0
IPv4_IPsec *        any any                    AH    any          0/0
IPv4_rawIP *        any any                    OSPF  any          0/0

-----------------------

statistics:

Type            Num. Entries         Accepts/Drops

------          ------------         -------------
ISIS            1                    0/0
IPv4_frag       1                    0/0
IPv4_IXMP       5                    5/0
IPv4_mcast      3                    0/0
IPv4_TCP        3                    0/0
IPv4_UDP        1                    4175/0
IPv4_IPsec      2                    0/0
IPv4_rawIP      2                    0/0
IPv6_frag       1                    0/0
IPv6_ICMP       2                    0/0
IPv6_mcast      3                    0/0
IPv6_TCP        3                    0/0
IPv6_UDP        1                    0/0
IPv6_IPsec      2                    0/0
IPv6_rawIP      2                    0/0
Total           32

Packets into Pre-IFIB: 4263
Lookups: 4263
Packets delivered locally: 4263
Packets delivered remotely: 0
```

This table describes the significant fields shown in the display for the **show lpts pifib** command with the **brief** and **statistics** keywords .

Table 39: show lpts pifib Command Field Descriptions

Field	Description
Type	Hardware entry type.
VRF ID	VPN routing and forwarding (VRF) identification (vrfid) number.

Field	Description
Local, Remote Address. Port	Indicates local address (in the form of local port and type) and remote address (remote port).
L4	Layer 4 protocol of the entry.
Interface	Interface for this entry.
Accepts/Drops	Number of packets sent to DestAddr/Number of packets dropped due to policing.
Num. Entries	Number of pre-ifib entries of the listed type.
Packets into Pre-IFIB	Packets presented for pre-IFIB lookups.
Lookups	Packets looked up.
Packets delivered locally	Packets delivered to local applications or the local stack (*n* duplicated) packets duplicated for delivery to applications and the local stack.
Packets delivered remotely	Packets delivered to applications or for lookup on other RPs.

show lpts pifib hardware police

To display the policer configuration value set, use the **show lpts pifib hardware police** command in XR EXEC mode.

show lpts pifib hardware police [**location** {**all***node-id*}]

Syntax Description

location *node-id*	(Optional) Displays pre-Internal Forwarding Information Base (IFIB) information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
all	Specifies all locations.

Command Default

If no policer is configured, the default value is the configured rate.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.3.2	Monitor LPTS host path drops via `Cisco-IOS-XR-lpts-pre-ifib-oper` YANG data model.
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
lpts	read

Examples

This sample output is from the **show lpts pifib hardware police** command with the **location** keyword for 0/RP0/CPU0:

```
RP/0/RP0/CPU0:router#show lpts pifib hardware police location 0/RP0/CPU0


------------------------------------------------------------
               Node 0/RP0/CPU0:
------------------------------------------------------------
 Burst = 100ms for all flow types
------------------------------------------------------------
FlowType               Policer Type    Cur. Rate Def. Rate Accepted   Dropped
---------------------- ------- ------- --------- --------- ---------- ---------
unconfigured-default   100     Static  500       500       0          0
Fragment               106     Static  1000      1000      0          0
OSPF-mc-known          107     Static  20000     20000     0          0
OSPF-mc-default        111     Static  5000      5000      0          0
OSPF-uc-known          161     Static  5000      5000      0          0
OSPF-uc-default        162     Static  1000      1000      0          0
ISIS-known             108     Static  20000     20000     0          0
ISIS-default           112     Static  5000      5000      0          0
```

```
BFD-known                170     Static  8500      8500      0           0
BFD-default              171     Static  8500      8500      0           0
BFD-MP-known             177     Static  8400      8400      0           0
BFD-MP-0                 178     Static  128       128       0           0
BGP-known                113     Static  25000     25000     0           0
BGP-cfg-peer             114     Static  10000     10000     0           0
BGP-default              115     Static  1500      1500      0           0
PIM-mcast-default        116     Static  23000     23000     0           0
PIM-mcast-known          176     Static  23000     23000     0           0
PIM-ucast                117     Static  10000     10000     0           0
IGMP                     118     Static  3500      3500      0           0
ICMP-local               119     Static  2500      2500      0           0
ICMP-app                 120     Static  2500      2500      0           0
ICMP-control             164     Static  2500      2500      0           0
ICMP-default             121     Static  2500      2500      0           0
LDP-TCP-known            122     Static  25000     25000     0           0
LDP-TCP-cfg-peer         152     Static  10000     10000     0           0
LDP-TCP-default          154     Static  10000     10000     0           0
LDP-UDP                  158     Static  2500      2500      0           0
All-routers              160     Static  10000     10000     0           0
LMP-TCP-known            123     Static  25000     25000     0           0
LMP-TCP-cfg-peer         153     Static  10000     10000     0           0
LMP-TCP-default          155     Static  10000     10000     0           0
LMP-UDP                  159     Static  2500      2500      0           0
RSVP-UDP                 124     Static  7000      7000      0           0
RSVP-default             125     Static  500       500       0           0
RSVP-known               126     Static  7000      7000      0           0
IKE                      127     Static  1000      1000      0           0
IPSEC-known              129     Static  3000      3000      0           0
IPSEC-default            128     Static  1000      1000      0           0
MSDP-known               130     Static  1000      1000      0           0
MSDP-cfg-peer            131     Static  1000      1000      0           0
MSDP-default             132     Static  1000      1000      0           0
SNMP                     133     Static  2000      2000      0           0
SSH-known                135     Static  1000      1000      0           0
SSH-default              136     Static  1000      1000      0           0
HTTP-known               137     Static  1000      1000      0           0
HTTP-default             138     Static  1000      1000      0           0
SHTTP-known              139     Static  1000      1000      0           0
IFIB_FT_SHTTP_DEFAULT    140     Static  1000      1000      0           0
TELNET-known             141     Static  1000      1000      0           0
TELNET-default           142     Static  1000      1000      0           0
CSS-known                143     Static  1000      1000      0           0
CSS-default              144     Static  1000      1000      0           0
RSH-known                145     Static  1000      1000      0           0
RSH-default              146     Static  1000      1000      0           0
UDP-known                147     Static  25000     25000     0           0
UDP-listen               156     Static  4000      4000      0           0
UDP-cfg-peer             157     Static  4000      4000      0           0
UDP-default              101     Static  500       500       0           0
TCP-known                148     Static  25000     25000     0           0
TCP-listen               149     Static  25000     25000     0           0
TCP-cfg-peer             150     Static  25000     25000     0           0
TCP-default              102     Static  500       500       0           0
Mcast-known              151     Static  25000     25000     0           0
Mcast-default            103     Static  500       500       0           0
Raw-listen               104     Static  500       500       0           0
Raw-default              105     Static  500       500       0           0
Ip-Sla                   163     Static  10000     10000     0           0
RIP                      110     Static  20000     20000     0           0
L2TPv3                   165     Static  25000     25000     0           0
PCEP                     166     Static  100       100       0           0
GRE                      167     Static  1000      1000      0           0
VRRP                     168     Static  1000      1000      0           0
```

```
HSRP                    169     Static  400         400         0           0
MPLS-oam                172     Static  100         100         0           0
L2TPv2                  179     Static  25000       25000       0           0
DNS                     173     Static  500         500         0           0
RADIUS                  174     Static  7000        7000        0           0
TACACS                  175     Static  500         500         0           0
NTP-default             134     Static  500         500         0           0
NTP-known               180     Static  500         500         0           0

------------------------
statistics:
Packets accepted by deleted entries: 0
Packets dropped by deleted entries: 0
Run out of statistics counter errors: 0
```

This table describes the significant fields shown in the display.

Table 40: show lpts pifib hardware police Command Field Descriptions

Field	Description
FlowType	Type of flow that is binding between a tuple and a destination.
Policer	Policer Values in PPS
Rate (PPS)	Policer rate in packets per second (PPS).
Accept	Number of packets that are accepted by this policer.
Drop	Number of packets that are dropped by this policer.

show lpts pifib hardware usage

To display hardware table usage, use the **show lpts pifib hardware usage** command in XR EXEC mode.

show lpts pifib hardware usage [**type** {**ipv4** | **ipv6** | **isis**}] [**location** {*node-id* | **all**}]

Syntax Description

type	(Optional) Specifies the hardware entry type. Enter one of the following types: • **ipv4** —Specifies IPv4 entries. • **ipv6** —Specifies IPv6 entries. • **isis** —Specifies ISIS entries.
location *node-id*	(Optional) Displays pre-Internal Forwarding Information Base (IFIB) information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
all	(Optional) Specifies all locations.

Command Default

Without the optional parameters, the **show lpts pifib hardware usage** command displays a brief summary of hardware entry information.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
lpts	read

Examples

The following sample output is from the **show lpts pifib hardware usage** command with the **location** keyword:

```
RP/0/RP0/CPU0:router# show lpts pifib hardware usage location 0/RP0/cpu0

Type       Size            Used            Used(%)
---------- --------------- --------------- -------
ipv4       6000            21              0.35
ipv6       4000            15              0.38
isis       4000            1               0.03
```

This table describes the significant fields shown in the display.

Table 41: show lpts pifib hardware usage Command Field Descriptions

Field	Description
Type	Type of pre-IFIB entry.
Size	Maximum number of entries (72-bits) allowed for the type.
Used	Number of entries in use.
Used(%)	Percentage of total entries in use.

show lpts pifib statistics

To display Pre-Internal Forwarding Information Base (Pre-IFIB) statistics, use the **show lpts ifib statistics** command in XR EXEC mode.

show lpts pifib statistics [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Displays Pre-IFIB statistics for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
lpts	read

Examples

The following sample output is from the **show lpts pifib statistics** command:

```
RP/0/RP0/CPU0:router# show lpts pifib statistics

Packets into Pre-IFIB:80
Lookups:80
Packets delivered locally:80
Packets delivered remotely:0
```

This table describes the significant fields shown in the display.

Table 42: show lpts pifib statistics Command Field Descriptions

Field	Description
Packets into Pre-IFIB	Packets presented for pre-IFIB lookups.
Lookups	Packets looked up.
Packets delivered locally	Packets delivered to local applications or the local stack (*n* duplicated) packets duplicated for delivery to applications and the local stack.
Packets delivered remotely	Packets delivered to applications or for lookup on other RPs.

show lpts port-arbitrator statistics

To display local packet transport services (LPTS) port arbitrator statistics, use the **show lpts port-arbitrator statistics** command in XR EXEC mode.

show lpts port-arbitrator statistics

Syntax Description This command has no keywords or arguments.

Command Default No default behavior or values

Command Modes XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
lpts	read

Examples The following sample output is from the **show lpts port-arbitrator statistics** command:

```
RP/0/RP0/CPU0:router# show lpts port-arbitrator statistics

LPTS Port Arbitrator statistics:
 PA FGID-DB library statistics:
  0 FGIDs in use, 512 cached, 0 pending retries
  0 free allocation slots, 0 internal errors, 0 retry attempts
  1 FGID-DB notify callback, 0 FGID-DB errors returned
  FGID-DB permit mask: 0x7 (alloc mark rack0)
  PA API calls:
            1 init              1 realloc_done
            8 alloc             8 free
           16 join             16 leave
            8 detach
  FGID-DB API calls:
            1 register          1 clear_old
            1 alloc             0 free
           16 join             16 leave
            0 mark              1 mark_done
```



Network Stack IPv4 and IPv6 Commands

This chapter describes the commands available on the NCS 5000 routers Cisco IOS XR software to configure and monitor features related to IP Version 4 (IPv4) and IP Version 6 (IPv6).

For detailed information about network stack concepts, configuration tasks, and examples, refer to the *IP Addresses and Services Configuration Guide for Cisco NCS 5000 Series Routers*.

- clear ipv6 neighbors, on page 393
- icmp ipv4 rate-limit unreachable, on page 394
- ipv4 address (network), on page 395
- ipv4 assembler max-packets, on page 397
- ipv4 assembler timeout, on page 398
- ipv4 mask-reply, on page 399
- ipv4 conflict-policy, on page 400
- ipv4 mtu, on page 401
- ipv4 unnumbered (point-to-point), on page 403
- ipv6 address, on page 405
- ipv6 assembler, on page 407
- ipv6 conflict-policy, on page 408
- ipv6 address link-local, on page 409
- ipv6 enable , on page 411
- ipv6 hop-limit, on page 413
- ipv6 icmp error-interval, on page 414
- ipv6 mtu, on page 416
- ipv6 nd dad attempts , on page 418
- ipv6 nd managed-config-flag, on page 421
- ipv6 nd ns-interval, on page 423
- ipv6 nd other-config-flag , on page 425
- ipv6 nd prefix, on page 427
- ipv6 nd ra-interval, on page 429
- ipv6 nd ra-lifetime, on page 431
- ipv6 nd reachable-time, on page 432
- ipv6 nd redirects, on page 434
- ipv6 nd scavenge-timeout, on page 435
- ipv6 nd suppress-ra, on page 436
- ipv6 neighbor, on page 437

- ipv6 path-mtu enable, on page 439
- ipv6 path-mtu timeout, on page 440
- ipv6 source-route, on page 441
- ipv6 tcp-mss-adjust, on page 442
- ipv6 virtual address, on page 443
- show arm conflicts, on page 445
- show arm registrations producers, on page 447
- show arm router-ids, on page 449
- show arm summary, on page 450
- show ipv4 interface, on page 451
- show ipv4 traffic, on page 454
- show ipv6 interface , on page 456
- show ipv6 neighbors, on page 460
- show ipv6 neighbors summary , on page 463
- show ipv6 path-mtu, on page 464
- show ipv6 traffic, on page 465

clear ipv6 neighbors

To delete all entries in the IPv6 neighbor discovery cache, except static entries, use the **clear ipv6 neighbors** command in XR EXEC mode.

clear ipv6 neighbors [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) The designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

None

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

If the location option is specified, only the neighbor entries specified in the **location** *node-id* keyword and argument are cleared.

Task ID

Task ID	Operations
network	read, write
IPv6	execute

Examples

In the following example, only the highlighted entry is deleted:

```
RP/0/RP0/CPU0:router# clear ipv6 neighbors ?
location specify a node name

RP/0/RP0/CPU0:router# show ipv6 neighbor

IPv6 Address Age Link-layer Addr State Interface
8888::3 - 1234.2345.9877 REACH tenGigE0/0/0/0
8888::8 - 1234.2345.9877 REACH tenGigE0/0/0/0
fe80::205:1ff:fe9f:6400 1335 0005.019f.6400 STALE tenGigE0/0/0/0
fe80::206:d6ff:fece:3808 1482 0006.d6ce.3808 STALE tenGigE0/0/0/0
fe80::200:11ff:fe11:1112 1533 0000.1111.1112 STALE tenGigE0/0/0/2

RP/0/RP0/CPU0:router# clear ipv6 neighbors location 0/2/0
RP/0/RP0/CPU0:router# show ipv6 neighbor

IPv6 Address Age Link-layer Addr State Interface
8888::3 - 1234.2345.9877 REACH tenGigE0/0/0/0
8888::8 - 1234.2345.9877 REACH tenGigE0/0/0/0
fe80::205:1ff:fe9f:6400 1387 0005.019f.6400 STALE tenGigE0/0/0/0
fe80::206:d6ff:fece:3808 1534 0006.d6ce.3808 STALE tenGigE0/0/0/0
```

icmp ipv4 rate-limit unreachable

To limit the rate that IPv4 Internet Control Message Protocol (ICMP) destination unreachable messages are generated, use the **icmp ipv4 rate-limit unreachable** command in XR Config mode. To remove the rate limit, use the **no** form of this command.

icmp ipv4 rate-limit unreachable [**DF**] *milliseconds*
no icmp ipv4 rate-limit unreachable [**DF**] *milliseconds*

Syntax Description

DF	(Optional) Limits the rate at which ICMP destination unreachable messages are sent when code 4 fragmentation is needed and data fragmentation is (DF) set, as specified in the IP header of the ICMP destination unreachable message.
milliseconds	Time period (in milliseconds) between the sending of ICMP destination unreachable messages. Range is 1 to 4294967295.

Command Default

The default value is one ICMP destination unreachable message every 500 milliseconds.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The Cisco IOS XR software maintains two timers: one for general destination unreachable messages and one for DF destination unreachable messages. Both share the same time limits and defaults. If the **DF** option is not configured, the **icmp ipv4 rate-limit unreachable** command sets the time values for DF destination unreachable messages. If the **DF** option is configured, its time values remain independent from those of general destination unreachable messages.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write

Examples

The following example shows how to set the time interval for the ICMP destination unreachable message to be generated at a minimum interval of 10 ms:

```
RP/0/RP0/CPU0:router(config)# icmp ipv4 rate-limit unreachable 10
```

ipv4 address (network)

To set a primary or secondary IPv4 address for an interface, use the **ipv4 address** command in interface configuration mode. To remove an IPv4 address, use the **no** form of this command.

ipv4 address *ipv4-address mask* [**secondary**] [**route-tag** *route-tag value*]
no ipv4 address *ipv4-address mask* [**secondary**] [**route-tag** *route-tag value*]

Syntax Description

ipv4-address	IPv4 address.
mask	Mask for the associated IP subnet. The network mask can be specified in either of two ways: • The network mask can be a four-part dotted decimal address. For example, 255.0.0.0 indicates that each bit equal to 1 means the corresponding address bit belongs to the network address. • The network mask can be indicated as a slash (/) and number. For example, /8 indicates that the first 8 bits of the mask are ones, and the corresponding bits of the address are network address.
secondary	(Optional) Specifies that the configured address is a secondary IPv4 address. If this keyword is omitted, the configured address is the primary IPv4 address.
route-tag	(Optional) Specifies that the configured address has a route tag to be associated with it.
route-tag value	(Optional) Value of the route tag. Range is 1 to 4294967295.

Command Default

No IPv4 address is defined for the interface.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

An interface can have one primary IPv4 address and multiple secondary IPv4 addresses. Packets generated by the software always use the primary IPv4 address. Therefore, all networking devices on a segment should share the same primary network number.



Note The same IPv4 address configured on two different interfaces causes an error message to display that indicates the conflict. The interface located in the highest rack, slot, module, instance, and port is disabled.

Hosts can determine subnet masks using the IPv4 Internet Control Message Protocol (ICMP) mask request message. Networking devices respond to this request with an ICMP mask reply message.

You can disable IPv4 processing on a particular interface by removing its IPv4 address with the **no ipv4 address** command. If the software detects another host using one of its IPv4 addresses, it will display 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 that the system never generates datagrams other than routing updates with secondary source addresses. IPv4 broadcasts and Address Resolution Protocol (ARP) requests are handled properly, as are interface routes in the IP routing table.

Secondary IPv4 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 to have 300 host addresses. Using secondary IPv4 addresses on the networking devices 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 there are many subnets on that segment.

The route-tag feature attaches a tag to all IPv4 addresses. The tag is propagated from the Management Agents (MA) to the Address Repository Managers (RPM) to routing protocols, thus enabling the user to control the redistribution of connected routes by looking at the route tags via RPL scripts.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write

Examples

The following example shows how to set 192.168.1.27 as the primary address and 192.168.7.17 and 192.168.8.17 as the secondary addresses on tenGigE interface 0/0/0/1:

```
RP/0/RP0/CPU0:router(config)# interface tenGigE0/0/0/1
RP/0/RP0/CPU0:router(config-if)# ipv4 address 192.168.1.27 255.255.255.0
RP/0/RP0/CPU0:router(config-if)# ipv4 address 192.168.7.17 255.255.255.0 secondary
RP/0/RP0/CPU0:router(config-if)# ipv4 address 192.168.8.17 255.255.255.0 secondary
```

ipv4 assembler max-packets

To configure the maximum number of packets that are allowed in assembly queues, use the **ipv4 assembler max-packets** command in XR Config mode. To disable this feature, use the **no** from of this command.

ipv4 assembler max-packets *percentage value*
no ipv4 assembler max-packets *percentage value*

Syntax Description

percentage value	Percentage of total packets available in the system. The range is from 1 to 50.

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write

Examples

The following example shows how to configure the maximum number of packets for the assembly queue:

```
RP/0/RP0/CPU0:router(config)# ipv4 assembler max-packets 35
```

ipv4 assembler timeout

To configure the number of seconds an assembly queue can hold before a timeout occurs, use the **ipv4 assembler timeout** command in XR Config mode. To disable this feature, use the **no** form of this command.

ipv4 assembler timeout *seconds*
no ipv4 assembler timeout *seconds*

Syntax Description

seconds	Number of seconds an assembly queue can hold before a timeout occurs. The range is from 1 to 120.

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write

Examples

The following example shows how to configure an assembly queue before a timeout occurs:

```
RP/0/RP0/CPU0:router(config)# ipv4 assembler timeout 88
```

ipv4 mask-reply

To enable the software to respond to IPv4 Internet Control Message Protocol (ICMP) mask requests by sending ICMP mask reply messages, use the **ipv4 mask-reply** command in interface configuration mode. To restore the default, use the **no** form of this command.

ipv4 mask-reply
no ipv4 mask-reply

Syntax Description

This command has no keywords or arguments.

Command Default

IPv4 mask replies are not sent.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

This command enables the software to respond to IPv4 ICMP mask requests by sending ICMP mask reply messages.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write

Examples

The following example enables the sending of ICMP mask reply messages on HundredGigEinterface 0/1/0/0:

```
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/1/0/0
RP/0/RP0/CPU0:router(config-if)# ipv4 mask-reply
```

ipv4 conflict-policy

To enable IP Address Repository Manager (IPARM) conflict resolution, use the **ipv4 conflict-policy** command in XR Config mode. To disable the IPARM conflict resolution, use the **no** form of the command.

ipv4 conflict-policy {**highest-ip** | **longest-prefix** | **static**}
no ipv4 conflict-policy {**highest-ip** | **longest-prefix** | **static**}

Syntax Description

highest-ip	Keeps the highest ip address in the conflict set.
longest-prefix	Keeps the longest prefix match in the conflict set.
static	Keeps the existing interface running across new address configurations.

Command Default

The precedence rule adopted is loopback > physical > other virtual interfaces. Within virtual interfaces, there is an alphabetical preference, for example, loopback1 > loopback2 > tunnel. Among physical interfaces, the lower rack or slot takes control.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use **ipv4 conflict-policy** command to set an IPARM policy that resolves a conflict in the configured addresses. The policy tells IPARM what address to select from the addresses in conflict. The policy then forces the address in conflict to become inactive.

Task ID

Task ID	Operations
ipv4	read, write
ip-services	read, write

Examples

The following example shows how to enable the static policy for conflict resolution:

```
RP/0/RP0/CPU0:router(config)# ipv4 conflict-policy static
```

ipv4 mtu

To set the maximum transmission unit (MTU) size of IPv4 packets sent on an interface, use the **ipv4 mtu** command in interface configuration mode.

To restore the default MTU size, use the **no** form of this command.

ipv4 mtu *bytes*
no ipv4 mtu

Syntax Description

bytes	MTU in bytes. Range is 68 to 65535 bytes for IPv4 packets. The maximum MTU size that can be set on an interface depends on the interface medium.

Command Default

If no MTU size is configured for IPv4 packets sent on an interface, the interface derives the MTU from the Layer 2 MTU.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The router punts the packets that needs fragmentation; whereas the software path drops the subscriber traffic that needs fragmentation.

The maximum MTU size that can be set on an interface depends on the interface medium. If the Layer 2 MTU is smaller than the Layer 3 MTU, the Cisco IOS XR software uses the Layer 2 MTU value for the Layer 3 MTU. Conversely, if the Layer 3 MTU is smaller than the Layer 2 MTU, the software uses Layer 3 MTU value. In other words the Cisco IOS XR software uses the lower of the two values for the MTU.

All devices on a physical medium must have the same protocol MTU to operate.



Note Changing the MTU value (with the **mtu** interface configuration command) can affect the IPv4 MTU value. If the current IPv4 MTU value is the same as the MTU value, and you change the MTU value, the IPv4 MTU value will be modified automatically to match the new MTU. However, the reverse is not true; changing the IPv4 MTU value has no effect on the value for the **mtu** command.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write
config-services	read, write

Examples

This example shows how to set the maximum IPv4 packet size for tenGigE interface 0/0/0/1 to 1500 bytes:

```
RP/0/(config)# interface tenGigE0/0/0/1
RP/0/(config-if)# ipv4 mtu 1500
```

ipv4 unnumbered (point-to-point)

To enable IPv4 processing on a point-to-point interface without assigning an explicit IPv4 address to that interface, use the **ipv4 unnumbered** command in an interface configuration mode. To disable this feature, use the **no** form of this command.

ipv4 unnumbered *interface-type interface-instance*
no ipv4 unnumbered *interface-type interface-instance*

Syntax Description

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

interface-instance	Either a physical interface instance or a virtual interface instance as follows:
	• Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation.
	  • *rack*: Chassis number of the rack.
	  • *slot*: Physical slot number of the modular services card or line card.
	  • *module*: Module number. A physical layer interface module (PLIM) is always 0.
	  • *port*: Physical port number of the interface.
	Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RSP0) and the module is CPU0. Example: interface MgmtEth0/RSP0 /CPU0/0.
	• Virtual interface instance. Number range varies depending on interface type.
	For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

IPv4 processing on a point-to-point interface is disabled unless an IPv4 address is assigned explicitly to that interface.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

For release Release 4.2.0 onward, to enter the dynamic template configuration mode, run the **dynamic-template** command in the XR Config mode.

Whenever the 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 IPv4 packet. It also uses the IPv4 address of the specified

interface in determining which routing processes are sending updates over the unnumbered interface. Restrictions include the following:

- 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.

The interface you specify by the *interface-type* and *interface-number* arguments must be enabled (listed as "up" in the **show interfaces** command display).

Task ID

Task ID	Operations
ipv4	read, write
network	read, write
config-services	read, write

Examples

This example shows how the tenGigE interface 0/0/0/1 is assigned the loopback interface address 5:

```
RP/0/RP0/CPU0:router(config)# interface loopback 5
RP/0/RP0/CPU0:router(config-if)# ipv4 address 192.168.6.6 255.255.255.0
RP/0/RP0/CPU0:router(config)# interface tenGigE 0/0/0/1
RP/0/RP0/CPU0:router(config-if)# ipv4 unnumbered loopback 5
```

ipv6 address

To configure an IPv6 address for an interface and enable IPv6 processing on the interface using an EUI-64 interface ID in the low-order 64 bits of the address, use the **ipv6 address** command in interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address *ipv6-prefix/prefix-length* [**eui-64**] [**route-tag** *route-tag value*]
no ipv6 address *ipv6-prefix/prefix-length* [**eui-64**] [**route-tag** *route-tag value*]

Syntax Description

ipv6-prefix	The IPv6 network assigned to the interface. 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 compose the prefix (the network portion of the address). A slash (/) must precede the decimal value.
eui-64	(Optional) Specifies an interface ID in the low-order 64 bits of the IPv6 address.
route-tag	(Optional) Specifies that the configured address has a route tag to be associated with it.
route-tag value	(Optional) Value of the route tag. Range is 1 to 4294967295.

Command Default

No IPv6 address is defined for the interface.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0	This command was introduced.
Release 7.6.1	The keyword algorithm was added.

Usage Guidelines

If the value specified for the */ prefix-length* argument is greater than 64 bits, the prefix bits have precedence over the interface ID.

Using the **no ipv6 address** command without arguments removes all manually configured IPv6 addresses from an interface.

If the Cisco IOS XR software detects another host using one of its IPv6 addresses, it displays an error message on the console.

The route-tag feature attaches a tag to all IPv6 addresses. The tag is propagated from the Management Agents (MA) to the Address Repository Managers (RPM) to routing protocols, thus enabling the user to control the redistribution of connected routes by looking at the route tags via RPL scripts.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Examples

The following example assigns IPv6 address 2001:0DB8:0:1::/64 to tenGigE interface 0/0/0/1 and specifies an EUI-64 interface ID in the low-order 64 bits of the address:

```
RP/0/RP0/CPU0:router(config)# interface tenGigE0/0/0/1
RP/0/RP0/CPU0:router(config-if)# ipv6 address 2001:0DB8:0:1::/64 eui-64
```

ipv6 assembler

To configure the maximum number of packets that are allowed in assembly queues or to configure the number of seconds an assembly queue will hold before timeout , use the **ipv6 assembler** command in the appropriate configuration mode. To disable this feature, use the **no** form of this command.

ipv6 assembler {**max-packets** *value* | **timeout** *seconds*}
no ipv6 assembler {**max-packets** *value* | **timeout** *seconds*}

Syntax Description

max-packets	Maximum packets allowed in assembly queues.
timeout	Number of seconds an assembly queue will hold before timeout.

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ipv6	read, write

Example

The following example shows how to configure the maximum number of packets that are allowed in assembly queues:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# ipv6 assembler max-packets 100
```

ipv6 conflict-policy

To enable IP Address Repository Manager (IPARM) conflict resolution, use the **ipv6 conflict-policy** command in XR Config mode mode. To disable the IPARM conflict resolution, use the **no** form of the command.

ipv6 conflict-policy {**highest-ip** | **longest-prefix** | **static**}
no ipv6 conflict-policy {**highest-ip** | **longest-prefix** | **static**}

Syntax Description

highest-ip	Keeps the highest IP address in the conflict set.
longest-prefix	Keeps the longest prefix match in the conflict set.
static	Keeps the existing interface running across new address configurations.

Command Default

Default is the lowest rack/slot if no conflict policy is configured.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ipv6	read, write
ip-services	read, write

Examples

The following example shows how to enable the longest prefix policy for conflict resolution:

```
RP/0/RP0/CPU0:router(config)# ipv6 conflict-policy longest-prefix
```

ipv6 address link-local

To configure an IPv6 link-local address for an interface and enable IPv6 processing on the interface, use the **ipv6 address link-local** command in interface configuration mode. The *ipv6-address* value specified with this command overrides the link-local address that is automatically generated for the interface. To remove the address from the interface, use the **no** form of this command.

ipv6 address *ipv6-address* **link-local** [**route-tag** *route-tag value*]
no ipv6 address *ipv6-address* **link-local** [**route-tag** *route-tag value*]

Syntax Description

ipv6-address	The IPv6 address assigned to the interface. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
link-local	Specifies a link-local address. The *ipv6-address* value specified with this command overrides the link-local address that is automatically generated for the interface.
route-tag	(Optional) Specifies that the configured address has a route-tag to be associated with it.
route-tag value	(Optional) Displays the route-tag value. Range is 1 to 4294967295.

Command Default

No IPv6 address is defined for the interface.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

If the Cisco IOS XR software detects another host using one of its IPv6 addresses, the software displays an error message on the console.

The system automatically generates a link-local address for an interface when IPv6 processing is enabled on the interface, typically when an IPv6 address is configured on the interface. To manually specify a link-local address to be used by an interface, use the **ipv6 address link-local** command.

A double colon may be used as part of the *ipv6-address* argument when consecutive 16-bit values are denoted as zero. You can configure multiple IPv6 addresses per interfaces, but only one link-local address.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Examples

The following example shows how to assign FE80::260:3EFF:FE11:6770 as the link-local address for tenGigE interface 0/0/0/1:

```
RP/0/RP0/CPU0:router(config)# interface tenGigE0/0/0/1
RP/0/RP0/CPU0:router(config-if)# ipv6 address FE80::260:3EFF:FE11:6770 link-local
```

ipv6 enable

To enable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **ipv6 enable** command in an appropriate configuration mode. To disable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **no** form of this command.

ipv6 enable
no ipv6 enable

Syntax Description

None

Command Default

IPv6 is disabled.

Command Modes

Interface configuration (not applicable for BNG)

Dynamic template configuration (for BNG)

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **ipv6 enable** command automatically configures an IPv6 link-local unicast address on the interface while also enabling the interface for IPv6 processing. The **no ipv6 enable** command does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address.

For BNG, ensure you run this command in the dynamic template configuration mode. To enter the dynamic template configuration mode, run **dynamic-template** command in the XR EXEC mode.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

This example (not applicable for BNG) shows how to enable IPv6 processing on tenGigE interface 0/0/0/1:

```
RP/0/RP0/CPU0:router(config)# interface tenGigE0/0/0/1
RP/0/RP0/CPU0:router(config-if)# ipv6 enable
```

For BNG, this example show how to enable IPv6 processing on dynamic template configuration mode:

```
RP/0/RP0/CPU0:router(config)# dynamic-template type ppp foo
RP/0/RP0/CPU0:router(config-dynamic-template-type)# ipv6 enable
```

ipv6 hop-limit

To configure the maximum number of hops used in router advertisements and all IPv6 packets that are originated by the router, use the **ipv6 hop-limit** command in XR Config mode mode. To return the hop limit to its default value, use the **no** form of this command.

ipv6 hop-limit *hops*
no ipv6 hop-limit *hops*

Syntax Description

hops	Maximum number of hops. Range is 1 to 255.

Command Default

hops : 64 hops

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Examples

The following example shows how to configure a maximum number of 15 hops for router advertisements and all IPv6 packets that are originated from the router:

```
RP/0/RP0/CPU0:router(config)# ipv6 hop-limit 15
```

ipv6 icmp error-interval

To configure the interval and bucket size for IPv6 Internet Control Message Protocol (ICMP) error messages on all nodes, use the **ipv6 icmp error-interval** command in XR Config mode mode. To return the interval to its default setting, use the **no** form of this command.

ipv6 icmp error-interval *milliseconds* [*bucketsize*]
no ipv6 icmp error-interval

Syntax Description

milliseconds	Time interval (in milliseconds) between tokens being placed in the bucket. Range is 0 to 2147483647.
bucketsize	(Optional) The maximum number of tokens stored in the bucket. The acceptable range is 1 to 200 with a default of 10 tokens.

Command Default

ICMP rate limiting is enabled by default. To disable ICMP rate limiting, set the interval to zero.

milliseconds : 100 milliseconds

bucketsize : 10 tokens

Command Modes

XR Config mode

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

Use the **ipv6 icmp error-interval** command in XR Config mode mode to limit the rate at which IPv6 ICMP error messages are sent for each node. A token bucket algorithm is used with one token representing one IPv6 ICMP error message. Tokens are placed in the virtual bucket at a specified interval until the maximum number of tokens allowed in the bucket is reached.

The *milliseconds* argument specifies the time interval between tokens being placed in the bucket. The optional *bucketsize* argument is used to define the maximum number of tokens stored in the bucket. Tokens are removed from the bucket when IPv6 ICMP error messages are sent, which means that if the *bucketsize* argument is set to 20, a rapid succession of 20 IPv6 ICMP error messages can be sent. When the bucket is empty of tokens, IPv6 ICMP error messages are not sent until a new token is placed in the bucket.

Use the **show ipv6 traffic** EXEC command to display IPv6 ICMP rate-limited counters.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Examples

The following example shows an interval of 50 milliseconds and a bucket size of 20 tokens being configured for IPv6 ICMP error messages:

```
RP/0/RP0/CPU0:router(config)# ipv6 icmp error-interval 50 20
```

ipv6 mtu

To set the maximum transmission unit (MTU) size of IPv6 packets sent on an interface, use the **ipv6 mtu** command in an appropriate configuration mode.

To restore the default MTU size, use the **no** form of this command.

ipv6 mtu *bytes*
no ipv6 mtu

Syntax Description

bytes	MTU in bytes. Range is 1280 to 65535 for IPv6 packets. The maximum MTU size that can be set on an interface depends on the interface medium.

Command Default

If no MTU size is configured for IPv6 packets sent on an interface, the interface derives the MTU from the Layer 2 MTU.

Command Modes

Interface configuration (not applicable for BNG)

Dynamic template configuration (for BNG)

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

If an IPv6 packet exceeds the MTU set for the interface, only the source router of the packet can fragment it.

The maximum MTU size that can be set on an interface depends on the interface medium. If the Layer 2 MTU is smaller than the Layer 3 MTU, the Cisco IOS XR software uses the Layer 2 MTU value for the Layer 3 MTU. Conversely, If the Layer 3 MTU is smaller than the Layer 2 MTU, the software uses Layer 3 MTU value. In other words the Cisco IOS XR software uses the lower of the two values for the MTU.

All devices on a physical medium must have the same protocol MTU to operate.

For BNG, ensure you run this command in the dynamic template configuration mode. To enter the dynamic template configuration mode, run **dynamic-template** command in the XR Config mode.



Note Changing the MTU value (with the **mtu** interface configuration command) can affect the IPv6 MTU value. If the current IPv6 MTU value is the same as the MTU value, and you change the MTU value, the IPv6 MTU value will be modified automatically to match the new MTU. However, the reverse is not true; changing the IPv6 MTU value has no effect on the value for the **mtu** command.

Task ID

Task ID	Operations
ipv6	read, write

Task ID	Operations
network	read, write
config-services	read, write

Examples

This example (not applicable for BNG) shows how to set the maximum IPv6 packet size for tenGigE interface 0/0/0/1 to 1350 bytes:

```
RP/0/RP0/CPU0:router(config)# interface tenGigE0/0/0/1
RP/0/RP0/CPU0:router(config-if)# ipv6 mtu 1350
```

For BNG, this example shows how to set the maximum IPv6 packet size to 1350 bytes in the dynamic template configuration mode:

```
RP/0/RP0/CPU0:router(config)# dynamic-template type ppp foo
RP/0/RP0/CPU0:router(config-dynamic-template-type)# ipv6 mtu 1350
```

ipv6 nd dad attempts

To configure the number of consecutive neighbor solicitation messages that are sent on an interface while duplicate address detection is performed on the unicast IPv6 addresses of the interface, use the **ipv6 nd dad attempts** command in an appropriate configuration mode. To return the number of messages to the default value, use the **no** form of this command.

ipv6 nd dad attempts *value*
no ipv6 nd dad attempts *value*

Syntax Description

value	Number of neighbor solicitation messages. Range is 0 to 600. Configuring a value of 0 disables duplicate address detection processing on the specified interface; a value of 1 configures a single transmission without follow-up transmissions.

Command Default

Duplicate address detection on unicast IPv6 addresses with the sending of one neighbor solicitation message is enabled. The default is one message.

Command Modes

Interface configuration (not applicable for BNG)

Dynamic template configuration (for BNG)

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Duplicate address detection verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces (the new addresses remain in a tentative state while duplicate address detection is performed). Duplicate address detection uses neighbor solicitation messages to verify the uniqueness of unicast IPv6 addresses.

The DupAddrDetectTransmits node configuration variable (as specified in RFC 2462, *IPv6 Stateless Address Autoconfiguration*) is used to automatically determine the number of consecutive neighbor solicitation messages that are sent on an interface while duplicate address detection is performed on a tentative unicast IPv6 address.

The interval between the sending of duplicate address detection neighbor solicitation messages (the duplicate address detection timeout interval) is specified by the neighbor discovery-related variable RetransTimer (as specified in RFC 2461, *Neighbor Discovery for IP Version 6 [IPv6]*), which is used to determine the time between retransmissions of neighbor solicitation messages to a neighbor when the address is being resolved or when the reachability of a neighbor is being probed. This is the same management variable used to specify the interval for neighbor solicitation messages during address resolution and neighbor unreachability detection. Use the **ipv6 nd ns-interval** command to configure the interval between neighbor solicitation messages that are sent during duplicate address detection.

Duplicate address detection is suspended on interfaces that are administratively down. While an interface is administratively down, the unicast IPv6 addresses assigned to the interface are set to a pending state. Duplicate address detection is automatically restarted on an interface when the interface returns to being administratively up.

For BNG, ensure you run this command in the dynamic template configuration mode. To enter the dynamic template configuration mode, run **dynamic-template** command in the .

Note An interface returning to administratively up restarts duplicate address detection for all of the unicast IPv6 addresses on the interface. While duplicate address detection is performed on the link-local address of an interface, the state for the other IPv6 addresses is still set to tentative. When duplicate address detection is completed on the link-local address, duplicate address detection is performed on the remaining IPv6 addresses.

When duplicate address detection identifies a duplicate address, the state of the address is set to duplicate and the address is not used. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface and an error message similar to the following is issued:

```
ipv6_nd[145]: %IPV6_ND-3-ADDRESS_DUPLICATE : Duplicate address 111::1 has been detected
```

If the duplicate address is a global address of the interface, the address is not used and an error message similar to the following is issued:

```
%IPV6-4-DUPLICATE: Duplicate address 3000::4 on tenGigE&;
```

All configuration commands associated with the duplicate address remain as configured while the state of the address is set to duplicate.

If the link-local address for an interface changes, duplicate address detection is performed on the new link-local address and all of the other IPv6 address associated with the interface are regenerated (duplicate address detection is performed only on the new link-local address).

Task ID

Task ID	Operations
ipv6	read, write
config-services	read, write

Examples

This example (not applicable for BNG) shows how to set the number of consecutive neighbor solicitation messages for interface 0/2/0/1 to 1 and then display the state (tentative or duplicate) of the unicast IPv6 address configured for an interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/2/0/1
RP/0/RP0/CPU0:router(config-if)# ipv6 nd dad attempts 1
RP/0/RP0/CPU0:router(config-if)# Uncommitted changes found, commit them before
exiting(yes/no/cancel)? [cancel]:y

RP/0/RP0/CPU0:router# show ipv6 interface
HundredGigE/2/0/0 is Up, line protocol is Up
  IPv6 is disabled, link-local address unassigned
  No global unicast address is configured
HundredGigE/2/0/1 is Up, line protocol is Up
  IPv6 is enabled, link-local address is fe80::203:fdff:fe1b:4501
  Global unicast address(es):
    1:4::1, subnet is 1:4::/64 [DUPLICATE]
  MTU is 1514 (1500 is available to IPv6)
```

```
  ICMP redirects are disabled
  ND DAD is enabled, number of DAD attempts 1
  ND reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
HundredGigE/2/0/2 is Shutdown, line protocol is Down
  IPv6 is enabled, link-local address is fe80::200:11ff:fe11:1111 [TENTATIVE]
  Global unicast address(es):
    111::2, subnet is 111::/64 [TENTATIVE]
  MTU is 1514 (1500 is available to IPv6)
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts 1
  ND reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
```

For BNG, this example shows how to display the state (tentative or duplicate) of the unicast IPv6 address on the dynamic template configuration mode:

```
RP/0/RP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RP0/CPU0:router(config-dynamic-template-type)# ipv6 nd dad attempts 1
```

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 an appropriate 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 keywords or arguments.

Command Default

The managed address configuration flag is not set in IPv6 router advertisements.

Command Modes

Interface configuration (not applicable for BNG)

Dynamic template configuration (for BNG)

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Setting the managed address configuration 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.

For BNG, ensure you run this command in the dynamic template configuration mode. To enter the dynamic template configuration mode, run **dynamic-template** command in the XR EXEC mode.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

This example (not applicable for BNG) shows how to configure the managed address configuration flag in IPv6 router advertisements on HundredGigE interface 0/1/0/1:

```
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/1/0/1
RP/0/RP0/CPU0:router(config-if)# ipv6 nd managed-config-flag
```

For BNG, this example shows how to configure the managed address configuration flag in IPv6 router advertisements on dynamic template configuration mode:

```
RP/0/RP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RP0/CPU0:router(config-dynamic-template-type)# ipv6 nd managed-config-flag
```

ipv6 nd ns-interval

To configure the interval between IPv6 neighbor solicitation retransmissions on an interface, use the **ipv6 nd ns-interval** command in an appropriate configuration mode. To restore the default interval, use the **no** form of this command.

ipv6 nd ns-interval *milliseconds*
no ipv6 nd ns-interval

Syntax Description

milliseconds	Interval (in milliseconds) between IPv6 neighbor solicit transmissions. Range is 1000 to 3600000.

Command Default

0 milliseconds (unspecified) is advertised in router advertisements, and the value 1000 is used for the neighbor discovery activity of the router itself.

Command Modes

Interface configuration (not applicable for BNG)

Dynamic template configuration (for BNG)

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

This value is included in all IPv6 router advertisements sent out from this interface. Very short intervals are not recommended in normal IPv6 operation. When a nondefault value is configured, the configured time is both advertised and used by the router itself.

For BNG, ensure you run this command in the dynamic template configuration mode. To enter the dynamic template configuration mode, run **dynamic-template** command in the XR Config mode.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

This example (not applicable for BNG) configures an IPv6 neighbor solicit transmission interval of 9000 milliseconds for tenGigE interface 0/1/0/1:

```
RP/0/RP0/CPU0:router(config)# interface tenGigE0/1/0/1
RP/0/RP0/CPU0:router(config-if)# ipv6 nd ns-interval 9000
```

For BNG, this example configures an IPv6 neighbor solicit transmission interval of 9000 milliseconds in the dynamic template configuration mode:

```
RP/0/RP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RP0/CPU0:router(config-dynamic-template-type)# ipv6 nd ns-interval 9000
```

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 an appropriate 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 keywords or arguments.

Command Default

The other stateful configuration flag is not set in IPv6 router advertisements.

Command Modes

Interface configuration (not applicable for BNG)

Dynamic template configuration (for BNG)

Command History

Release	Modification
Release 6.0	This command was introduced.

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.

For BNG, ensure you run this command in the dynamic template configuration mode. To enter the dynamic template configuration mode, run **dynamic-template** command in the XR Config mode.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

This example (not applicable for BNG) configures the “other stateful configuration” flag in IPv6 router advertisements on HundredGigE interface 0/1/0/1:

```
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/1/0/1
RP/0/RP0/CPU0:router(config-if)# ipv6 nd other-config-flag
```

For BNG, this example configures the “other stateful configuration” flag for IPv6 router advertisements in the dynamic template configuration mode:

```
RP/0/RP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RP0/CPU0:router(config-dynamic-template-type)# ipv6 nd other-config-flag
```

ipv6 nd prefix

To configure how IPv6 prefixes are advertised in IPv6 router advertisements, use the **ipv6 nd prefix** command in interface configuration mode. To advertise a prefix with default parameter values, use the **no** form of this command. To prevent a prefix (or prefixes) from being advertised, use the **no- adv** keyword.

ipv6 nd prefix {*ipv6prefix/prefix-length* | **default** [*valid-lifetime* | **at** | **infinite** | **no-adv** | **no-autoconfig** | **off-link**]}
no ipv6 nd prefix {*ipv6prefix/prefix-length* | **default** [*valid-lifetime* | **at** | **infinite** | **no-adv** | **no-autoconfig** | **off-link**]}

Syntax Description

ipv6-prefix	The IPv6 network number to include in router advertisements. This keyword 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 compose the prefix (the network portion of the address). A slash (/) must precede the decimal value.
default	(Optional) Specifies all prefixes.
valid-lifetime	(Optional) The amount of time (in seconds) that the specified IPv6 prefix is advertised as being valid. The range of values is 0 to 4294967295 seconds.
at	(Optional) The date and time at which the lifetime and preference expire. The prefix is valid until this specified date and time are reached. Dates are expressed in the form *date-valid-expire month-valid-expire hh:mm-valid-expire date-prefer-expire month-prefer-expire hh:mm-prefer-expire.*
infinite	(Optional) The valid lifetime does not expire.
no-adv	(Optional) The prefix is not advertised.
no-autoconfig	(Optional) Indicates to hosts on the local link that the specified prefix cannot be used for IPv6 autoconfiguration.
off-link	(Optional) Indicates that the specified prefix is assigned to the link. Nodes sending traffic to such addresses that contain the specified prefix consider the destination to be locally reachable on the link. This prefix should not be used for *onlink* determination.

Command Default

All prefixes configured on interfaces that originate IPv6 router advertisements are advertised with a valid lifetime of 2592000 seconds (30 days) and a preferred lifetime of 604800 seconds (7 days), and with both the "onlink" and "autoconfig" flags set.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

This command allows control over the individual parameters per prefix, including whether or not the prefix should be advertised.

To control how prefixes are advertised, use the **ipv6 nd prefix** command. By default, prefixes configured as addresses on an interface using the **ipv6 address** command are advertised with default values. If you configure prefixes for advertisement using the **ipv6 nd prefix** command, only the specified prefixes are advertised with the configured values, all other prefixes are advertised with default values.

The default keyword can be used to set default parameters for all prefixes.

A date can be set to specify the expiration of a prefix. The valid and preferred lifetimes are counted down in real time. When the expiration date is reached, the prefix is no longer advertised.

When onlink is “on” (by default), the specified prefix is assigned to the link. Nodes sending traffic to such addresses that contain the specified prefix consider the destination to be locally reachable on the link.

When autoconfig is “on” (by default), it indicates to hosts on the local link that the specified prefix can be used for IPv6 autoconfiguration.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Examples

The following example includes the IPv6 prefix 2001:0DB8::/35 in router advertisements sent out HundredGigE interface 0/1/0/0 with a valid lifetime of 1000 seconds and a preferred lifetime of 900 seconds:

```
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/1/0/0
RP/0/RP0/CPU0:router(config-if)# ipv6 nd prefix 2001:0DB8::/35 1000 900
```

ipv6 nd ra-interval

To configure the interval between IPv6 router advertisement transmissions on an interface, use the **ipv6 nd ra-interval** command in an appropriate configuration mode. To restore the default interval, use the **no** form of this command.

ipv6 nd ra-interval *seconds*
no ipv6 nd ra-interval *seconds*

Syntax Description

seconds	The interval (in seconds) between IPv6 router advertisement transmissions.

Command Default

seconds : 200 seconds

Command Modes

Interface configuration (not applicable for BNG)

Dynamic template configuration (for BNG)

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The interval between transmissions should be less than or equal to the IPv6 router advertisement lifetime if the router is configured as a default router by using the **ipv6 nd ra-lifetime** command. To prevent synchronization with other IPv6 nodes, randomly adjust the actual value used to within 20 percent of the specified value.

For BNG, ensure you run this command in the dynamic template configuration mode. To enter the dynamic template configuration mode, run **dynamic-template** command in the XR Config mode.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

This example (not applicable for BNG) configures an IPv6 router advertisement interval of 201 seconds on HundredGigE interface 0/1/0/1:

```
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/1/0/1
RP/0/RP0/CPU0:router(config-if)# ipv6 nd ra-interval 201
```

For BNG, this example configures an IPv6 router advertisement interval of 201 seconds in the dynamic template configuration mode:

```
RP/0/RP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RP0/CPU0:router(config-dynamic-template-type)# ipv6 nd ra-interval 201
```

ipv6 nd ra-lifetime

To configure the router lifetime value in IPv6 router advertisements on an interface, use the **ipv6 nd ra-lifetime** command in an appropriate configuration mode. To restore the default lifetime, use the **no** form of this command.

ipv6 nd ra-lifetime *seconds*
no ipv6 nd ra-lifetime

Syntax Description

seconds	The validity (in seconds) of this router as a default router on this interface.

Command Default

seconds : 1800 seconds

Command Modes

Interface configuration (not applicable for BNG)

Dynamic template configuration (for BNG)

Usage Guidelines

The router lifetime value is included in all IPv6 router advertisements sent out the interface. The value indicates the usefulness of the router as a default router on this interface. Setting the value to 0 indicates that the router should not be considered a default router on this interface. The router lifetime value can be set to a nonzero value to indicate that it should be considered a default router on this interface. The nonzero value for the router lifetime value should not be less than the router advertisement interval.

For BNG, ensure you run this command in the dynamic template configuration mode. To enter the dynamic template configuration mode, run **dynamic-template** command in the XR Config mode.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

This example (not applicable for BNG) configures an IPv6 router advertisement lifetime of 1801 seconds on HundredGigE interface 0/1/0/1:

```
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/1/0/1
RP/0/RP0/CPU0:router(config-if)# ipv6 nd ra-lifetime 1801
```

For BNG, this example configures an IPv6 router advertisement lifetime of 1801 seconds in the dynamic template configuration mode:

```
RP/0/RP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RP0/CPU0:router(config-dynamic-template-type)# ipv6 nd ra-lifetime 1801
```

ipv6 nd reachable-time

To configure the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred, use the **ipv6 nd reachable-time** command in an appropriate configuration mode. To restore the default time, use the **no** form of this command.

ipv6 nd reachable-time *milliseconds*
no ipv6 nd reachable-time

Syntax Description

milliseconds	The amount of time (in milliseconds) that a remote IPv6 node is considered reachable. The range is from 0 to 3600000.

Command Default

0 milliseconds (unspecified) is advertised in router advertisements and 30000 (30 seconds) is used for the neighbor discovery activity of the router itself.

Command Modes

Interface configuration (not applicable for BNG)

Dynamic template configuration (for BNG)

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The configured time enables the router to detect unavailable neighbors. Shorter configured times enable the router to detect unavailable neighbors more quickly; however, shorter times consume more IPv6 network bandwidth and processing resources in all IPv6 network devices. Very short configured times are not recommended in normal IPv6 operation.

The configured time is included in all router advertisements sent out of an interface so that nodes on the same link use the same time value. A value of 0 indicates that the configured time is unspecified by this router.

For BNG, ensure you run this command in the dynamic template configuration mode. To enter the dynamic template configuration mode, run **dynamic-template** command in the XR Config mode.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

This example (not applicable for BNG) shows how to configure an IPv6 reachable time of 1,700,000 milliseconds for HundredGigE interface 0/1/0/1:

```
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/1/0/1
```

```
RP/0/RP0/CPU0:router(config-if)# ipv6 nd reachable-time 1700000
```

For BNG, this example shows how to configure an IPv6 reachable time of 1,700,000 milliseconds in the dynamic template configuration mode:

```
RP/0/RP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RP0/CPU0:router(config-dynamic-template-type)# ipv6 nd reachable-time 1700000
```

ipv6 nd redirects

To send Internet Control Message Protocol (ICMP) redirect messages, use the **ipv6 nd redirects** command in interface configuration mode. To restore the system default, use the **no** form of this command.

ipv6 nd redirects
no ipv6 nd redirects

Syntax Description

This command has no keywords or arguments.

Command Default

The default value is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

This command has no keywords or arguments.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Examples

The following example shows how to redirect IPv6 nd-directed broadcasts on HundredGigE interface 0/2/0/2:

```
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/2/0/2
RP/0/RP0/CPU0:router(config-if)# ipv6 nd redirects
```

ipv6 nd scavenge-timeout

To set the lifetime for neighbor entries in the stale state, use the **ipv6 nd scavenge-timeout** command in XR Config mode mode. To disable this feature, use the **no** form of this command.

ipv6 nd scavenge-timeout *seconds*
no ipv6 nd scavenge-timeout *seconds*

Syntax Description

seconds	RA lifetime in seconds. The range is from 0 to 43200.

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

When the scavenge-timer for a neighbor entry expires, the entry is cleared.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Examples

The following example shows how to set the lifetime for the neighbor entry:

```
RP/0/RP0/CPU0:router(config)# ipv6 nd scavenge-timeout 3000
```

ipv6 nd suppress-ra

To suppress IPv6 router advertisement transmissions on a LAN interface, use the **ipv6 nd suppress-ra** command in an appropriate configuration mode. To reenable the sending of IPv6 router advertisement transmissions on a LAN interface, use the **no** form of this command.

ipv6 nd suppress-ra
no ipv6 nd suppress-ra

Syntax Description

This command has no keywords or arguments.

Command Default

IPv6 router advertisements are automatically sent on other types of interlaces if IPv6 unicast routing is enabled on the interfaces. IPv6 router advertisements are not sent on other types of interfaces.

Command Modes

Interface configuration (not applicable for BNG)

Dynamic template configuration (for BNG)

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **no ipv6 nd suppress-ra** command to enable the sending of IPv6 router advertisement transmissions on non-LAN interface types (for example, serial or tunnel interfaces).

For BNG, ensure you run this command in the dynamic template configuration mode. To enter the dynamic template configuration mode, run **dynamic-template** command in the XR Config mode.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

This example (not applicable for BNG) shows how to suppress IPv6 router advertisements on HundredGigE interface 0/1/0/1:

```
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/1/0/1
RP/0/RP0/CPU0:router(config-if)# ipv6 nd suppress-ra
```

For BNG, this example shows how to suppress IPv6 router advertisements in the dynamic template configuration mode:

```
RP/0/RP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RP0/CPU0:router(config-dynamic-template-type)# ipv6 nd suppress-ra
```

ipv6 neighbor

To configure a static entry in the IPv6 neighbor discovery cache, use the **ipv6 neighbor** command in XR Config mode mode. To remove a static IPv6 entry from the IPv6 neighbors discovery cache, use the **no** form of this command.

ipv6 neighbor *ipv6-address interface-type interface-instance hardware-address*
no ipv6 neighbor *ipv6-address interface-type interface-instance hardware-address*

Syntax Description

ipv6-address	The IPv6 address that corresponds to the local data-link 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 type. For more information, use the question mark (?) online help function.

interface-instance	Either a physical interface instance or a virtual interface instance as follows:
	• Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation.
	  • *rack*: Chassis number of the rack.
	  • *slot*: Physical slot number of the modular services card or line card.
	  • *module*: Module number. A physical layer interface module (PLIM) is always 0.
	  • *port*: Physical port number of the interface.
	Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RSP0) and the module is CPU0. Example: interface MgmtEth0/RSP0 /CPU0/0.
	• Virtual interface instance. Number range varies depending on interface type.
	For more information about the syntax for the router, use the question mark (?) online help function.

hardware-address	The local data-link address (a 48-bit address).

Command Default

Static entries are not configured in the IPv6 neighbor discovery cache.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **ipv6 neighbor** command is similar to the **arp** (global) command.

If an entry for the specified IPv6 address already exists in the neighbor discovery cache—learned through the IPv6 neighbor discovery process—the entry is automatically converted to a static entry.

Use the **show ipv6 neighbors** command to display static entries in the IPv6 neighbors discovery cache. A static entry in the IPv6 neighbor discovery cache has one state: reach (reachable)—The interface for this entry is up. If the interface for the entry is down, the **show ipv6 neighbors** command does not show the entry.

Note Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache; therefore, the descriptions for the reach (reachable) state are different for dynamic and static cache entries. See the **show ipv6 neighbors** command for a description of the reach (reachable) state for dynamic cache entries.

The **clear ipv6 neighbors** command deletes all entries in the IPv6 neighbors discovery cache, except static entries. The **no ipv6 neighbor** command deletes a specified static entry from the neighbor discovery cache; the command does not remove dynamic entries—learned from the IPv6 neighbor discovery process—from the cache. Disabling IPv6 on an interface by using the **no ipv6 enable** or the **no ipv6 unnumbered** command deletes all IPv6 neighbor discovery cache entries configured for that interface, except static entries (the state of the entry changes to reach [reachable]).

Static entries in the IPv6 neighbor discovery cache are not modified by the neighbor discovery process.

Note Static entries for IPv6 neighbors can be configured only on IPv6-enabled LAN and ATM LAN Emulation interfaces.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Examples

The following example shows how to configure a static entry in the IPv6 neighbor discovery cache for a neighbor with the IPv6 address 2001:0DB8::45A and link-layer address 0002.7D1A.9472 on ethernet interface 0/RSP0/CPU0:

```
RP/0/RP0/CPU0:router(config)# ipv6 neighbor 2001:0DB8::45A 0002.7D1A.9472
```

ipv6 path-mtu enable

To enable the command to configure path maximum transmission unit (MTU) discovery of IPv6 packets, use the **ipv6 path-mtu enable** command in the XR Config mode.

ipv6 path-mtu enable

Command Default

None.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Path MTU discovery for IPv6 packets is supported only for applications using TCP and Ping protocol.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

This example shows how to enable path MTU discovery command of IPv6 packets:

```
RP/0/RP0/CPU0:router(config)#  ipv6 path-mtu enable
```

ipv6 path-mtu timeout

To set the maximum transmission unit (MTU) timeout value of IPv6 packets, use the **ipv6 path-mtu timeout** command in the XR Config mode.

ipv6 path-mtu timeout *minutes*

Syntax Description

minutes	MTU timeout in minutes. Range is 1 to 15 minutes. Default timeout value is 10 minutes.

Command Default

None.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Path MTU discovery for IPv6 packets is supported only for applications using TCP and Ping protocol.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

This example shows how to set path MTU timeout of IPv6 packets:

```
RP/0/RP0/CPU0:router(config)#  ipv6 path-mtu timeout 15
```

ipv6 source-route

To enable processing of the IPv6 type source (type 0) routing header, use the **ipv6 source-route** command in XR EXEC mode mode. To disable the processing of this IPv6 extension header, use the **no** form of this command.

ipv6 source-route
no ipv6 source-route

Syntax Description

This command has no keywords or arguments.

Command Default

The **no** version of the **ipv6 source-route** command is the default.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **no ipv6 source-route** command (which is the default) prevents hosts from performing source routing using your routers. When the **no ipv6 source-route** command is configured and the router receives a packet with a type 0 source routing header, the router drops the packet and sends an IPv6 ICMP error message back to the source and logs an appropriate debug message.

Task ID

Task ID	Operation
network	read, write
ipv6	read, write

Example

The following example shows how to allow the processing of any IPv6 datagrams containing a source-route header option:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# ipv6 source-route
RP/0/RP0/CPU0:router(config)#
```

ipv6 tcp-mss-adjust

To enable the transit traffic of TCP flows to be a Maximum Segment Size (MSS) below the GRE tunnel interface or VLAN sub-interface MTU so that traffic fragmentation is prevented when a session is established for IPv6 packets, use the **ipv6 tcp-mss-adjust** command in the interface configuration submode. To disable the transit traffic of TCP flows to be a Maximum Segment Size (MSS) below the GRE tunnel interface or VLAN sub-interface MTU, use the **no** form of this command.

ipv6 tcp-mss-adjust enable
no ipv6 tcp-mss-adjust enable

Syntax Description

enable	Enables Maximum Segment Size (MSS) adjustment for tcp flows on the interface..

Command Default

None

Command Modes

Interface Configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

This command has no keywords or arguments.

Task ID

Task ID	Operation
mpls-te	read, write
ipv6	read, write

Example

This example shows how to enable the transit traffic of TCP flows for IPv6 packets using the **ipv6 tcp-mss-adjust** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface HundredEthernet 0/0/0/4.20
RP/0/RP0/CPU0:router(config-if)# ipv6 tcp-mss-adjust enable
```

ipv6 virtual address

To define an IPv6 virtual address for a network of management Ethernet interfaces, use the **ipv6 virtual address** command in XR Config mode. To remove an IPv6 virtual address from the configuration, use the **no** form of this command.

ipv6 virtual address {[**vrf** *vrf-name*]*ipv6-address/prefix-length* | **use-as-src-addr**}
no ipv6 virtual address {[**vrf** *vrf-name*]*ipv6-address/prefix-length* | **use-as-src-addr**}

Syntax Description

vrf *vrf-name*	(Optional) Configures the virtual address on a per VPN routing and forwarding (VRF) basis for the management interfaces The *vrf-name* argument specifies the name of the VRF.
ipv6 address	The virtual IPv6 address to be used.
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). A slash mark must precede the decimal value.
use-as-src-addr	Enables the virtual address to be used as the default SRC address on sourced packets.

Command Default

No IPv6 virtual address is defined for the configuration.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Configuring an IPv6 virtual address enables you to access the router from a single virtual address with a management network. An IPv6 virtual address persists across route processor (RP) failover situations.

Configuring an IPv6 virtual address enables you to access a dual RP router from a single address without prior knowledge of which RP is active. An IPv6 virtual address persists across RP failovers. For this to happen, the virtual IPv6 address must share a common IPv6 subnet with a Management Ethernet interface on both RPs.

If you disable the **ipv6 virtual address** command with the **vrf** keyword, the virtual IP address is unconfigured for the corresponding VRF or for the default if no VRF is specified. This results in the removal of the entry for the virtual IP address in the VRF table and in the ARP cache.

The default VRF is chosen when no VRF is specified. The virtual IP address is activated on a management interface that is attached to a default VRF.

The **use-as-src-addr** keyword eliminates the need for configuring a loopback interface as the source interface (that is, update source) for management applications. When an update source is not configured, management applications allow the transport processes (TCP, UDP, raw_ip) to pick a suitable source address. The transport processes, in turn, consult the FIB to do so. If a Management Ethernet's IP address is picked as the source address and if the **use-as-src-addr keyword** is configured, then the transport processes replace the Management Ethernet's IP address with a relevant virtual IP address. This functionality works across RP switchovers.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Examples

The following example shows how to define an IPv6 virtual address:

```
RP/0/RP0/CPU0:router(config)# ipv6 virtual address 0:0:0:7272::72/64
```

The following example shows how to configure the virtual IP addresses for management interfaces on a per VRF basis:

```
RP/0/RP0/CPU0:router(config)# ipv6 virtual address vrf ppp 0:0:0:7272::72/64
```

show arm conflicts

To display IPv4 or IPv6 address conflict information identified by the Address Repository Manager (ARM), use the **show arm conflicts** command in XR EXEC mode.

show arm {**ipv4** | **ipv6**} [**vrf** *vrf-name*] **conflicts** [**address** | **override** | **unnumbered**]

Syntax Description

ipv4	Displays IPv4 address conflicts.
ipv6	Displays IPv6 address conflicts.
vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information. Available for IPv4 only.
vrf-name	(Optional) Name of a VRF.
address	(Optional) Displays address conflict information.
override	(Optional) Displays address conflict override information.
unnumbered	(Optional) Displays unnumbered interface conflict information.

Command Default

None

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **show arm conflicts** command to display information about IPv4 or IPv6 address conflicts. You can use address conflict information to identify misconfigured IPv4 or IPv6 addresses.

Conflict information is displayed for interfaces that are forced down and for interfaces that are up.

Issuing the **show arm conflicts** command without specifying any optional keywords displays the output generated from both the **address** and **unnumbered** keywords.

Task ID

Task ID	Operations
network	read

Examples

The following sample output is from the **show arm ipv4 conflicts** command:

```
RP/0/RP0/CPU0:router# show arm ipv4 conflicts

F Forced down
| Down interface & addr                  Up interface & addr

F Lo2 10.1.1.2/24                         Lo1 10.1.1.1/24

Forced down interface          Up interface
```

```
tu2->tu1                        tu1->Lo1
```

The following is sample output from the **show arm ipv4 conflicts** command with the **address** keyword:

```
RP/0/RP0/CPU0:router# show arm ipv4 conflicts address

F Forced down
| Down interface & addr                   Up interface & addr

F Lo2 10.1.1.2/24                          Lo1 10.1.1.1/24
```

The following is sample output from the **show arm ipv4 conflicts** command with the **unnumbered** keyword:

```
RP/0/RP0/CPU0:router# show arm ipv4 conflicts unnumbered

Forced down interface          Up interface                   VRF
tu2->tu1                       tu1->Lo1
```

This table describes the significant fields shown in the display.

Table 43: show arm conflicts Command Field Descriptions

Field	Description
Forced down	Legend defining a symbol that may appear in the output for this command.
Down interface & addr	Forced down interface name, type, and address.
Up interface & addr	List of interfaces that are up.
Forced down interface	Unnumbered interfaces that are in conflict and forced down.
Up interface	Unnumbered interfaces that are in conflict and are up.

show arm registrations producers

To display producer registration information for the Address Repository Manager (ARM), use the **show arm registrations producers** command in XR EXEC mode.

show arm {**ipv4** | **ipv6**} **registrations producers**

Syntax Description

ipv4	Displays IPv4 producer registration information.
ipv6	Displays IPv6 producer registration information.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **show arm registrations producers** command to display information on producers of IP ARM registrations. Registration information is displayed with the ID.

Task ID

Task ID	Operations
network	read

Examples

The following is sample output from the **show arm registrations producers** command:

```
RP/0/RP0/CPU0:router# show arm ipv4 registrations producers

Id    Node            Producer Id   IPC Version Connected?
0     0/0/0           ipv4_io       1.1         Y
4     0/1/0           ipv4_io       1.1         Y
3     0/2/0           ipv4_io       1.1         Y
2     0/4/0           ipv4_io       1.1         Y
1     0/6/0           ipv4_io       1.1         Y
```

This table describes the significant fields shown in the display.

Table 44: show arm registrations producers Command Field Descriptions

Field	Description
Id	An identifier used by the IP Address ARM (IP ARM) to keep track of the producer of the IP address.
Node	The physical node (RP/LC CPU) where the producer is running.
Producer Id	The string used by the producer when registering with IP ARM.

Field	Description
IPC Version	Version of the apis used by the producer to communicate with IP ARM.
Connected?	Status of whether the producer is connected or not.

show arm router-ids

To display the router identification information with virtual routing and forwarding table information for the Address Repository Manager (ARM), use the **show arm router-ids** command in XR EXEC mode.

show arm [**ipv4**] **router-ids**

Syntax Description

ipv4	(Optional) Displays IPv4 router information.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **show arm router-ids** command with the **ipv4** keyword to display the selected router ID information for the router.

Task ID

Task ID	Operations
network	read

Examples

The following is sample output from the **show arm router-ids** command:

```
RP/0/RP0/CPU0:router# show arm router-ids

Router-ID         Interface

10.10.10.10       Loopback0
```

This table describes the significant fields shown in the display.

Table 45: show arm router-ids Command Field Descriptions

Field	Description
Router-ID	Router identification.
Interface	Interface identification.

show arm summary

To display summary information for the IP Address Repository Manager (ARM), use the **show arm summary** command in XR EXEC mode.

show arm {**ipv4** | **ipv6**} **summary**

Syntax Description

ipv4	Displays IPv4 summary information.
ipv6	Displays IPv6 summary information.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **show arm summary** command to display a summary of the number of producers, address conflicts, and unnumbered interface conflicts in the router.

Task ID

Task ID	Operations
network	read

Examples

The following is sample output from the **show arm summary** command:

```
Router# show arm ipv4 summary

IPv4 Producers                          :          1
IPv4 address conflicts                  :          0
IPv4 unnumbered interface conflicts     :          0
IPv4 VRF known                          :          0
IPv4 DB Master version                  : 0x00000000
```

This table describes the significant fields shown in the display.

Table 46: show arm summary Command Field Descriptions

Field	Description
IPv4 Producers	Number of IPv4 producers on the router.
IPv4 address conflicts	Number of IPv4 address conflicts on the router.
IPv4 unnumbered interface conflicts	Number of IPv4 conflicts on unnumbered interfaces.
IPv4 DB Master version	IPv4 DB Master version

show ipv4 interface

To display the usability status of interfaces configured for IPv4, use the **show ipv4 interface** command in the XR EXEC mode.

show ipv4 interface [*type interface-path-id* | **brief** | **summary**]

Syntax Description

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

interface-path-id	Either a physical interface instance or a virtual interface instance as follows:
	• Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation.
	  • *rack*: Chassis number of the rack.
	  • *slot*: Physical slot number of the modular services card or line card.
	  • *module*: Module number. A physical layer interface module (PLIM) is always 0.
	  • *port*: Physical port number of the interface.
	Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RSP0) and the module is CPU0. Example: interface MgmtEth0/RSP0 /CPU0/0.
	• Virtual interface instance. Number range varies depending on interface type.
	For more information about the syntax for the router, use the question mark (?) online help function.

brief	(Optional) Displays the primary IPv4 addresses configured on the router's interfaces and their protocol and line states.
summary	(Optional) Displays the number of interfaces on the router that are assigned, unassigned, or unnumbered.

Command Default

If VRF is not specified, the software displays the default VRF.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **show ipv4 interface** command provides output similar to the **show ipv6 interface** command, except that it is IPv4-specific.

The interface name will be displayed only if the name belongs to the VRF instance. If the *vrf-name* is not specified then the interface instance will be displayed only if the interface belongs to the default VRF.

Task ID

Task ID	Operations
ipv4	read
network	read

Examples

This is the sample output of the **show ipv4 interface** command:

```
RP/0/RP0/CPU0:router# show ipv4 interface

  Loopback0 is Up, line protocol is Up
  Internet address is 10.0.0.1/8

  Secondary address 10.0.0.2/8
  MTU is 1514 (1514 is available to IP)
  Multicast reserved groups joined: 10.0.0.1
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  tenGigE/0/0/0/0 is Up, line protocol is Up
  Internet address is 10.25.58.1/16
  MTU is 1514 (1500 is available to IP)
  Multicast reserved groups joined: 10.0.224.1
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  tenGigE/0/0/0/0 is Shutdown, line protocol is Down
  Vrf is default (vrfid 0x60000000)
  Internet protocol processing disabled
```

This table describes the significant fields shown in the display.

Table 47: show ipv4 interface Command Field Descriptions

Field	Description
Loopback0 is Up	If the interface hardware is usable, the interface is marked “Up.” For an interface to be usable, both the interface hardware and line protocol must be up.
line protocol is Up	If the interface can provide two-way communication, the line protocol is marked “Up.” For an interface to be usable, both the interface hardware and line protocol must be up.
Internet address	IPv4 Internet address and subnet mask of the interface.

Field	Description
Secondary address	Displays a secondary address, if one has been set.
MTU	Displays the IPv4 MTU[8] value set on the interface.
Multicast reserved groups joined	Indicates the multicast groups this interface belongs to.
Directed broadcast forwarding	Indicates whether directed broadcast forwarding is enabled or disabled.
Outgoing access list	Indicates whether the interface has an outgoing access list set.
Inbound access list	Indicates whether the interface has an incoming access list set.
Proxy ARP	Indicates whether proxy ARP[9] is enabled or disabled on an interface.
ICMP redirects	Specifies whether ICMPv4[10] redirects are sent on this interface.
ICMP unreachables	Specifies whether unreachable messages are sent on this interface.
Internet protocol processing disabled	Indicates an IPv4 address has not been configured on the interface.

[8] MTU = maximum transmission unit
[9] ARP = Address Resolution Protocoladdress resolution protocol
[10] ICMPv4 = Internet Control Message Protocol internet control message protocol version 4

show ipv4 traffic

To display the IPv4 traffic statistics, use the **show ipv4 traffic** command in the XR EXEC mode.

show ipv4 traffic [**brief**]

Syntax Description

brief	(Optional) Displays only IPv4 and Internet Control Message Protocol version 4 (ICMPv4) traffic.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **show ipv4 traffic** command provides output similar to the **show ipv6 traffic** command, except that it is IPv4-specific.

Task ID

Task ID	Operations
ipv4	read
network	read

Examples

This is the sample output of the **show ipv4 traffic** command:

```
RP/0/RP0/CPU0:router# show ipv4 traffic

IP statistics:
  Rcvd:  16372 total, 16372 local destination
         0 format errors, 0 bad hop count
         0 unknown protocol, 0 not a gateway
         0 security failures, 0 bad source, 0 bad header
         0 with options, 0 bad, 0 unknown
  Opts:  0 end, 0 nop, 0 basic security, 0 extended security
         0 strict source rt, 0 loose source rt, 0 record rt
         0 stream ID, 0 timestamp, 0 alert, 0 cipso
  Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
         0 fragmented, 0 fragment count
  Bcast: 0 sent, 0 received
  Mcast: 0 sent, 0 received
   Drop: 0 encapsulation failed, 0 no route, 0 too big, 0 sanity address check
   Sent: 16372 total

ICMP statistics:
  Sent: 0 admin unreachable, 0 network unreachable
        0 host unreachable, 0 protocol unreachable
        0 port unreachable, 0 fragment unreachable
        0 time to live exceeded, 0 reassembly ttl exceeded
        5 echo request, 0 echo reply
```

```
        0 mask request, 0 mask reply
        0 parameter error, 0 redirects
        5 total
  Rcvd: 0 admin unreachable, 0 network unreachable
        2 host unreachable, 0 protocol unreachable
        0 port unreachable, 0 fragment unreachable
        0 time to live exceeded, 0 reassembly ttl exceeded
        0 echo request, 5 echo reply
        0 mask request, 0 mask reply
        0 redirect, 0 parameter error
        0 source quench, 0 timestamp, 0 timestamp reply
        0 router advertisement, 0 router solicitation
        7 total, 0 checksum errors, 0 unknown

UDP statistics:
        16365 packets input, 16367 packets output
        0 checksum errors, 0 no port
        0 forwarded broadcasts

TCP statistics:
        0 packets input, 0 packets output
        0 checksum errors, 0 no port
```

This table describes the significant fields shown in the display.

Table 48: show ipv4 traffic Command Field Descriptions

Field	Description
bad hop count	Occurs when a packet is discarded because its TTL[11] field was decremented to zero.
encapsulation failed	Usually indicates that the router had no ARP request entry and therefore did not send a datagram.
format errors	Indicates a gross error in the packet format, such as an impossible Internet header length.
IP statistics Rcvd total	Indicates the total number of local destination and other packets received in the software plane. It does not account for the IP packets forwarded or discarded in hardware.
no route	Counted when the Cisco IOS XR software discards a datagram it did not know how to route.

[11] TTL = time-to-live

show ipv6 interface

To display the usability status of interfaces configured for IPv6, use the **show ipv6 interface** command in the XR EXEC mode.

show ipv6 interface [**summary** | [*type interface-path-id*][**brief** [**link-local** | **global**]]]

Syntax Description

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

interface-path-id	(Optional) Either a physical interface instance or a virtual interface instance as follows:
	• Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation.
	  • *rack*: Chassis number of the rack.
	  • *slot*: Physical slot number of the modular services card or line card.
	  • *module*: Module number. A physical layer interface module (PLIM) is always 0.
	  • *port*: Physical port number of the interface.
	Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RSP0) and the module is CPU0. Example: interface MgmtEth0/RSP0 /CPU0/0.
	• Virtual interface instance. Number range varies depending on interface type.
	For more information about the syntax for the router, use the question mark (?) online help function.

brief	(Optional) Displays the primary IPv6 addresses configured on the router interfaces and their protocol and line states.
link-local	(Optional) Displays the link local IPv6 address.
global	(Optional) Displays the global IPv6 address.
summary	(Optional) Displays the number of interfaces on the router that are assigned, unassigned, or unnumbered.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **show ipv6 interface** command provides output similar to the **show ipv4 interface** command, except that it is IPv6-specific.

Use the **link-local** or **global** keywords along with the **brief** keyword to view the link local or global IPv6 addresses.

Task ID

Task ID	Operations
ipv6	read

Examples

This is the sample output of the **show ipv6 interface** command:

```
RP/0/RP0/CPU0:router# show ipv6 interface

  TenGigE0/0/0/0 is Up, ipv6 protocol is Up, Vrfid is default (0x60000000)
  IPv6 is enabled, link-local address is fe80::c672:95ff:fea6:9324
  Global unicast address(es):
    200::1, subnet is 200::/64
  Joined group address(es): ff02::1:ff00:1 ff02::1:ffa6:9324 ff02::2
      ff02::1
  MTU is 1514 (1500 is available to IPv6)
  ICMP redirects are disabled
  ICMP unreachables are enabled
  ND DAD is enabled, number of DAD attempts 1
  ND reachable time is 0 milliseconds
  ND cache entry limit is 1000000000
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 160 to 240 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
  Outgoing access list is not set
  Inbound  common access list is not set, access list is not set
  Table Id is 0xe0800000
  Complete protocol adjacency: 2
  Complete glean adjacency: 0
  Incomplete protocol adjacency: 0
  Incomplete glean adjacency: 0
  Dropped protocol request: 0
```

This table describes the significant fields shown in the display.

Table 49: show ipv6 interface Command Field Descriptions

Field	Description
tenGigE0/0/0/2 is Up	Indicates whether the interface hardware is currently active (whether line signal is present) and whether it has been taken down by an administrator. If the interface hardware is usable, the interface is marked “Up.” For an interface to be usable, both the interface hardware and line protocol must be up.

Field	Description
line protocol is Up (or down)	Indicates whether the software processes that handle the line protocol consider the line usable (that is, whether keepalives are successful). If the interface can provide two-way communication, the line protocol is marked "Up." For an interface to be usable, both the interface hardware and line protocol must be up.
IPv6 is enabled, stalled, disabled (stalled and disabled are not shown in sample output)	Indicates that IPv6 is enabled, stalled, or disabled on the interface. If IPv6 is enabled, the interface is marked "enabled." If duplicate address detection processing identified the link-local address of the interface as being a duplicate address, the processing of IPv6 packets is disabled on the interface and the interface is marked "stalled." If IPv6 is not enabled, the interface is marked "disabled."
link-local address	Displays the link-local address assigned to the interface.
TENTATIVE	The state of the address in relation to duplicate address detection. States can be any of the following: • duplicate—The address is not unique and is not being used. If the duplicate address is the link-local address of an interface, the processing of IPv6 packets is disabled on that interface. • tentative—Duplicate address detection is either pending or under way on this interface. **Note** If an address does not have one of these states (the state for the address is blank), the address is unique and is being used.
Global unicast addresses	Displays the global unicast addresses assigned to the interface.
ICMP redirects	State of Internet Control Message Protocol (ICMP) IPv6 redirect messages on the interface (the sending of the messages is enabled or disabled).
ND DAD	State of duplicate address detection on the interface (enabled or disabled).
number of DAD attempts	Number of consecutive neighbor solicitation messages that are sent on the interface while duplicate address detection is performed.
ND reachable time	Displays the neighbor discovery reachable time (in milliseconds) assigned to this interface.

This is the sample output of the **show ipv6 interface brief link-local** command:

```
RP/0/RP0/CPU0:router#show ipv6 interface brief link-local

Interface                  IPv6-Address                    Status     Protocol
tenGigE0/0/0/0    fe80::fe:8ff:fecb:26c5        Up         Up
tenGigE0/0/0/1    fe80::4f:88ff:fea0:8c9d       Up         Up
tenGigE0/0/0/3    unassigned                    Shutdown   Down
tenGigE0/0/0/4    unassigned                    Shutdown   Down
```

This is the sample output of the **show ipv6 interface brief global** command:

```
RP/0/#show ipv6 interface brief global

Interface       IPv6-Address                  Status     Protocol
tenGigE0/0/0/0    2001:db8::1                   Up         Up
tenGigE0/0/0/1    2001:db8::2                   Up         Up
tenGigE0/0/0/3    unassigned                    Shutdown   Down
tenGigE0/0/0/4    unassigned                    Shutdown   Down
```

This is the sample output of the **show ipv6 interface** *type interface-path-id* **brief link-local** command:

```
RP/0/RP0/CPU0:router#show ipv6 interface tenGigE 0/0/0/0 brief link-local

Interface                  IPv6-Address                  Status     Protocol
tenGigE0/0/0/0    fe80::fe:8ff:fecb:26c5        Up         Up
```

This is the sample output of the **show ipv6 interface** *type interface-path-id* **brief global** command:

```
RP/0/RP0/CPU0:router#show ipv6 interface tenGigE 0/0/0/0 brief global

Interface                  IPv6-Address                  Status     Protocol
tenGigE0/0/0/0    2001:db8::1                   Up         Up
```

show ipv6 neighbors

To display the IPv6 neighbor discovery cache information, use the **show ipv6 neighbors** command in the XR EXEC mode.

show ipv6 neighbors [*type interface-path-id* | **location** *node-id*]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	(Optional) Physical interface instance or a virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
location *node-id*	(Optional) Designates a node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

All IPv6 neighbor discovery cache information is displayed.

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

When the *interface-type* and *interface-number* arguments are not specified, cache information for all IPv6 neighbors is displayed. Specifying the *interface-type* and *interface-number* arguments displays only cache information about the specified interface.

Task ID

Task ID	Operations
ipv6	read

Examples

This is the sample output of the **show ipv6 neighbors** command when entered with an IPv6 address:

```
RP/0/RP0/CPU0:router# show ipv6 neighbors 2000:0:0:4::2

IPv6 Address                              Age Link-layer Addr State Interface
Location
200::2                                    166  6c9c.ed28.8b74 REACH Te0/0/0/0
0/RP0/CPU0
fe80::6e9c:edff:fe28:8b74                 164  6c9c.ed28.8b74 REACH Te0/0/0/0
0/RP0/CPU0
[Mcast adjacency]                           - 0000.0000.0000 REACH Te0/0/0/0
0/RP0/CPU0
```

```
[Mcast adjacency]                           - 0000.0000.0000 REACH Te0/0/0/4
0/RP0/CPU0
```

This is the sample output of the **show ipv6 neighbors** command when entered with a location:

```
RP/0/RP0/CPU0:router# show ipv6 neighbors  location 0/2/CPU0

IPv6 Address    Age Link-layer Addr State Interface     Location
2001:3::2       119  0013.9400.0002 REACH BE3           0/2/CPU0
2001:3::3       179  0013.9400.0003 DELAY BE3           0/2/CPU0
2001:3::4       166  0013.9400.0004 REACH BE3           0/2/CPU0
2001:3::5       78   0013.9400.0005 REACH BE3           0/2/CPU0
2001:3::6       19   0013.9400.0006 REACH BE3           0/2/CPU0
2001:3::7       173  0013.9400.0007 REACH BE3           0/2/CPU0
2001:3::8       140  0013.9400.0008 REACH BE3           0/2/CPU0
2001:3::9       163  0013.9400.0009 REACH BE3           0/2/CPU0
2001:3::a       40   0013.9400.000a REACH BE3           0/2/CPU0
2001:3::b       90   0013.9400.000b REACH BE3           0/2/CPU0
2001:3::c       35   0013.9400.000c REACH BE3           0/2/CPU0
2001:3::d       114  0013.9400.000d REACH BE3           0/2/CPU0
2001:3::e       117  0013.9400.000e REACH BE3           0/2/CPU0
2001:3::f       157  0013.9400.000f REACH BE3           0/2/CPU0
2001:3::10      9    0013.9400.0010 REACH BE3           0/2/CPU0
2001:3::11      120  0013.9400.0011 REACH BE3           0/2/CPU0
2001:3::12      87   0013.9400.0012 REACH BE3           0/2/CPU0
2001:3::13      180  0013.9400.0013 DELAY BE3           0/2/CPU0
2001:3::14      103  0013.9400.0014 REACH BE3           0/2/CPU0
2001:3::15      132  0013.9400.0015 REACH BE3           0/2/CPU0
2001:3::16      33   0013.9400.0016 REACH BE3           0/2/CPU0
2001:3::17      150  0013.9400.0017 REACH BE3           0/2/CPU0
2001:3::18      117  0013.9400.0018 REACH BE3           0/2/CPU0
2001:3::19      48   0013.9400.0019 REACH BE3           0/2/CPU0
2001:3::1a      67   0013.9400.001a REACH BE3           0/2/CPU0
2001:3::1b      91   0013.9400.001b REACH BE3           0/2/CPU0
2001:3::1c      33   0013.9400.001c REACH BE3           0/2/CPU0
2001:3::1d      174  0013.9400.001d DELAY BE3           0/2/CPU0
2001:3::1e      144  0013.9400.001e REACH BE3           0/2/CPU0
2001:3::1f      121  0013.9400.001f REACH BE3           0/2/CPU0
2001:3::20      53   0013.9400.0020 REACH BE3           0/2/CPU0
```

This table describes significant fields shown in the display.

Table 50: show ipv6 neighbors Command Field Descriptions

Field	Description
IPv6 Address	IPv6 address of neighbor or interface.
Age	Time (in minutes) since the address was confirmed to be reachable. A hyphen (-) indicates a static entry.
Link-layer Addr	MAC address. If the address is unknown, a hyphen (-) is displayed.

Field	Description
State	The state of the neighbor cache entry. These are the states for dynamic entries in the IPv6 neighbor discovery cache: • INCMP (incomplete)—Address resolution is being performed on the entry. A neighbor solicitation message has been sent to the solicited-node multicast address of the target, but the corresponding neighbor advertisement message has not yet been received. • reach (reachable)—Positive confirmation was received within the last ReachableTime milliseconds that the forward path to the neighbor was functioning properly. While in reach state, the device takes no special action as packets are sent. • stale—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. While in stale state, the device takes no action until a packet is sent. • delay—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. A packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the delay state, send a neighbor solicitation message and change the state to probe. • probe—A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer milliseconds until a reachability confirmation is received. These are the possible states for static entries in the IPv6 neighbor discovery cache: • reach (reachable)—The interface for this entry is up. • INCMP (incomplete)—The interface for this entry is down. **Note** Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache; therefore, the descriptions for the INCMP (incomplete) and reach (reachable) states are different for dynamic and static cache entries.
Interface	Interface from which the address is reachable.

show ipv6 neighbors summary

To display summary information for the neighbor entries, use the **show ipv6 neighbors summary** command in the XR EXEC mode.

show ipv6 neighbors summary

Syntax Description

This command has no keywords or arguments.

Command Default

The default value is disabled.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Task ID

Task ID	Operations
ipv6	read

Examples

This is the sample output of the **show ipv6 neighbors summary** command that shows the summary information for the neighbor entries:

```
XR EXEC mode# show ipv6 neighbors summary

Mcast nbr entries:
    Subtotal: 0
Static nbr entries:
    Subtotal: 0
Dynamic nbr entries:
    Subtotal: 0

Total nbr entries: 0
```

show ipv6 path-mtu

To display path maximum transmission unit (MTU) details of IPv6 packets, use the **show ipv6 path-mtu** command in the XR Config mode.

show ipv6 path-mtu [**vrf** { *vrf-name* | **all**} [**location** *node-id*]] [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) The designated node. The node-id argument is entered in the *rack/slot/module* notation.

Command Default

None.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

If the location option is specified, only the details of the node specified in the **location** *node-id* keyword and argument are displayed. Path MTU discovery for IPv6 packets is supported only for applications using TCP and Ping protocol.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

This example shows how to display path MTU details of IPv6 packets:

```
RP/0/RP0/CPU0:router(config)#  show ipv6 pmtu

Destination         Ifhandle        Vrfid              Path Mtu       Time Left
bb::1               0x300           0x60000000         1300           00:01:27
cd::1               0x300           0x60000000         1300           00:01:42
```

show ipv6 traffic

To display the IPv6 traffic statistics, use the **show traffic** command in the XR EXEC mode.

show ipv6 traffic [**brief**]

Syntax Description

brief	(Optional) Displays only IPv6 and Internet Control Message Protocol version 6 (ICMPv6) traffic statistics.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **show ipv6 traffic** command provides output similar to the **show ipv4 traffic** command, except that it is IPv6-specific.

Task ID

Task ID	Operations
ipv6	read
network	read

Examples

This is the sample output of the **show ipv6 traffic** command:

```
RP/0/RP0/CPU0:router# show ipv6 traffic

 IPv6 statistics:
  Rcvd:  0 total, 0 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
         0 reassembly max drop
         0  sanity address check drops
  Sent:  0 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         0 no route, 0 too big
  Mcast: 0 received, 0 sent

ICMP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 too short
        0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor,
                 0 address, 0 port, 0 unknown
```

```
        parameter: 0 error, 0 header, 0 option,
                   0 unknown
        0 hopcount expired, 0 reassembly timeout,
        0 unknown timeout, 0 too big,
        0 echo request, 0 echo reply
  Sent: 0 output, 0 rate-limited
        unreach: 0 routing, 0 admin, 0 neighbor,
                 0 address, 0 port, 0 unknown
        parameter: 0 error, 0 header, 0 option
                 0 unknown
        0 hopcount expired, 0 reassembly timeout,
        0 unknown timeout, 0 too big,
        0 echo request, 0 echo reply

Neighbor Discovery ICMP statistics:
  Rcvd: 0 router solicit, 0 router advert, 0 redirect
        0 neighbor solicit, 0 neighbor advert
  Sent: 0 router solicit, 0 router advert, 0 redirect
        0 neighbor solicit, 0 neighbor advert

UDP statistics:
        0 packets input, 0 checksum errors
        0 length errors, 0 no port, 0 dropped
        0 packets output

TCP statistics:s
        0 packets input, 0 checksum errors, 0 dropped
        0 packets output, 0 retransmitted
```

This table describes the significant fields shown in the display.

Table 51: show ipv6 traffic Command Field Descriptions

Field	Description
Rcvd:	Statistics in this section refer to packets received by the router.
total	Total number of packets received by the software.
local destination	Locally destined packets received by the software.
source-routed	Packets seen by the software with RH.
truncated	Truncated packets seen by the software.
bad header	An error was found in generic HBH, RH, DH, or HA. Software only.
unknown option	Unknown option type in IPv6 header.
unknown protocol	Protocol specified in the IP header of the received packet is unreachable.
Sent:	Statistics in this section refer to packets sent by the router.
forwarded	Packets forwarded by the software. If the packet cannot be forwarded in the first lookup (for example, the packet needs option processing), then the packet is not included in this count, even if it ends up being forwarded by the software.
Mcast:	Multicast packets.

Field	Description
ICMP statistics:	Internet Control Message Protocol statistics.



Prefix List Commands

This chapter describes the Cisco IOS XR software commands used to configure IP Version 4 (IPv4) and IP Version 6 (IPv6) prefix on NCS 5000 routers.

For detailed information about prefix list concepts, configuration tasks, and examples, refer to the *IP Addresses and Services Configuration Guide for Cisco NCS 5000 Series Routers*.

- clear prefix-list ipv4, on page 470
- copy prefix-list ipv4 , on page 472
- deny (prefix-list), on page 474
- ipv4 prefix-list, on page 476
- ipv6 prefix-list, on page 478
- permit (prefix-list), on page 479
- remark (prefix-list), on page 481
- resequence prefix-list ipv4, on page 483
- resequence prefix-list ipv6, on page 485
- show prefix-list afi-all, on page 487
- show prefix-list, on page 488
- show prefix-list ipv4, on page 489
- show prefix-list ipv6, on page 491
- show prefix-list ipv4 standby, on page 493

clear prefix-list ipv4

To reset the hit count on an IP Version 4 (IPv4) prefix list, use the **clear prefix-list ipv4** command in XR EXEC mode.

clear prefix-list ipv4 *name* [*sequence-number*]

Syntax Description

name	Name of the prefix list from which the hit count is to be cleared.
sequence-number	(Optional) Sequence number of a prefix list. Range is 1 to 2147483646.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The hit count is a value indicating the number of matches to a specific prefix list entry. Use the **clear prefix-list ipv4** command to clear counters for a specified configured prefix list.

Use the *sequence-number* argument to clear counters for a prefix list with a specific sequence number.

Task ID

Task ID	Operations
acl	read, write

Examples

The following example displays IPv4 prefix lists, shows how to clear the counters for list3, then shows how to display the IPv4 prefix lists again, showing that counters are cleared for list3:

```
RP/0/RP0/CPU0:router# show prefix-list ipv4

ipv4 prefix-list list1
 10 permit 172.18.30.154/16 (8 matches)
ipv4 prefix-list list2
 20 deny 172.24.30.164/16 (12 matches)
ipv4 prefix-list list3
 30 permit 172.19.31.154/16 (32 matches)

RP/0/RP0/CPU0:router# clear prefix-list ipv4 list3

RP/0/RP0/CPU0:router# show prefix-list ipv4

ipv4 prefix-list list1
 10 permit 172.18.30.154/16 (8 matches)
ipv4 prefix-list list2
 20 deny 172.24.30.164/16 (12 matches)
```

```
ipv4 prefix-list list3
 30 permit 172.19.31.154/16
```

copy prefix-list ipv4

To create a copy of an existing IP Version 4 (IPv4) prefix list, use the **copy prefix-list ipv4** command in XR EXEC mode.

copy prefix-list ipv4 *source-name destination-name*

Syntax Description

source-name	Name of the prefix list to be copied.
destination-name	Destination prefix list where the contents of the *source-name* will be copied.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **copy prefix-list ipv4** command to copy a configured prefix list. Use the *source-name* argument to specify the prefix list to be copied and the *destination-name* argument to specify where to copy the contents of the source prefix list. The *destination-name* argument must be a unique name; if the *destination-name* argument name exists for a prefix list or access list, the prefix list is not copied. The **copy prefix-list ipv4** command checks that the source prefix list exists, then checks the existing list names to prevent overwriting existing prefix lists.

Task ID

Task ID	Operations
acl	read, write
filesystem	execute

Examples

The following example displays IPv4 prefix lists, shows how to copy prefix-list1 to list4, then displays the IPv4 prefix lists again, showing prefix list4:

```
RP/0/RP0/CPU0:router# show prefix-list ipv4

ipv4 prefix-list list1
 10 permit 172.24.20.164/16
ipv4 prefix-list list2
 20 deny 172.18.30.154/16
ipv4 prefix-list list3
 30 permit 172.29.30.154/16

RP/0/RP0/CPU0:router# copy prefix-list ipv4 list1 list4

RP/0/RP0/CPU0:router# show prefix-list ipv4
```

```
ipv4 prefix-list list1
 10 permit 172.24.20.164/16
ipv4 prefix-list list2
 20 deny 172.18.30.154/16
ipv4 prefix-list list3
 30 permit 172.29.30.154/16
ipv4 prefix-list list4
 10 permit 172.24.20.164/16
```

deny (prefix-list)

To set deny conditions for an IP Version 4 (IPv4) prefix list, use the **deny** command in IPv4 prefix list configuration modes. To remove a condition from a prefix list, use the **no** form of this command.

[*sequence-number*] **deny** *network/length* [**ge** *value*] [**le** *value*] [**eq** *value*]
no *sequence-number* **deny**

Syntax Description

sequence-number	(Optional) Sets deny conditions for a prefix list with a specific sequence number. If you do not use a sequence number, the condition defaults to the next available sequence number in the prefix list. Range is 1 to 2147483646. By default, the first statement is number 10, and the subsequent statements are incremented by 10. The **sequence-number** argument must be used with the **no** form of the command.
network / *length*	Network number and length (in bits) of the network mask.
ge *value*	(Optional) Specifies a prefix length greater than or equal to the value. It is the lowest value of a range of the *length* (the "from" portion of the length range).
le *value*	(Optional) Specifies a prefix length less than or equal to the value. It is the highest value of a range of the *length* (the "to" portion of the length range).
eq *value*	(Optional) Exact value of the *length* .

Command Default

There is no specific condition under which a packet is denied passing the IPv4 prefix list.

Command Modes

IPv4 prefix list configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **deny** command to specify conditions under which a packet cannot pass the prefix list.

The **ge**, **le** and **eq** keywords can be used to specify the range of the prefix length to be matched, for prefixes that are more specific than the *network/length* argument. Exact match is assumed when neither **ge** nor **le** is specified. The range is assumed to be from the **ge** *value* to 32 if only the **ge** keyword is specified. The range is assumed to be from the *length* to the **le** *value argument* if only the **le** attribute is specified.

A specified **ge** *value* or **le** *value* must satisfy the following condition:

length < **ge** *value* < **le** *value* <= 32 (for IPv4)

length < **ge** *value* < **le** *value* <= 128 (for IPv6)

Task ID

Task ID	Operations
acl	read, write

Examples

The following example shows how to deny the route 10.0.0.0/0:

```
RP/0/RP0/CPU0:router(config)# ipv4 prefix-list list1
RP/0/RP0/CPU0:router(config-ipv4_pfx)# 50 deny 10.0.0.0/0
```

The following example shows how to deny all routes with a prefix of 10.3.32.154:

```
RP/0/RP0/CPU0:router(config)# ipv4 prefix-list list1
RP/0/RP0/CPU0:router(config-ipv4_pfx)#80 deny 10.3.32.154 le 32
```

The following example shows how to deny all masks with a length greater than 25 bits routes with a prefix of 172.18.30.154/16:

```
RP/0/RP0/CPU0:router(config)# ipv4 prefix-list list1
RP/0/RP0/CPU0:router(config-ipv4_pfx)#100 deny 172.18.30.154/16 ge 25
```

The following example shows how to deny mask lengths greater than 25 bits in all address space:

```
RP/0/RP0/CPU0:router(config)# ipv6 prefix-list list2
RP/0/RP0/CPU0:router(config-ipv6_pfx)# 70 deny  2000:1::/64 ge 25
```

The following example shows how to add deny conditions to list3, then use the **no** form of the command to remove the condition with the sequence number 30:

```
RP/0/RP0/CPU0:router(config)# ipv6 prefix-list list3

RP/0/RP0/CPU0:router(config-ipv6_pfx)# deny 2000:1::/64 ge 25
RP/0/RP0/CPU0:router(config-ipv6_pfx)# deny 3000:1::/64 le 32
RP/0/RP0/CPU0:router(config-ipv6_pfx)# deny 4000:1::/64 ge 25
Uncommitted changes found, commit them? [yes]: y

RP/0/RP0/CPU0:router# show prefix-list ipv6

ipv6 prefix-list list3
 10 deny 2000:1::/64 ge 25
 20 deny 3000:1::/64 le 32
 30 deny 4000:1::/64 ge 25

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipv6 prefix-list list3
RP/0/RP0/CPU0:router(config-ipv6_pfx)# no 30
Uncommitted changes found, commit them? [yes]: y
RP/0/RP0/CPU0:router# show prefix-list ipv6

ipv6 prefix-list list3
 10 deny 2000:1::/64 ge 25
 20 deny 3000:1::/64 le 32
```

ipv4 prefix-list

To define an IP Version (IPv4) prefix list by name, use the **ipv4 prefix-list** command in XR Config mode. To remove the prefix list, use the **no** form of this command.

ipv4 prefix-list *name*
no ipv4 prefix-list *name*

Syntax Description

name	Name of the prefix list. Names cannot contain a space or quotation marks.

Command Default

No IPv4 prefix list is defined.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **ipv4 prefix-list** command to configure an IPv4 prefix list. This command places the router in prefix-list configuration mode, in which the denied or permitted access conditions must be defined with the **deny** or **permit** command. You must add a condition to create the prefix list.

Use the **resequence prefix-list ipv4** command to renumber existing statements and increment subsequent statements to allow a new IPv4 prefix list statement (**permit**, **deny**, or **remark**) to be added. Specify the first entry number (the *base*) and the increment by which to separate the entry numbers of the statements. The software will renumber the existing statements, thereby making room to add new statements with the unused entry numbers.

Task ID

Task ID	Operations
acl	read, write
ipv4	read, write

Examples

The following example shows the prefix lists, then configures list2, then shows the conditions in both prefix lists:

```
RP/0/RP0/CPU0:router# show prefix-list ipv4

ipv4 prefix-list list1
 10 permit 172.20.10.171/16 le 24
 20 permit 172.18.0.0/16
 30 deny 172.24.20.164/16 ge 25

RP/0/RP0/CPU0:router# configure
```

```
RP/0/RP0/CPU0:router(config)# ipv4 prefix-list list2

RP/0/RP0/CPU0:router(config-ipv4_pfx)#deny 172.18.30.154/16 ge 25
RP/0/RP0/CPU0:router(config-ipv4_pfx)#
Uncommitted changes found, commit them? [yes]: Y

RP/0/RP0/CPU0:router# show prefix-list ipv4

ipv4 prefix-list list1
 10 permit 172.20.10.171/16 le 24
 20 permit 172.18.0.0/16
 30 deny 172.24.20.164/16 ge 25
ipv4 prefix-list list2
 10 deny 172.18.30.154/16 ge 25
```

ipv6 prefix-list

To define an IP Version (IPv6) prefix list by name, use the **ipv6 prefix-list** command in XR Config mode. To remove the prefix list, use the **no** form of this command.

ipv6 prefix-list *name*
no ipv6 prefix-list *name*

Syntax Description

name	Name of the prefix list. Names cannot contain a space or quotation marks.

Command Default

No IPv6 prefix list is defined.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
acl	read, write
ipv6	read, write

Examples

The following example shows how to create a prefix list named list-1:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipv6 prefix-list list-1
RP/0/RP0/CPU0:router(config-ipv6-pfx)# 40 permit 2000:1::/64
RP/0/RP0/CPU0:router(config-ipv6-pfx)# 60 deny 3000:1::/64
RP/0/RP0/CPU0:router(config-ipv6-pfx)#
Uncommitted changes found, commit them? [yes]: y

RP/0/RP0/CPU0:router# show prefix-list ipv6

ipv6 prefix-list list1
 40 permit 2000:1::/64
 60 deny 3000:1::/64
RP/0/RP0/CPU0:router#
```

permit (prefix-list)

To set permit conditions for an IP Version 4 (IPv4) prefix list, use the **permit** command in IPv4 prefix list configuration modes. To remove a condition from a prefix list, use the **no** form of this command.

[*sequence-number*] **permit** *network/length* [**ge** *value*] [**le** *value*] [**eq** *value*]
no *sequence-number* **permit**

Syntax Description

sequence-number	(Optional) Number of the **permit** statement in the prefix list. This number determines the order of the statements in the prefix list. Range is 1 to 2147483646. By default, the first statement is number 10, and the subsequent statements are incremented by 10.
network / length	Network number and length (in bits) of the network mask.
ge *value*	(Optional) Specifies a prefix length greater than or equal to the value. It is the lowest value of a range of the *length* (the "from" portion of the length range). Range is 1 to 128.
le *value*	(Optional) Specifies a prefix length less than or equal to the value. It is the highest value of a range of the *length* (the "to" portion of the length range). Range is 1 to 128.
eq *value*	(Optional) Exact value of the *length* . Range is 1 to 128.

Command Default

No default behavior or value

Command Modes

IPv4 prefix list configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **permit** command to specify conditions under which a packet can pass the prefix list.

The **ge**, **le** and **eq** keywords can be used to specify the range of the prefix length to be matched, for prefixes that are more specific than the *network/length* argument. Exact match is assumed when neither **ge** nor **le** is specified. The range is assumed to be from the **ge** *value* to 32 if only the **ge** keyword is specified. The range is assumed to be from the *length* to the **le** *value* argument if only the **le** attribute is specified.

A specified **ge** *value* or **le** *value* must satisfy the following condition:

length < **ge** *value* < **le** *value* <= 32 (for IPv4)

length < **ge** *value* < **le** *value* <= 128 (for IPv6)

Task ID

Task ID	Operations
acl	read, write

Examples

The following example shows how to permit the prefix 172.18.0.0/16:

```
RP/0/RP0/CPU0:router(config)# ipv4 prefix-list list1
RP/0/RP0/CPU0:router(config-ipv4_pfx)# permit 172.18.0.0/16
```

The following example shows how to accept a mask length of up to 24 bits in routes with the prefix 172.20.10.171/16:

```
RP/0/RP0/CPU0:router(config)# ipv4 prefix-list list1
RP/0/RP0/CPU0:router(config-ipv4_pfx)# permit 172.20.10.171/16 le 24
```

The following example shows how to permit mask lengths from 8 to 24 bits in all address space:

```
RP/0/RP0/CPU0:router(config)# ipv6 prefix-list list1
RP/0/RP0/CPU0:router(config-ipv6_pfx)# permit 2000:1::/64 ge 8 le 24
```

The following example shows how to add permit conditions to list3, then remove the condition with the sequence number 30:

```
RP/0/RP0/CPU0:router(config)# ipv6 prefix-list list3
RP/0/RP0/CPU0:router(config-ipv6_pfx)# permit 2000:1::/64 ge 25
RP/0/RP0/CPU0:router(config-ipv6_pfx)# permit 3000:1::/64 le 32
RP/0/RP0/CPU0:router(config-ipv6_pfx)# permit 3000:1::/64 ge 25
Uncommitted changes found, commit them? [yes]: y
RP/0/RP0/CPU0:router#show ipv6 prefix-list

ipv6 prefix-list list3
 10 permit 2000:1::/64 ge 25
 20 permit 3000:1::/64 le 32
 30 permit 4000:1::/64 ge 25

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipv6 prefix-list list3
RP/0/RP0/CPU0:router(config-ipv6_pfx)# no 30
Uncommitted changes found, commit them? [yes]: y
RP/0/RP0/CPU0:router# show prefix-list ipv6

ipv6 prefix-list list3
 10 permit 2000:1::/64 ge 25
 20 permit 3000:1::/64 le 32

10 deny 2000:1::/64 ge 25
 20 deny 3000:1::/64 le 32
 30 deny 4000:1::/64 ge 25
```

remark (prefix-list)

To write a helpful comment (remark) for an entry in either an IP Version 4 (IPv4) prefix list, use the **remark** command in IPv4 prefix-list configuration mode. To remove the remark, use the **no** form of this command.

[*sequence-number*] **remark** *remark*
no *sequence-number*

Syntax Description

sequence-number	(Optional) Number of the **remark** statement in the prefix list. This number determines the order of the statements in the prefix list. The number can be from 1 to 2147483646. (By default, the first statement is number 10, and the subsequent statements are incremented by 10).
remark	Comment that describes the entry in the prefix list, up to 255 characters long.

Command Default

The prefix list entries have no remarks.

Command Modes

IPv4 prefix-list configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **remark** command to write a helpful comment for an entry in a prefix list. The remark can be up to 255 characters in length; anything longer is truncated.

If you know the sequence number of the remark you want to delete, you can remove it by entering the **no** *sequence-number* command.

Use the **resequence prefix-list ipv4** command if you want to add statements to an existing IPv4 prefix list.

Task ID

Task ID	Operations
acl	read, write

Examples

In the following example, a remark is made to explain a prefix list entry:

```
RP/0/RP0/CPU0:router(config)# ipv4 prefix-list deny-ten
RP/0/RP0/CPU0:router(config-ipv4_pfx)# 10 remark Deny all routes with a prefix of 10/8
RP/0/RP0/CPU0:router(config-ipv4_pfx)# 20 deny 10.0.0.0/8 le 32
RP/0/RP0/CPU0:router(config-ipv4_pfx)# end
```

In the following example, a remark is made to explain usage:

```
RP/0/RP0/CPU0:router# show prefix-list ipv6
```

```
ipv6 prefix-list list1
 40 permit 2000:1::/64
 60 deny 3000:1::/64

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipv6 prefix-list list1
RP/0/RP0/CPU0:router(config-ipv6-pfx)# 10 remark use from july23 forward
RP/0/RP0/CPU0:router(config-ipv6-pfx)#
Uncommitted changes found, commit them? [yes]: y

RP/0/0/CPU0:Apr  4 02:20:34.851 : config[65700]: %LIBTARCFG-6-COMMIT : Configura
tion committed by user 'UNKNOWN'.   Use 'show commit changes 1000000023' to view
 the changes.
RP/0/0/CPU0:Apr  4 02:20:34.984 : config[65700]: %SYS-5-CONFIG_I : Configured fr
om console by console
RP/0/RP0/CPU0:router# show prefix-list ipv6

ipv6 prefix-list list1
 10 remark use from july23 forward
 40 permit 2000:1::/64
 60 deny 3000:1::/64
```

resequence prefix-list ipv4

To renumber existing statements and increment subsequent statements to allow a new prefix list statement (**permit**, **deny**, or **remark**) to be added, use the **resequence prefix-list ipv4** command in System Admin Config mode XR Config mode.

resequence prefix-list ipv4 *name* [*base* [*increment*]]

Syntax Description

name	Name of a prefix list.
base	(Optional) Number of the first statement in the specified prefix list, which determines its order in the prefix list. Maximum value is 2147483646.
increment	(Optional) Number by which the base sequence number is incremented for subsequent statements. Maximum value is 2147483646.

Command Default

base: 10

increment: 10

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The sequence number of a prefix list entry determines the order of the entries in the list. The router compares network addresses to the prefix list entries. The router begins the comparison at the top of the prefix list, with the entry having the lowest sequence number.

If multiple entries of a prefix list match a prefix, the entry with the lowest sequence number is considered the real match. When a match or deny occurs, the router does not go through the rest of the prefix list.

By default, the first statement in a prefix list is sequence number 10, and the subsequent statements are incremented by 10.

Use the **resequence prefix-list ipv4** command to add a **permit**, **deny**, or **remark** statement between consecutive entries in an existing IPv4 prefix list. Specify the first entry number (the *base*) and the increment by which to separate the entry numbers of the statements. The software renumbers the existing statements, thereby making room to add new statements with the unused entry numbers.

Task ID

Task ID	Operations
acl	read, write

Examples

The following example shows how to display the sequence number intervals for prefix list list1, resequence list1 from 10 to 30, and displays the resulting sequence numbers:

```
RP/0/RP0/CPU0:router# show prefix-list ipv4

ipv4 prefix-list list1
 10 permit 172.20.10.171/16 le 24
 20 permit 172.18.0.0/16
 30 deny 172.24.20.164/16 ge 25
ipv4 prefix-list list2
 10 deny 172.18.30.154/16 ge 25


RP/0/RP0/CPU0:router# resequence prefix-list ipv4 list1 10 30

RP/0/0/CPU0:Apr  4 02:29:39.513 : ipv4_acl_action_edm[183]: %LIBTARCFG-6-COMMIT
: Configuration committed by user 'UNKNOWN'.   Use 'show commit changes 10000000
24' to view the changes.

RP/0/RP0/CPU0:router#  resequence prefix-list ipv4 ldp_filter 30 10

RP/0/RP0/CPU0:router# show prefix-list ipv4

ipv4 prefix-list list1
 10 permit 172.20.10.171/16 le 24
 40 permit 172.18.0.0/16
 70 deny 172.24.20.164/16 ge 25
ipv4 prefix-list list2
 10 deny 172.18.30.154/16 ge 25
```

resequence prefix-list ipv6

To renumber existing statements and increment subsequent statements to allow a new prefix list statement (**permit**, **deny**, or **remark**) to be added, use the **resequence prefix-list ipv6** command in XR EXEC mode.

resequence prefix-list ipv6 *name* [*base* [*increment*]]

Syntax Description

name	Name of a prefix list.
base	(Optional) Number of the first statement in the specified prefix list, which determines its order in the prefix list. Maximum value is 2147483644.
increment	(Optional) Number by which the base sequence number is incremented for subsequent statements. Maximum value is 2147483644.

Command Default

base: 10

increment: 10

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

The sequence number of a prefix list entry determines the order of the entries in the list. The router compares network addresses to the prefix list entries. The router begins the comparison at the top of the prefix list, with the entry having the lowest sequence number.

If multiple entries of a prefix list match a prefix, the entry with the lowest sequence number is considered the real match. Once a match or deny occurs, the router does not go through the rest of the prefix list.

By default, the first statement in a prefix list is sequence number 10, and the subsequent statements are incremented by 10.

Use the **resequence prefix-list ipv6** command to add a **permit**, **deny**, or **remark** statement between consecutive entries in an existing IPv6 prefix list. Specify the first entry number (the *base*) and the increment by which to separate the entry numbers of the statements. The software renumbers the existing statements, thereby making room to add new statements with the unused entry numbers.

Task ID

Task ID	Operations
acl	read, write

Examples

The following example shows how to display the sequence number intervals for prefix list 1, resequence list1 from 10 to 30, and displays the resulting sequence numbers:

```
RP/0/RP0/CPU0:router# show prefix-list ipv6
ipv6 prefix-list list1
 10 permit 2000:1::
/16 le 24
 20 permit 3000:1::/16 le 32
 20 permit 172.18.0.0/16
 30 deny 3000:1::
/16 ge 25
ipv6
prefix-list list2
 10 deny 4000:1::
/16 ge 25

RP/0/RP0/CPU0:router# resequence prefix-list ipv4 list1 10 30

RP/0//CPU0:
Apr  4 02:29:39.513 : ipv6_acl_action_edm
[183]: %LIBTARCFG-6-COMMIT
: Configuration committed by user 'UNKNOWN'.   Use 'show commit changes 10000000
24' to view the changes.
```

show prefix-list afi-all

To display the contents of the prefix list for all the address families, use the **show prefix-list afi-all** command in XR EXEC mode.

show prefix-list afi-all

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
acl	read

Examples

The following sample output is from the **show prefix-list afi-all** command:

```
RP/0/RP0/CPU0:router# show prefix-list afi-all

ipv4 prefix-list ldp_filter
 10 permit 120.0.0.0/8 ge 8 le 32 (2000 matches)
 30 permit 130.3.0.0/24 ge 8 le 32
```

show prefix-list

To display information about a prefix list or prefix list entries, use the **show prefix-list** command in XR EXEC mode.

show prefix-list [*list-name*] [*sequence-number*]

Syntax Description

list-name	(Optional) Name of a prefix list.
sequence-number	(Optional) Sequence number of the prefix list entry. Range is 1 to 2147483646.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
acl	read

Examples

The following sample output is from the **show prefix-list** command:

```
RP/0/RP0/CPU0:router#  show prefix-list ipv4 summary

Prefix List Summary:
  Total Prefix Lists configured:         0
  Total Prefix List entries configured : 0
```

show prefix-list ipv4

To display the contents of current IP Version 4 (IPv4) prefix list, use the **show prefix-list ipv4** command in XR EXEC mode.

show prefix-list ipv4 [*list-name*] [*sequence-number*] [**summary**]

Syntax Description

list-name	(Optional) Name of a prefix list.
sequence-number	(Optional) Sequence number of the prefix list entry. Range is 1 to 2147483646.
summary	(Optional) Displays summary output of prefix list contents.

Command Default

All IPv4 prefix lists are displayed.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **show prefix-list ipv4** command to display the contents of all IPv4 prefix lists. To display the contents of a specific IPv4 prefix list, use the *name* argument. Use the *sequence-number* argument to specify a given prefix list entry. Use the **summary** keyword to display a summary of prefix list contents.

Task ID

Task ID	Operations
acl	read

Examples

The following example displays all configured prefix lists:

```
RP/0/RP0/CPU0:router# show prefix-list ipv4

ipv4 prefix-list list1
 10 permit 172.20.10.171/16 le 24
 20 permit 172.18.0.0/16
 30 deny 172.24.20.164/16 ge 25
ipv4 prefix-list list2
 10 deny 172.18.30.154/16 ge 25
```

The following example uses the *list-name* argument to display the prefix list named list1:

```
RP/0/RP0/CPU0:router# show prefix-list ipv4 list1

ipv4 prefix-list list1
 10 permit 172.20.10.171/16 le 24
```

```
 20 permit 172.18.0.0/16
 30 deny 172.24.20.164/16 ge 25
```

The following example uses the *list-name* and *sequence-number* argument to display a prefix list named list1 with a sequence number of 10:

```
RP/0/RP0/CPU0:router# show prefix-list ipv4 list1 30

ipv4 prefix-list list1
 30 deny 172.24.20.164/16 ge 25
```

show prefix-list ipv6

To display the contents of the current IP Version 6 (IPv6) prefix list, use the **show prefix-list ipv6** command in XR EXEC mode.

show prefix-list ipv6 [**summary**][*list-name*] [*sequence-number*] [**summary**]

Syntax Description

list-name	(Optional) Name of a prefix list.
sequence-number	(Optional) Sequence number of the prefix list entry. Range is 1 to 2147483646.
summary	(Optional) Displays summary output of prefix list contents.

Command Default

All IPv6 prefix lists are displayed.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

Use the **show prefix-list ipv6** command to display the contents of all IPv4 prefix lists.

To display the contents of a specific IPv6 prefix list, use the *name* argument. Use the *sequence-number* argument to specify a given prefix list entry. Use the **summary** keyword to display a summary of prefix list contents.

Task ID

Task ID	Operations
acl	read

Examples

The following example shows how to display all configured prefix lists:

```
RP/0/RP0/CPU0:router# show prefix-list ipv6

ipv6 prefix-list list1
 10 permit 5555::/24
 20 deny 3000::/24
 30 permit 2000::/24
ipv6 prefix-list list2
 10 permit 2000::/24
```

The following example uses the *list-name* argument to display the prefix list named list1:

```
RP/0/RP0/CPU0:router# show prefix-list ipv6 list1

ipv6 prefix-list list1
```

```
 10 permit 5555::/24
 20 deny 3000::/24
 30 permit 2000::/24
```

The following example uses the *list-name* and *sequence-number* argument to display a prefix list named list1 with a sequence number of 10:

```
RP/0/RP0/CPU0:router# show prefix-list ipv6 list1 10

ipv6 prefix-list abc
 10 permit 5555::/24
```

The following example displays a summary of prefix list contents:

```
RP/0/RP0/CPU0:router# show prefix-list ipv6 summary

Prefix List Summary:
  Total Prefix Lists configured:        2
  Total Prefix List entries configured: 2
```

show prefix-list ipv4 standby

To display the contents of current IPv4 standby access lists, use the **show access-lists ipv4 standby** command in XR EXEC mode.

show prefix-list ipv4 standby [*prefix-list name*] [**summary**]

Syntax Description

prefix-list name	(Optional) Name of a particular IPv4 prefix list. The value of the prefix-list-name argument is a string of alphanumeric characters that cannot include spaces or quotation marks.
summary	(Optional) Displays a summary of all current IPv4 standby prefix lists.

Command Default

No default behavior or values

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **show prefix-list ipv4 standby** command to display the contents of current IPv4 standby prefix lists. To display the contents of a specific IPv4 prefix list, use the *name* argument.

Use the **show prefix-list ipv4 standby summary** command to display a summary of all standby IPv4 prefix lists.

Task ID

Task ID	Operations
acl	read

Examples

In the following example, the contents of all IPv4 access lists are displayed:

```
RP/0/RP0/CPU0:router# show prefix-list ipv4 standby summary
Prefix List Summary:
  Total Prefix Lists configured:         2
  Total Prefix List entries configured : 6
```



Transport Stack Commands

This chapter describes the Cisco IOS XR softwarecommands used to configure and monitor features related to the transport stack (Nonstop Routing, Stream Control Transmission Protocol (SCTP), NSR, TCP, User Datagram Protocol (UDP), and RAW. Any IP protocol other than TCP or UDP is known as a *RAW* protocol.

For detailed information about transport stack concepts, configuration tasks, and examples, refer to the *IP Addresses and Services Configuration Guide for Cisco NCS 5000 Series Routers*.

- clear raw statistics pcb, on page 496
- clear tcp pcb, on page 498
- clear tcp statistics, on page 499
- clear udp statistics, on page 500
- forward-protocol udp, on page 501
- service tcp-small-servers, on page 503
- service udp-small-servers, on page 504
- show raw brief, on page 505
- show raw detail pcb, on page 507
- show raw extended-filters, on page 509
- show raw statistics pcb, on page 511
- show tcp brief, on page 513
- show tcp detail, on page 515
- show tcp extended-filters, on page 516
- show tcp statistics, on page 518
- show udp brief, on page 520
- show udp detail pcb, on page 522
- show udp extended-filters, on page 524
- show udp statistics, on page 525
- tcp mss, on page 527
- tcp path-mtu-discovery, on page 528
- tcp selective-ack, on page 529
- tcp synwait-time, on page 530
- tcp timestamp, on page 531
- tcp window-size, on page 532

clear raw statistics pcb

To clear statistics for a single RAW connection or for all RAW connections, use the **clear raw statistics pcb** command in XR EXEC mode.

clear raw statistics pcb {**all***pcb-address*} [**location***node-id*]

Syntax Description

all	Clears statistics for all RAW connections.
pcb-address	Clears statistics for a specific RAW connection.
location *node-id*	(Optional) Clears statistics for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **all** keyword to clear all RAW connections. To clear a specific RAW connection, enter the protocol control block (PCB) address of the RAW connection. **Use the show raw brief** command to obtain the PCB address.

Use the **location** keyword and *node-id* argument to clear RAW statistics for a designated node.

Task ID

Task ID	Operations
transport	execute

Examples

The following example shows how to clear statistics for a RAW connection with PCB address 0x80553b0:

```
RP/0/RP0/CPU0:router# clear raw statistics pcb 0x80553b0
RP/0/RP0/CPU0:router# show raw statistics pcb 0x80553b0

Statistics for PCB 0x80553b0
Send: 0 packets received from application
0 xipc pulse received from application
0 packets sent to network
0 packets failed getting queued to network
Rcvd: 0 packets received from network
0 packets queued to application
0 packets failed queued to application
```

The following example shows how to clear statistics for all RAW connections:

```
RP/0/RP0/CPU0:router# clear raw statistics pcb all
RP/0/RP0/CPU0:router# show raw statistics pcb all

Statistics for PCB 0x805484c
Send: 0 packets received from application
0 xipc pulse received from application
0 packets sent to network
0 packets failed getting queued to network
Rcvd: 0 packets received from network
0 packets queued to application
0 packets failed queued to application

Statistics for PCB 0x8054f80
Send: 0 packets received from application
0 xipc pulse received from application
0 packets sent to network
0 packets failed getting queued to network
Rcvd: 0 packets received from network
0 packets queued to application
0 packets failed queued to application

Statistics for PCB 0x80553b0
Send: 0 packets received from application
0 xipc pulse received from application
0 packets sent to network
0 packets failed getting queued to network
Rcvd: 0 packets received from network
0 packets queued to application
0 packets failed queued to application
```

clear tcp pcb

To clear TCP protocol control block (PCB) connections, use the **clear tcp pcb** command in XR EXEC mode.

clear tcp pcb {*pcb-address* | **all**} [**location** *node-id*]

Syntax Description

pcb-address	Clears the TCP connection at the specified PCB address.
all	Clears all open TCP connections.
location *node-id*	(Optional) Clears the TCP connection for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **clear tcp pcb** command is useful for clearing hung TCP connections. Use the show tcp brief, on page 513 command to find the PCB address of the connection you want to clear.

If the **clear tcp pcb all** command is used, the software does not clear a TCP connection that is in the listen state. If a specific PCB address is specified, then a connection in listen state is cleared.

Task ID

Task ID	Operations
transport	execute

Examples

The following example shows that the TCP connection at PCB address 60B75E48 is cleared:

```
RP/0/RP0/CPU0:router# clear tcp pcb 60B75E48
```

clear tcp statistics

To clear TCP statistics, use the **clear tcp statistics** command in

XR EXEC mode.

clear tcp statistics {**pcb** {**all** *pcb-address*} | **summary**} [**location** *node-id*]

Syntax Description

pcb all	(Optional) Clears statistics for all TCP connections.
pcb *pcb-address*	(Optional) Clears statistics for a specific TCP connection.
summary	(Optional) Clears summary statistic for a specific node or connection.
location *node-id*	(Optional) Clears TCP statistics for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **clear tcp statistics** command to clear TCP statistics. Use the show tcp statistics, on page 518 command to display TCP statistics. You might display TCP statistics and then clear them before you start debugging TCP.

The optional **location** keyword and *node-id* argument can be used to clear TCP statistics for a designated node.

Task ID

Task ID	Operations
transport	execute

Examples

The following example shows how to clear TCP statistics:

RP/0/RP0/CPU0:router

```
# clear tcp statistics
```

clear udp statistics

To clear User Datagram Protocol (UDP) statistics, use the **clear udp statistics** command in XR EXEC mode.

clear udp statistics {**pcb** {**all** *pcb-address*} | **summary**} [**location** *node-id*]

Syntax Description

pcb all	Clears statistics for all UDP connections.
pcb *pcb-address*	Clears statistics for a specific UDP connection.
summary	Clears UDP summary statistics.
location *node-id*	(Optional) Clears UDP statistics for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **clear udp statistics** command to clear UDP statistics. Use the show udp statistics, on page 525 command to display UDP statistics. You might display UDP statistics and then clear them before you start debugging UDP.

The optional **location** keyword and *node-id* argument can be used to clear UDP statistics for a designated node.

Task ID

Task ID	Operations
transport	execute

Examples

The following example shows how to clear UDP summary statistics:

```
RP/0/RP0/CPU0:router
# clear udp statistics summary
```

forward-protocol udp

To configure the system to forward any User Datagram Protocol (UDP) datagrams that are received as broadcast packets to a specified helper address, use the **forward-protocol udp** command in

XR Config mode.

To restore the system to its default condition with respect to this command, use the **no** form of this command.

forward-protocol udp {*port-number* | **disable** | **domain** | **nameserver** | **netbios-dgm** | **netbios-ns** | **tacacs** | **tftp**}
no forward-protocol udp {*port-number* | **disable** | **domain** | **nameserver** | **netbios-dgm** | **netbios-ns** | **tacacs** | **tftp**}

Syntax Description

port-number	Forwards UDP broadcast packets to a specified port number. Range is 1 to 65535.
disable	Disables IP Forward Protocol UDP.
domain	Forwards UDP broadcast packets to Domain Name Service (DNS, 53).
nameserver	Forwards UDP broadcast packets to IEN116 name service (obsolete, 42).
netbios-dgm	Forwards UDP broadcast packets to NetBIOS datagram service (138).
netbios-ns	Forwards UDP broadcast packets to NetBIOS name service (137).
tacacs	Forwards UDP broadcast packets to TACACS (49).
tftp	Forwards UDP broadcast packets to TFTP (69).

Command Default

forward-protocol udp is enabled.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **forward-protocol udp** command to specify that UDP broadcast packets received on the incoming interface are forwarded to a specified helper address.

When you configure the **forward-protocol udp** command, you must also configure the **helper-address** command to specify a helper address on an interface. The helper address is the IP address to which the UDP datagram is forwarded. Configure the **helper-address** command with IP addresses of hosts or networking devices that can handle the service. Because the helper address is configured per interface, you must configure a helper address for each incoming interface that will be receiving broadcasts that you want to forward.

You must configure one **forward-protocol udp** command per UDP port you want to forward. The port on the packet is either port 53 (**domain**), port 69 (**tftp**), or a port number you specify.

Task ID

Task ID	Operations
transport	read, write

Examples

The following example shows how to specify that all UDP broadcast packets with port 53 or port 69 received on incoming tenGigE interface 0/RP0/CPU0 are forwarded to 172.16.0.1. tenGigE interface 0/RP0/CPU0 receiving the UDP broadcasts is configured with a helper address of 172.16.0.1, the destination address to which the UDP datagrams are forwarded.

```
RP/0/RP0/CPU0:router(config)# forward-protocol udp domain disable
RP/0/RP0/CPU0:router(config)# forward-protocol udp tftp disable
RP/0/RP0/CPU0:router(config)# interface tenGigE 0/RP0/CPU0
RP/0/RP0/CPU0:router(config-if)# ipv4 helper-address 172.16.0.1
```

service tcp-small-servers

To enable small TCP servers such as the ECHO, use the **service tcp-small-servers** command in XR Config mode. To disable the TCP server, use the **no** form of this command.

service {**ipv4** | **ipv6**} **tcp-small-servers** [**max-servers** *number* | **no-limit**] [*access-list-name*]
no service {**ipv4** | **ipv6**} **tcp-small-servers** [**max-servers** *number* | **no-limit**] [*access-list-name*]

Syntax Description

ip4	Specifies IPv4 small servers.
ipv6	Specifies IPv6 small servers.
max-servers	(Optional) Sets the number of allowable TCP small servers.
number	(Optional) Number value. Range is 1 to 2147483647.
no-limit	(Optional) Sets no limit to the number of allowable TCP small servers.
access-list-name	(Optional) The name of an access list.

Command Default

TCP small servers are disabled.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The TCP small servers currently consist of three services: Discard (port 9), Echo (port 7), and Chargen (port 19). These services are used to test the TCP transport functionality. The Discard server receives data and discards it. The Echo server receives data and echoes the same data to the sending host. The Chargen server generates a sequence of data and sends it to the remote host.

Task ID

Task ID	Operations
ipv4	read, write
ip-services	read, write

Examples

In the following example, small IPv4 TCP servers are enabled:

```
RP/0/RP0/CPU0:router(config)# service ipv4 tcp-small-servers max-servers 5 acl100
```

service udp-small-servers

To enable small User Datagram Protocol (UDP) servers such as the ECHO, use the **service udp-small-servers** command in XR Config mode. To disable the UDP server, use the **no** form of this command.

service {**ipv4** | **ipv6**} **udp-small-servers** [**max-servers** *number* | **no-limit**] [*access-list-name*]
no service {**ipv4** | **ipv6**} **udp-small-servers** [**max-servers** *number* | **no-limit**] [*access-list-name*]

Syntax Description

ip4	Specifies IPv4 small servers.
ipv6	Specifies IPv6 small servers.
max-servers	(Optional) Sets the number of allowable UDP small servers.
number	(Optional) Number value. Range is 1 to 2147483647.
no-limit	(Optional) Sets no limit to the number of allowable UDP small servers.
access-list-name	(Optional) Name of an access list.

Command Default

UDP small servers are disabled.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The UDP small servers currently consist of three services: Discard (port 9), Echo (port 7), and Chargen (port 19). These services are used to test the UDP transport functionality. The discard server receives data and discards it. The echo server receives data and echoes the same data to the sending host. The chargen server generates a sequence of data and sends it to the remote host.

Task ID

Task ID	Operations
ipv6	read, write
ip-services	read, write

Examples

The following example shows how to enable small IPv6 UDP servers and set the maximum number of allowable small servers to 10:

```
RP/0/RP0/CPU0:router(config)# service ipv6 udp-small-servers max-servers 10
```

show raw brief

To display information about active RAW IP sockets, use the **show raw brief** command in XR EXEC mode.

show raw brief [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Displays information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Protocols such as Open Shortest Path First (OSPF) and Protocol Independent Multicast (PIM) use long-lived RAW IP sockets. The **ping** and **traceroute** commands use short-lived RAW IP sockets. Use the **show raw brief** command if you suspect a problem with one of these protocols.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show raw brief** command:

```
RP/0/RP0/CPU0:router# show raw brief

PCB      Recv-Q Send-Q Local Address          Foreign Address Protocol
0x805188c        0      0 0.0.0.0               0.0.0.0            2
0x8051dc8        0      0 0.0.0.0               0.0.0.0          103
0x8052250        0      0 0.0.0.0               0.0.0.0          255
```

This table describes the significant fields shown in the display.

Table 52: show raw brief Command Field Descriptions

Field	Description
PCB	Protocol control block address. This is the address to a structure that contains connection information such as local address, foreign address, local port, foreign port, and so on.
Recv-Q	Number of bytes in the receive queue.
Send-Q	Number of bytes in the send queue.
Local Address	Local address and local port.

Field	Description
Foreign Address	Foreign address and foreign port.
Protocol	Protocol that is using the RAW IP socket. For example, the number 2 is IGMP, 103 is PIM, and 89 is OSPF.

show raw detail pcb

To display detailed information about active RAW IP sockets, use the **show raw detail pcb** command in XR EXEC mode.

show raw detail pcb {*pcb-address* | **all**} **location** *node-id*

Syntax Description

pcb-address	Displays statistics for a specified RAW connection.
all	Displays statistics for all RAW connections.
location *node-id*	Displays information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **show raw detail pcb** command displays detailed information for all connections that use the RAW transport. Information that is displayed includes family type (for example, 2 for AF_INET also known as IPv4), PCB address, Layer 4 (also known as transport) protocol, local address, foreign address, and any filter that is being used.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show raw detail pcb** command:

```
RP/0/RP0/CPU0:router# show raw detail pcb 0x807e89c

============================================================
PCB is 0x807e89c, Family: 2, PROTO: 89
 Local host: 0.0.0.0
 Foreign host: 0.0.0.0

Current send queue size: 0
Current receive queue size: 0
Paw socket: Yes
```

This table describes the significant fields shown in the display.

Table 53: show raw detail pcb Command Field Descriptions

Field	Description
JID	Job ID of the process that created the socket.
Family	Network protocol. IPv4 is 2; IPv6 is 26.
PCB	Protocol control block address.
L4-proto	Layer 4 (also known as transport) protocol.
Laddr	Local address.
Faddr	Foreign address.
ICMP error filter mask	If an ICMP filter is being set, output in this field has a nonzero value.
LPTS socket options	If an LPTS option is being set, output in this field has a nonzero value.
Packet Type Filters	Packet filters that are being set for a particular RAW socket, including the number of packets for that filter type. Multiple filters can be set.

show raw extended-filters

To display information about active RAW IP sockets, use the **show raw extended-filters** command in XR EXEC mode.

show raw extended-filters {**interface-filter location** *node-id* | **location** *node-id* | **paktype-filter location** *node-id*}

Syntax Description

interface-filter	Displays the protocol control blocks (PCBs) with configured interface filters.
location *node-id*	Displays information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
paktype-filter	Displays the PCBs with configured packet type filters.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **show raw extended-filters** command displays detailed information for all connections that use the RAW transport. Information that is displayed includes family type (for example, 2 for AF_INET also known as IPv4), PCB address, Layer 4 (also known as transport) protocol, local address, foreign address, and any filter that is being used.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show raw extended-filters** command:

```
RP/0/RP0/CPU0:router# show raw extended-filters 0/RP0/CPU0

Total Number of matching PCB's in database: 1
JID: 0/0
Family: 2
PCB: 0x0803dd38
L4-proto: 1
Laddr: 0.0.0.0
Faddr: 0.0.0.0
ICMP error filter mask: 0x3ff
LPTS socket options: 0x0020
Packet Type Filters:
0
[220 pkts in]
3
[0 pkts in]
```

```
4
[0 pkts in]
```

This table describes the significant fields shown in the display.

Table 54: show raw extended-filters Output Command Field Descriptions

Field	Description
JID	Job ID of the process that created the socket.
Family	Network protocol. IPv4 is 2; IPv6 is 26.
PCB	Protocol control block address.
L4-proto	Layer 4 (also known as transport) protocol.
Laddr	Local address.
Faddr	Foreign address.
ICMP error filter mask	If an ICMP filter is being set, output in this field has a nonzero value.
LPTS socket options	If an LPTS option is being set, output in this field has a nonzero value.
Packet Type Filters	Packet filters that are being set for a particular RAW socket, including the number of packets for that filter type. Multiple filters can be set.

show raw statistics pcb

To display statistics for a single RAW connection or for all RAW connections, use the **show raw statistics pcb** command in XR EXEC mode.

show raw statistics pcb {**all** | **pcb-address**} **location** *node-id*

Syntax Description

all	Displays statistics for all RAW connections.
pcb-address	Displays statistics for a specified RAW connection.
location *node-id*	(Optional) Displays RAW statistics for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **all** keyword to display all RAW connections. If a specific RAW connection is desired, then enter the protocol control block (PCB) address of that RAW connection. Use the **show raw brief** command to obtain the PCB address.

Use the **location** keyword and *node-id* argument to display RAW statistics for a designated node.

Task ID

Task ID	Operations
transport	read

Examples

In the following example, statistics for a RAW connection with PCB address 0x80553b0 are displayed:

```
RP/0/RP0/CPU0:router# show raw statistics pcb 0x80553b0

Statistics for PCB 0x80553b0
Send: 0 packets received from application
0 xipc pulse received from application
0 packets sent to network
0 packets failed getting queued to network
Rcvd: 0 packets received from network
0 packets queued to application
0 packets failed queued to application
```

In this example, statistics for all RAW connections are displayed:

```
RP/0/RP0/CPU0:router# show raw statistics pcb all
```

```
Statistics for PCB 0x805484c
Send: 0 packets received from application
0 xipc pulse received from application
0 packets sent to network
0 packets failed getting queued to network
Rcvd: 0 packets received from network
0 packets queued to application
0 packets failed queued to application
```

This table describes the significant fields shown in the display.

Table 55: show raw statistics pcb Command Field Descriptions

Field	Description
Send:	Statistics in this section refer to packets sent from an application to RAW.
Vrfid	VPN routing and forwarding (VRF) identification (vrfid) number.
xipc pulse received from application	Number of notifications sent from applications to RAW.
packets sent to network	Number of packets sent to the network.
packets failed getting queued to network	Number of packets that failed to get queued to the network.
Rcvd:	Statistics in this section refer to packets received from the network.
packets queued to application	Number of packets queued to an application.
packets failed queued to application	Number of packets that failed to get queued to an application.

show tcp brief

To display a summary of the TCP connection table, use the **show tcp brief** command in XR EXEC mode.

show tcp brief [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Displays information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Release 6.0

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show tcp brief** command:

```
RP/0/RP0/CPU0:router# show tcp brief

TCPCB     Recv-Q Send-Q  Local Address          Foreign Address        State
0x80572a8      0      0  0.0.0.0:513            0.0.0.0:0              LISTEN
0x8056948      0      0  0.0.0.0:23             0.0.0.0:0              LISTEN
0x8057b60      0      3  10.8.8.2:23            10.8.8.1:1025          ESTAB
```

This table describes the significant fields shown in the display.

Table 56: show tcp brief Command Field Descriptions

Field	Description
TCPCB	Memory address of the TCP control block.
Recv-Q	Number of bytes waiting to be read.
Send-Q	Number of bytes waiting to be sent.
Local Address	Source address and port number of the packet.

Field	Description
Foreign Address	Destination address and port number of the packet.
State	State of the TCP connection.

show tcp detail

To display the details of the TCP connection table, use the **show tcp detail** command in XR EXEC mode.

show tcp detail pcb [*value* | **all**]

Syntax Description

pcb	Displays TCP connection information.
value	Displays a specific connection information. Range is from 0 to ffffffff.
all	Displays all connections information.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show tcp detail pcb all** command:

```
RP/0/RP0/CPU0:router# show tcp detail pcb all

Connection state is LISTEN, I/O status: 0, socket status: 0
PCB 0x8092774, vrfid 0x0
Local host: 0.0.0.0, Local port: 23
Foreign host: 0.0.0.0, Foreign port: 0

Current send queue size: 0 (max 16384)
Current receive queue size: 0 (max 16384)  mis-ordered: 0 bytes

Timer          Starts    Wakeups         Next(msec)
Retrans             0          0                 0
SendWnd             0          0                 0
TimeWait            0          0                 0
AckHold             0          0                 0
KeepAlive           0          0                 0
PmtuAger            0          0                 0
GiveUp              0          0                 0
Throttle            0          0                 0
iss: 0           snduna: 0           sndnxt: 0
sndmax: 0           sndwnd: 0           sndcwnd: 1073725440
   irs: 0           rcvnxt: 0           rcvwnd: 16384   rcvadv: 0
```

show tcp extended-filters

To display the details of the TCP extended-filters, use the **show tcp extended-filters** command in XR EXEC mode.

show tcp extended-filters [**location** *node-id*]
peer-filter [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Displays information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
peer-filter	(Optional) Displays connections with peer filter configured.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show tcp extended-filters** command for a specific location (0/RP0/CPU0):

```
RP/0/RP0/CPU0:router# show tcp extended-filters location 0/RP0/CPU0

Total Number of matching PCB's in database: 3
----------------------------------
JID: 135
Family: 2
PCB: 0x4826c5dc
L4-proto: 6
Lport: 23
Fport: 0
Laddr: 0.0.0.0
Faddr: 0.0.0.0
ICMP error filter mask: 0x12
LPTS options: 0x00000000

----------------------------------

----------------------------------
JID: 135
Family: 2
```

```
PCB: 0x4826dd8c
L4-proto: 6
Lport: 23
Fport: 59162
Laddr: 12.31.22.10
Faddr: 223.255.254.254
ICMP error filter mask: 0x12
LPTS options: 0x00000000

-----------------------------------

-----------------------------------
JID: 135
Family: 2
PCB: 0x4826cac0
L4-proto: 6
Lport: 23
Fport: 59307
Laddr: 12.31.22.10
Faddr: 223.255.254.254
ICMP error filter mask: 0x12
LPTS options: 0x00000000

-----------------------------------
```

show tcp statistics

To display TCP statistics, use the **show tcp statistics** command in XR EXEC mode.

show tcp statistics {**pcb** {**all** *pcb-address*} | **summary** } [**location** *node-id*]

Syntax Description

pcb *pcb-address*	(Optional) Displays detailed statistics for a specified connection.
pcb all	(Optional) Displays detailed statistics for all connections.
summary	(Optional) Clears summary statistic for a specific node or connection.
location *node-id*	(Optional) Displays statistics for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show tcp statistics** command:

```
RP/0/RP0/CPU0:router# show tcp statistics pcb 0x08091bc8

Statistics for PCB 0x8091bc8 VRF Id 0x60000000
Send:   0 bytes received from application
        0 xipc pulse received from application
        0 bytes sent to network
        0 packets failed getting queued to network
Rcvd:   0 packets received from network
        0 packets queued to application
        0 packets failed queued to application
```

This table describes the significant fields shown in the display.

Table 57: show tcp statistics Command Field Descriptions

Field	Description
vrfid	VPN routing and forwarding (VRF) identification (vrfid) number.
Send	Statistics in this section refer to packets sent by the router.
Rcvd:	Statistics in this section refer to packets received by the router.

show udp brief

To display a summary of the User Datagram Protocol (UDP) connection table, use the **show udp brief** command in XR EXEC mode.

show udp brief [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Displays information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show udp brief** command:

```
RP/0/RP0/CPU0:router# show udp brief

PCB        Recv-Q Send-Q  Local Address          Foreign Address
0x8040c4c      0      0  0.0.0.0:7              0.0.0.0:0
0x805a120      0      0  0.0.0.0:9              0.0.0.0:0
0x805a430      0      0  0.0.0.0:19             0.0.0.0:0
0x805a740      0      0  0.0.0.0:67             0.0.0.0:0
0x804fcb0      0      0  0.0.0.0:123            0.0.0.0:0
```

This table describes the significant fields shown in the display.

Table 58: show udp brief Command Field Descriptions

Field	Description
PCB	Protocol control block address. This is the address to a structure that contains connection information such as local address, foreign address, local port, foreign port, and so on.
Recv-Q	Number of bytes in the receive queue.
Send-Q	Number of bytes in the send queue.

Field	Description
Local Address	Local address and local port.
Foreign Address	Foreign address and foreign port.

show udp detail pcb

To display detailed information of the User Datagram Protocol (UDP) connection table, use the **show udp detail pcb** command in XR EXEC mode.

show udp detail pcb {*pcb-address* | **all**} [**location** *node-id*]

Syntax Description

pcb-address	Address of a specified UDP connection.
all	Provides statistics for all UDP connections.
location *node-id*	(Optional) Displays information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show udp detail pcb all** command:

```
RP/0/RP0/CPU0:router# show udp detail pcb all location 0/RP0/CPU0

==============================================
PCB is 0x4822fea0, Family: 2, VRF: 0x60000000
 Local host: 0.0.0.0:3784
 Foreign host: 0.0.0.0:0

Current send queue size: 0
Current receive queue size: 0
==============================================
PCB is 0x4822d0e0, Family: 2, VRF: 0x60000000
 Local host: 0.0.0.0:3785
 Foreign host: 0.0.0.0:0

Current send queue size: 0
Current receive queue size: 0
```

This table describes the significant fields shown in the display.

Table 59: show raw pcb Command Field Descriptions

Field	Description
PCB	Protocol control block address.
Family	Network protocol. IPv4 is 2; IPv6 is 26.
VRF	VPN routing and forwarding (VRF) instance name.
Local host	Local host address.
Foreign host	Foreign host address.
Current send queue size	Size of the send queue (in bytes).
Current receive queue size	Size of the receive queue (in bytes).

show udp extended-filters

To display the details of the UDP extended-filters, use the **show udp extended-filters** command in XR EXEC mode.

show udp extended-filters {**location** *node-id* | **peer-filter** {**location** *node-id}*}

Syntax Description

location *node-id*	Displays information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
peer-filter	Displays connections with peer filter configured.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show udp extended-filters** command for a specific location (0/RP0/CPU0):

```
RP/0/RP0/CPU0:router# show udp extended-filters location 0/RP0/CPU0

Total Number of matching PCB's in database: 1
----------------------------------
JID: 248
Family: 2
PCB: 0x48247e94
L4-proto: 17
Lport: 646
Fport: 0
Laddr: 0.0.0.0
Faddr: 0.0.0.0
ICMP error filter mask: 0x0
LPTS options: 0x00000000
----------------------------------
```

show udp statistics

To display User Datagram Protocol (UDP) statistics, use the **show udp statistics** command in XR EXEC mode.

show udp statistics {**summary** | **pcb** {*pcb-addressall*}} [**location** *node-id*]

Syntax Description

summary	Displays summary statistics.
pcb *pcb-address*	Displays detailed statistics for each connection.
pcb *all*	Displays detailed statistics for all connections.
location *node-id*	(Optional) Displays information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

UDP clones the received packets if there are multiple multicast applications that are interested in receiving those packets.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show udp statistics summary** command:

```
RP/0/RP0/CPU0:router# show udp statistics summary

UDP statistics:
Rcvd: 0 Total, 0 drop, 0 no port
      0 checksum error, 0 too short
Sent: 0 Total, 0 error
0 Total forwarding broadcast packets
0 Cloned packets, 0 failed cloningication
```

This table describes the significant fields shown in the display.

Table 60: show udp Command Field Descriptions

Field	Description
Rcvd: Total	Total number of packets received.

Field	Description
Rcvd: drop	Total number of packets received that were dropped.
Rcvd: no port	Total number of packets received that have no port.
Rcvd: checksum error	Total number of packets received that have a checksum error.
Rcvd: too short	Total number of packets received that are too short for UDP packets.
Sent: Total	Total number of packets sent successfully.
Sent: error	Total number of packets that cannot be sent due to errors.
Total forwarding broadcast packets	Total number of packets forwarded to the helper address.
Cloned packets	Total number of packets cloned successfully.
failed cloning	Total number of packets that failed cloning.

tcp mss

To configure the TCP maximum segment size that determines the size of the packet that TCP uses for sending data, use the **tcp mss** command in XR Config mode.

tcp mss *segment-size*

Syntax Description

segment-size	Size, in bytes, of the packet that TCP uses to send data. Range is 68 to 10000 bytes.

Command Default

If this configuration does not exist, TCP determines the maximum segment size based on the settings specified by the application process, interface maximum transfer unit (MTU), or MTU received from Path MTU Discovery.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
transport	read, write

Examples

This example shows how to configure the TCP maximum segment size:

```
RP/0/RSP0/CPU0:router(config)# tcp mss 1460
RP/0/RSP0/CPU0:router(config)# exit

Uncommitted changes found, commit them? [yes]:
RP/0/RSP0/CPU0:router:Sep  8 18:29:51.084 : config[65700]: %LIBTARCFG-6-COMMIT :

Configuration committed by user 'lab'.   Use 'show commit changes 1000000596' to view the
changes.
Sep  8 18:29:51.209 : config[65700]: %SYS-5-CONFIG_I : Configured from console by lab
```

tcp path-mtu-discovery

To allow TCP to automatically detect the highest common maximum transfer unit (MTU) for a connection, use the **tcp path-mtu-discovery** in XR Config mode. To reset the default, use the **no** form of this command.

tcp path-mtu-discovery [**age-timer** *minutes* | **infinite**]
no tcp path-mtu-discovery

Syntax Description

age-timer *minutes*	(Optional) Specifies a value in minutes. Range is 10 to 30.
infinite	(Optional) Turns off the age timer.

Command Default

tcp path-mtu-discovery is disabled

age-timer default is 10 minutes

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **tcp path-mtu-discovery** command to allow TCP to automatically detect the highest common MTU for a connection, such that when a packet traverses between the originating host and the destination host the packet is not fragmented and then reassembled.

The age timer value is in minutes, with a default value of 10 minutes. The age timer is used by TCP to automatically detect if there is an increase in MTU for a particular connection. If the **infinite** keyword is specified, the age timer is turned off.

Task ID

Task ID	Operations
transport	read, write

Examples

The following example shows how to set the age timer to 20 minutes:

```
RP/0/RP0/CPU0:router(config)# tcp path-mtu-discovery age-timer 20
```

tcp selective-ack

To enable TCP selective acknowledgment (ACK) and identify which segments in a TCP packet have been received by the remote TCP, use the **tcp selective-ack** command in XR Config mode. To reset the default, use the **no** form of this command.

tcp selective-ack
no tcp selective-ack

Syntax Description

XR Config mode

This command has no keywords or arguments.

Command Default

TCP selective ACK is disabled.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was supported.

Usage Guidelines

If TCP Selective ACK is enabled, each packet contains information about which segments have been received by the remote TCP. The sender can then resend only those segments that are lost. If selective ACK is disabled, the sender receives no information about missing segments and automatically sends the first packet that is not acknowledged and then waits for the other TCP to respond with what is missing from the data stream. This method is inefficient in Long Fat Networks (LFN), such as high-speed satellite links in which the bandwidth * delay product is large and valuable bandwidth is wasted waiting for retransmission.

Task ID

Task ID	Operations
transport	read, write

Examples

In the following example, the selective ACK is enabled:

```
RP/0/RP0/CPU0:router(config)# tcp selective-ack
```

tcp synwait-time

To set a period of time the software waits while attempting to establish a TCP connection before it times out, use the **tcp synwait-time** command in XR Config mode. To restore the default time, use the **no** form of this command.

tcp synwait-time *seconds*
no tcp synwait-time *seconds*

Syntax Description

seconds	Time (in seconds) the software waits while attempting to establish a TCP connection. Range is 5 to 30 seconds.

Command Default

The default value for the synwait-time is 30 seconds.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was supported.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
transport	read, write

Examples

The following example shows how to configure the software to continue attempting to establish a TCP connection for 18 seconds:

```
RP/0/RP0/CPU0:router(config)# tcp synwait-time 18
```

tcp timestamp

To more accurately measure the round-trip time of a packet, use the **tcp timestamp** command in XR Config mode. To reset the default, use the **no** form of this command.

tcp timestamp
no tcp timestamp

Syntax Description

This command has no keywords or arguments.

Command Default

A TCP time stamp is not used.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was supported.

Usage Guidelines

Use the **tcp timestamp** command to more accurately measure the round-trip time of a packet. If a time stamp is not used, a TCP sender deduces the round-trip time when an acknowledgment of its packet is received, which is not a very accurate method because the acknowledgment can be delayed, duplicated, or lost. If a time stamp is used, each packet contains a time stamp to identify packets when acknowledgments are received and the round-trip time of that packet.

This feature is most useful in Long Fat Network (LFN) where the bandwidth * delay product is long.

Task ID

Task ID	Operations
transport	read, write

Examples

The following example shows how to enable the timestamp option:

```
RP/0/RP0/CPU0:router(config)# tcp timestamp
```

tcp window-size

To alter the TCP window size, use the **tcp window-size** command in XR Config mode. To restore the default value, use the **no** form of this command.

tcp window-size *bytes*
no tcp window-size

Syntax Description

bytes	Window size in bytes. Range is 2048 to 65535 bytes.

Command Default

The default value for the window size is 16k.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was supported.

Usage Guidelines

Do not use this command unless you clearly understand why you want to change the default value.

Task ID

Task ID	Operations
transport	read, write

Examples

The following example shows how to set the TCP window size to 3000 bytes:

```
RP/0/RP0/CPU0:router(config)# tcp window-size 3000
```



VRRP Commands

This document describes the Cisco IOS XR software commands used to configure and monitor the Virtual Router Redundancy Protocol (VRRP) features.

For detailed information about VRRP concepts, configuration tasks, and examples, refer to the *IP Addresses and Services Configuration Guide for Cisco NCS 5000 Series Routers*.

- accept-mode, on page 534
- accept-mode (subordinate), on page 536
- address-family, on page 537
- address (VRRP), on page 538
- address global, on page 540
- address linklocal, on page 542
- address secondary, on page 544
- clear vrrp statistics, on page 546
- delay (VRRP), on page 548
- interface (VRRP), on page 549
- message state disable, on page 551
- router vrrp, on page 552
- session name(vrrp), on page 553
- show vrrp, on page 554
- vrrp slave follow, on page 560
- subordinate primary virtual IPv4 address(vrrp), on page 561
- subordinate secondary virtual IPv4 address(vrrp), on page 562
- snmp-server traps vrrp events, on page 563
- track object(vrrp), on page 564
- unicast-peer, on page 565
- vrrp, on page 566
- vrrp preempt, on page 568
- vrrp priority, on page 570
- vrrp text-authentication, on page 571
- vrrp timer, on page 572
- vrrp track interface, on page 573

accept-mode

To disable the installation of routes for the Virtual Router Redundancy Protocol (VRRP) virtual addresses, use the **accept-mode** command in the VRRP virtual router submode. To enable the installation of routes for the VRRP virtual addresses, use the **no** form of this command.

accept-mode disable

no accept-mode disable

Syntax Description

disable	Disables the accept mode.

Command Default

By default, the accept mode is enabled.

Command Modes

VRRP virtual router configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
vrrp	read, write

Example

This example shows how to disable the installation of routes for the VRRP virtual addresses:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router vrrp
RP/0/RP0/CPU0:router(config-vrrp)# interface TenGigE 0/4/0/4
RP/0/RP0/CPU0:router(config-vrrp-if)# address-family ipv4
RP/0/RP0/CPU0:router(config-vrrp-address-family)# vrrp 3 version 2
RP/0/RP0/CPU0:router(config-vrrp-virtual-router)# accept-mode disable
RP/0/RP0/CPU0:router(config-vrrp-virtual-router)#
```

Related Commands

Command	Description
address (VRRP), on page 538	Sets the primary virtual IPv4 address for a virtual router.
address global, on page 540	Configures the global virtual IPv6 address for a virtual router.
address linklocal, on page 542	Sets the virtual link-local IPv6 address for a virtual router.

Command	Description
address secondary, on page 544	Sets the secondary virtual IPv4 address for a virtual router.
message state disable, on page 551	Disables the task of logging the VRRP state change events.

accept-mode (subordinate)

To disable the installation of routes for the Virtual Router Redundancy Protocol (VRRP) virtual addresses, use the **accept-mode** command in the VRRP slave submode. To enable the installation of routes for the VRRP virtual addresses, use the **no** form of this command.

accept-mode disable

no accept-mode disable

Syntax Description

disable	Disables the accept mode.

Command Default

By default, the accept mode is enabled.

Command Modes

VRRP slave submode configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
vrrp	read, write

Example

This example shows how to disable the installation of routes for the VRRP virtual addresses:

```
Router# configure
Router(config)# router vrrp
Router(config-vrrp)# interface tenGigE 0/4/0/4
Router(config-vrrp-if)# address-family ipv4
Router(config-vrrp-address-family)# vrrp 3 slave
Router(config-vrrp-virtual-router)# accept-mode disable
Router(config-vrrp-virtual-router)#
```

Related Commands

Command	Description
accept-mode, on page 534	Disable the installation of routes for the Virtual Router Redundancy Protocol (VRRP) virtual addresses.

address-family

To enable address-family mode, use the **address-family** command in interface configuration mode. To terminate address-family mode, use the **no** form of this command.

address-family {**ipv4** | **ipv6**}
no address-family {**ipv4** | **ipv6**}

Syntax Description

ipv4	IPv4 address-family.
ipv6	IPv6 address-family.

Command Default

None.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
vrrp	read, write

Example

The following example shows how to enable address-family mode:

```
RP/0/RP0/CPU0:router # config
RP/0/RP0/CPU0:router(config)# router vrrp
RP/0/RP0/CPU0:router(config-vrrp)# interface tenGigE 0/4/0/4
RP/0/RP0/CPU0:router(config-vrrp-if)# address-family ipv4
```

Related Commands

Command	Description
interface (VRRP), on page 549	Enables VRRP interface configuration mode.

address (VRRP)

To configure the primary virtual IPv4 address for a virtual router, use the **address** command in the Virtual Router Redundancy Protocol (VRRP) virtual router submode. To deconfigure the primary virtual IPv4 address for the virtual router, use the **no** form of this command.

address *address*

no address *address*

Syntax Description

address	VRRP IPv4 address.

Command Default

None

Command Modes

VRRP virtual router

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
vrrp	read, write

Example

This example shows how to set the primary virtual IPv4 address for the virtual router:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router vrrp
RP/0/RP0/CPU0:router(config-vrrp)# interface TenGigE 0/4/0/4
RP/0/RP0/CPU0:router(config-vrrp-if)# address-family ipv4
RP/0/RP0/CPU0:router(config-vrrp-address-family)# vrrp 3 version 3
RP/0/RP0/CPU0:router(config-vrrp-virtual-router)# address 192.168.18.1
RP/0/RP0/CPU0:router(config-vrrp-virtual-router)#
```

Related Commands

Command	Description
accept-mode, on page 534	Disables the installation of routes for the VRRP virtual addresses.
address global, on page 540	Configures the global virtual IPv6 address for a virtual router.
address linklocal, on page 542	Sets the virtual link-local IPv6 address for a virtual router.

Command	Description
address secondary, on page 544	Sets the secondary virtual IPv4 address for a virtual router.
message state disable, on page 551	Disables the task of logging the VRRP state change events.

address global

To configure the global virtual IPv6 address for a virtual router, use the **address global** command in the Virtual Router Redundancy Protocol (VRRP) virtual router submode. To deconfigure the global virtual IPv6 address for a virtual router, use the **no** form of this command.

address global *ipv6-address*

no address global *ipv6-address*

Syntax Description

ipv6-address	Global VRRP IPv6 address.

Command Default

None

Command Modes

VRRP virtual router

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
vrrp	read, write

Example

This example shows how to add a global virtual IPv6 address for the virtual router:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router vrrp
RP/0/RP0/CPU0:router(config-vrrp)# interface TenGigE 0/4/0/4
RP/0/RP0/CPU0:router(config-vrrp-if)# address-family ipv6
RP/0/RP0/CPU0:router(config-vrrp-address-family)# vrrp 3 version 3
RP/0/RP0/CPU0:router(config-vrrp-virtual-router)# address global 4000::1000
RP/0/RP0/CPU0:router(config-vrrp-virtual-router)#
```

Related Commands

Command	Description
address (VRRP), on page 538	Sets the primary virtual IPv4 address for a virtual router.
accept-mode, on page 534	Disables the installation of routes for the VRRP virtual addresses.
address linklocal, on page 542	Sets the virtual link-local IPv6 address for a virtual router.

Command	Description
address secondary, on page 544	Sets the secondary virtual IPv4 address for a virtual router.
message state disable, on page 551	Disables the task of logging the VRRP state change events.

address linklocal

To either configure the virtual link-local IPv6 address for a virtual router or to specify that the virtual link-local IPv6 address should be enabled and calculated automatically from the virtual router virtual Media Access Control (MAC) address, use the **address linklocal** command in the Virtual Router Redundancy Protocol (VRRP) virtual router submode. To deconfigure the virtual link-local IPv6 address for a virtual router, use the **no** form of this command.

address linklocal [*ipv6-address* | **autoconfig**]

no address linklocal [*ipv6-address* | **autoconfig**]

Syntax Description

ipv6-address	VRRP IPv6 link-local address.
autoconfig	Autoconfigures the VRRP IPv6 link-local address.

Command Default

None

Command Modes

VRRP virtual router

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
vrrp	read, write

Example

This example shows how to autoconfigure the VRRP IPv6 link-local address:

```
RP/0/RP0/CPU0:router#configure
RP/0/RP0/CPU0:router(config)#router vrrp
RP/0/RP0/CPU0:router(config-vrrp)#interface TenGigE 0/4/0/4
RP/0/RP0/CPU0:router(config-vrrp-if)#address-family ipv6
RP/0/RP0/CPU0:router(config-vrrp-address-family)#vrrp 3
RP/0/RP0/CPU0:router(config-vrrp-virtual-router)#address linklocal autoconfig
RP/0/RP0/CPU0:router(config-vrrp-virtual-router)#
```

This example shows how to configure the virtual link-local IPv6 address for the virtual router:

```
RP/0/RP0/CPU0:router#configure
RP/0/RP0/CPU0:router(config)#router vrrp
RP/0/RP0/CPU0:router(config-vrrp)#interface TenGigE 0/4/0/4
```

```
RP/0/RP0/CPU0:router(config-vrrp-if)#address-family ipv6
RP/0/RP0/CPU0:router(config-vrrp-address-family)#vrrp 3
RP/0/RP0/CPU0:router(config-vrrp-virtual-router)#address linklocal FE80::260:3EFF:FE11:6770

RP/0/RP0/CPU0:router(config-vrrp-virtual-router)#
```

Note The **version** keyword is available only if IPv4 address-family is selected. By default, version is set to 3 for IPv6 address families.

Related Commands

Command	Description
address (VRRP), on page 538	Sets the primary virtual IPv4 address for a virtual router.
address global, on page 540	Configures the global virtual IPv6 address for a virtual router.
accept-mode, on page 534	Disables the installation of routes for the VRRP virtual addresses.
address secondary, on page 544	Sets the secondary virtual IPv4 address for a virtual router.
message state disable, on page 551	Disables the task of logging the VRRP state change events.

address secondary

To configure the secondary virtual IPv4 address for a virtual router, use the **address secondary** command in the Virtual Router Redundancy Protocol (VRRP) virtual router submode. To deconfigure the secondary virtual IPv4 address for a virtual router, use the **no** form of this command.

address *address* **secondary**

no address *address* **secondary**

Syntax Description

secondary	Sets the secondary VRRP IP address.
address	VRRP IPv4 address.

Command Default

None

Command Modes

VRRP virtual router

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
vrrp	read, write

Example

This example shows how to set the secondary virtual IPv4 address for the virtual router:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router vrrp
RP/0/RP0/CPU0:router(config-vrrp)# interface TenGigE 0/4/0/4
RP/0/RP0/CPU0:router(config-vrrp-if)# address-family ipv4
RP/0/RP0/CPU0:router(config-vrrp-address-family)# vrrp 3 version 2
RP/0/RP0/CPU0:router(config-vrrp-virtual-router)# address 192.168.18.1 secondary
RP/0/RP0/CPU0:router(config-vrrp-virtual-router)#
```

Related Commands

Command	Description
address (VRRP), on page 538	Sets the primary virtual IPv4 address for a virtual router.
address global, on page 540	Configures the global virtual IPv6 address for a virtual router.

Command	Description
address linklocal, on page 542	Sets the virtual link-local IPv6 address for a virtual router.
accept-mode, on page 534	Disables the installation of routes for the VRRP virtual addresses.
message state disable, on page 551	Disables the task of logging the VRRP state change events.

clear vrrp statistics

To reset the Virtual Router Redundancy Protocol (VRRP) statistics (to zero or default value), use the **clear vrrp statistics** command in XR EXEC mode.

clear vrrp statistics {**ipv4** | **ipv6**}[**interface** *type* *interface-path-id* [*vrid*]]

Syntax Description

ipv4	(Optional) Resets the IPv4 information.
ipv6	(Optional) Resets the IPv6 information.
interface *type*	(Optional) Interface type. For more information, use the question mark (?) online help function.

interface-path-id	(Optional) Either a physical interface instance or a virtual interface instance as follows:
	• Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation.
	  • *rack*: Chassis number of the rack.
	  • *slot*: Physical slot number of the modular services card or line card.
	  • *module*: Module number. A physical layer interface module (PLIM) is always 0.
	  • *port*: Physical port number of the interface.
	• Virtual interface instance. Number range varies depending on interface type.
	For more information about the syntax for the router, use the question mark (?) online help function.

vrid	(Optional) Virtual router identifier, which is the number identifying the virtual router for which status is displayed.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

If no **interface** is specified, the statistics for all virtual routers on all interfaces are cleared.

If no value for *vrid* is specified, the statistics for all virtual routers on the specified interface are cleared.

Task ID

Task ID	Operations
vrrp	read, write

Examples

The following example shows how to clear vrrp statistics:

```
RP/0/RP0/CPU0:router# clear vrrp statistics
```

Related Commands

Command	Description
show vrrp	Displays a brief or detailed status of one or all Virtual Router Redundancy Protocol (VRRP) virtual routers.

delay (VRRP)

To configure the activation delay for a VRRP router, use the **delay** command in VRRP interface configuration mode. To delete the activation delay, use the **no** form of this command.

delay minimum *value* **reload** *value*
no delay

Syntax Description

minimum *value*	Sets the minimum delay in seconds for every interface up event. Range is 0 to 10000.
reload *value*	Sets the reload delay in seconds for first interface up event. Range is 0 to 10000.

Command Default

minimum *value:* 1

reload *value:* 5

Command Modes

VRRP interface configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

The **vrrp delay** command delays the start of the VRRP finite state machine (FSM) on an interface up event to ensure that the interface is ready to pass traffic. This ensures that there are no mistaken state changes due to loss of hello packets. The minimum delay is applied on all interface up events and the reload delay is applied on the first interface up event.

The values of zero must be explicitly configured to turn this feature off.

Task ID

Task ID	Operations
vrrp	read, write

Examples

The following example shows how to configure a minimum delay of 10 seconds with a reload delay of 100 seconds:

```
RP/0/RP0/CPU0:router(config)# router vrrp
RP/0/RP0/CPU0:router(config-vrrp)# interface tenGigE 0/RSP0/CPU0/0
RP/0/RP0/CPU0:router(config-vrrp-if)# delay minimum 10 reload 100
```

Related Commands

Command	Description
show vrrp	Displays a brief or detailed status of one or all Virtual Router Redundancy Protocol (VRRP) virtual routers.

interface (VRRP)

To enable VRRP interface configuration mode, use the **interface (VRRP)** command in VRRP configuration mode. To terminate VRRP interface configuration mode, use the **no** form of this command.

interface *type interface-path-id*
no interface *type interface-path-id*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

VRRP is disabled.

Command Modes

VRRP configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

Use the **interface (VRRP)** command to enter VRRP interface configuration mode.

You must configure all VRRP configuration commands in VRRP interface configuration mode.

Task ID

Task ID	Operations
vrrp	read, write

Examples

The following example shows how to configure VRRP and a virtual router 1 on 10-Gigabit Ethernet interface 0/3/0/0:

```
RP/0/RP0/CPU0:router(config)# router vrrp
RP/0/RP0/CPU0:router(config-vrrp)# interface TenGigE 0/3/0/0
RP/0/RP0/CPU0:router(config-vrrp-if)# vrrp 1 ipv4 192.168.18.1
```

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# router vrrp
RP/0/RP0/CPU0:router(config-vrrp)# interface tenGigE 0/4/0/4
RP/0/RP0/CPU0:router(config-vrrp-if)# address-family ipv4
```

```
RP/0/RP0/CPU0:router(config-vrrp-address-family)# vrrp 3 version 2
RP/0/RP0/CPU0:router(config-vrrp-virtual-router)#
```

Related Commands

Command	Description
router vrrp, on page 552	Configures a VRRP redundancy process.

message state disable

To disable the task of logging the Virtual Router Redundancy Protocol (VRRP) state change events via syslog, use the **message state disable** command in the VRRP virtual router submode. To re-enable the task of logging the VRRP state change events , use the **no** form of this command.

message state disable

no message state disable

Syntax Description

This command has no keywords or arguments.

Command Default

By default, the task of logging the VRRP state change events is enabled.

Command Modes

VRRP global

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
vrrp	read, write

Example

This example shows how to disable the logging of VRRP state change events:

```
RP/0/RP0/CPU0:router#configure
RP/0/RP0/CPU0:router(config)#router vrrp
RP/0/RP0/CPU0:router(config-vrrp)#message state disable
RP/0/RP0/CPU0:router(config-vrrp)#
```

Related Commands

Command	Description
address (VRRP), on page 538	Sets the primary virtual IPv4 address for a virtual router.
address global, on page 540	Configures the global virtual IPv6 address for a virtual router.
accept-mode, on page 534	Disables the installation of routes for the VRRP virtual addresses.
address secondary, on page 544	Sets the secondary virtual IPv4 address for a virtual router.
address linklocal, on page 542	Sets the virtual link-local IPv6 address for a virtual router.

router vrrp

To configure Virtual Router Redundancy Protocol (VRRP), use the **router vrrp** command in XR Config mode. To remove the VRRP configuration, use the **no** form of this command.

router vrrp
no router vrrp

Command Default

This command has no keywords or arguments.

VRRP is disabled.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

Use the **router vrrp** command to enter VRRP configuration mode.

You must configure all VRRP configuration commands in VRRP interface configuration mode.

Task ID

Task ID	Operations
vrrp	read, write

Examples

The following example shows how to configure a VRRP with virtual router 1 on an interface:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# router vrrp
RP/0/RP0/CPU0:router(config-vrrp)# interface tenGigE 0/4/0/4
RP/0/RP0/CPU0:router(config-vrrp-if)# address-family ipv4
RP/0/RP0/CPU0:router(config-vrrp-address-family)# vrrp 3 version 2
RP/0/RP0/CPU0:router(config-vrrp-virtual-router)#
```

Related Commands

Command	Description
interface (VRRP), on page 549	Enables VRRP interface configuration mode.

session name(vrrp)

To configure a VRRP session name, use the **session name** command in the VRRP virtual router submode. To deconfigure a VRRP session name, use the **no** form of this command.

name *name*
no name *name*

Syntax Description

name	MGO session name

Command Default

None

Command Modes

VRRP virtual router configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
vrrp	read

Example

This example shows how to configure a VRRP session name.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router vrrp
RP/0/RP0/CPU0:router(config-vrrp)# interface tenGigE 0/4/0/4
RP/0/RP0/CPU0:router(config-vrrp-if)# address-family ipv4
RP/0/RP0/CPU0:router(config-vrrp-ipv4)# vrrp 1
RP/0/RP0/CPU0:router(config-vrrp-virtual-router)# name s1
RP/0/RP0/CPU0:router(config-vrrp-virtual-router)#
```

Related Commands

Command	Description
accept-mode, on page 534	Disable the installation of routes for the Virtual Router Redundancy Protocol (VRRP) virtual addresses.

show vrrp

To display a brief or detailed status of one or all Virtual Router Redundancy Protocol (VRRP) virtual routers, use the **show vrrp** command in XR EXEC mode.

show vrrp [**ipv4** | **ipv6**] [**interface** *type interface-path-id* [*vrid*]] [**brief** | **detail** | **statistics** [**all**]]

Syntax Description

ipv4	(Optional) Displays the IPv4 information.
ipv6	(Optional) Displays the IPv6 information.
interface	(Optional) Displays the status of the virtual router interface.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the show interfaces command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
vrid	(Optional) Virtual router identifier, which is the number identifying the virtual router for which status is displayed. The virtual router identifier is configured with the **vrrp ipv4** command. Range is 1 to 255.
brief	(Optional) Provides a summary view of the virtual router information.
detail	(Optional) Displays detailed running state information.
statistics	(Optional) Displays total statistics.

all	(Optional) Displays statistics for each virtual router.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 7.11.1	This command was modified. The fields **Mcast packet in Ucast mode**, **IPv4 Unicast Peer**, and **IPv4 Unicast Peer** were added.

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

If no interface is specified, all virtual routers on all interfaces are displayed. If no vrid is specified, all vrids on the given interface are displayed.

Task ID

Task ID	Operations
vrrp	read

Examples

The following sample output is from the **show vrrp** command:

```
Router# show vrrp

                    A indicates IP address owner
                    | P indicates configured to preempt
                    | |
Interface   vrID Prio A P State    Master addr     VRouter addr
Te0/3/0/0      1  100   P Init     unknown         192.168.18.10
Te0/3/0/2      7  100   P Init     unknown         192.168.19.1
```

This table describes the significant fields shown in the display.

Table 61: show vrrp Command Field Descriptions

Field	Description
Interface	Interface of the virtual router.
vrID	ID of the virtual router.
Prio	Priority of the virtual router.
A	Indicates whether the VRRP router is the IP address owner.
P	Indicates whether the VRRP router is configured to preempt (default).

Field	Description
State	State of the virtual router.
Master addr	IP address of the IP address owner router.
VRouter addr	Virtual router IP address of the virtual router.

The following sample output is from the **show vrrp** command with the **detail** keyword:

```
Router# show vrrp detail
Fri Sep  8 15:02:35.268 IST
GigabitEthernet0/0/0/0 - IPv4 vrID 1
  State is Master
    2 state changes, last state change 04:00:02
    State change history:
    Sep  8 11:02:29.518 IST  Init     -> Backup   Virtual IP configured
    Sep  8 11:02:33.127 IST  Backup   -> Master   Master down timer expired
  Last resign sent:     Never
  Last resign received: Never
  Virtual IP address is 10.0.0.100
  Virtual MAC address is 0000.5E00.0101, state is active
  Master router is local
  Version is 2
  Advertise time 1 secs
    Master Down Timer 3.609 (3 x 1 + (156 x 1/256))
  Minimum delay 1 sec, reload delay 5 sec
  Current priority 100
    Configured priority 100, may preempt
      minimum delay 0 secs
  IPv4 Unicast Peer: 10.0.1.1 --> IPv4 unicast transport is enabled on VRRP.

GigabitEthernet0/0/0/0 - IPv6 vrID 2
  State is Init
    0 state changes, last state change never
    State change history:
  Last resign sent:     Never
  Last resign received: Never
  Virtual IP address is ::
  Virtual MAC address is 0000.5E00.0202, state is stored
  Master router is unknown
  Version is 3
  Advertise time 1 secs
    Master Down Timer 3.609 (3 x 1 + (156 x 1/256))
  Minimum delay 1 sec, reload delay 5 sec
  Current priority 100
    Configured priority 100, may preempt
      minimum delay 0 secs
  IPv6 Unicast Peer: FE80::260:3EFF:FE11:6770 --> IPv6 unicast transport is enabled on VRRP.
```

This table describes the significant fields shown in the displays.

Table 62: show vrrp detail Command Field Descriptions

Field	Description
TenGigE 0/3/0/0 - vrID 1	Interface type and number, and VRRP group number.
State is	Role this interface plays within VRRP (IP address owner router or backup router).
Virtual IP address is	Virtual IP address for this virtual router.
Virtual MAC address is	Virtual MAC address for this virtual router.
Master router is	Location of the IP address owner router.
Advertise time	Interval (in seconds) at which the router sends VRRP advertisements when it is the IP address owner virtual router. This value is configured with the **vrrp timer** command.
Master Down Timer	Time the backup router waits for the IP address owner router advertisements before assuming the role of IP address owner router.
Minimum delay	Time that the state machine start-up is delayed when an interface comes up, giving the network time to settle. The minimum delay is the delay that is applied after any subsequent interface up event (if the interface flaps) and the reload delay is the delay applied after the first interface up event.
Current priority	Priority of the virtual router.
Configured priority	Priority configured on the virtual router.
may preempt	Indication of whether preemption is enabled or disabled.
minimum delay	Delay time before preemption (default) occurs.
Tracked items	Section indicating the items being tracked by the VRRP router.
Interface	Interface being tracked.
State	State of the tracked interface.
Priority Decrement	Priority to decrement from the VRRP priority when the interface is down.
IPv4 Unicast Peer	IPv4 address of the unicast peer.
IPv6 Unicast Peer	IPv6 address of the unicast peer.

The following sample output is from the **show vrrp** command with the **statistics** keyword .

```
show vrrp statistics
Fri Sep  8 15:03:03.521 IST
Invalid packets:
  Invalid checksum:                     0
  Unknown/unsupported versions:         0
  Invalid vrID:                         0
```

```
  Too short:                            0
Protocol:
  Transitions to Master                 1
Packets:
  Total received:                       0
  Adverts sent:                     14476
  Bad TTL:                              0
  Short Packets:                        0
  Failed authentication:                0
  Unknown authentication:               0
  Conflicting authentication:           0
  Unknown Type field:                   0
  Conflicting Advertise time:           0
  Conflicting Addresses:                0
  Received with zero priority:          0
  Sent with zero priority:              0
  Mcast packet in Ucast mode:           0
```

This table describes the significant fields shown in the displays.

Table 63: show vrrp statistics Command Field Descriptions

Field	Description
Invalid packets	Number of invalid packets.
Invalid checksum	Number of packets with checksum errors.
Unknown/unsupported versions	Number of packets with unknown/unsupported versions.
Invalid vrID	Number of packets with invalid VRRP ID
Too short	Number of packets that are too short.
Protocol	Role of the VRRP routers.
Transitions to Master	Number of VRRP routers that have taken over the master.
Packets	Number of packets received.
Total received	Cumulative number of packets received.
Adverts sent	Number of times the router has advertised its VRRP status.
Bad TTL	Number of packets with incorrect Time-to-Live values.
Short Packets	Number of packets with a size shorter than expected.
Failed authentication	Number of packets that failed authentication during VRRP operation.
Unknown authentication	Number of packets that failed authentication because the authentication was not recognized.
Conflicting authentication	Number of packets that failed authentication due to conflicts.
Conflicting IP addresses	Number of packets where conflicting IP addresses are detected within the VRRP configuration.
Received with zero priority	Number of packets received with zero priority.

Field	Description
Sent with zero priority	Number of packets sent by a VRRP router with a priority of zero.
Mcast packet in Ucast mode	Number of multicast packets received in a specific VRRP instance when it's configured to function in unicast mode.

The following sample output is from the **show vrrp** command with the **interface** keyword for 10-Gigabit Ethernet interface 0/3/0/0:

```
Router# show vrrp interface Ethernet0/3/0/0

                     A indicates IP address owner
                     | P indicates configured to preempt
                     | |
Interface   vrID Prio A P State    Master addr     VRouter addr
Te0/3/0/0      1  100   P Init     unknown         192.168.10.20
Te0/3/0/2      7  100   P Init     unknown         192.168.20.0
```

vrrp slave follow

To instruct the subordinate group to inherit its state from a specified group, use the **vrrp slave follow** command in VRRP slave submode.

follow *mgo-session-name*

Syntax Description

mgo-session-name	Name of the MGO session from which the subordinate group will inherit the state.

Command Default

None

Command Modes

VRRP slave submode configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
vrrp	read, write

Example

This example shows how to instruct the subordinate group to inherit its state from a specified group.

```
Router# configure
Router(config)# router vrrp
Router(config-vrrp)# interface tenGigE 0/4/0/4
Router(config-vrrp-if)# address-family ipv4
Router(config-vrrp-address-family)# vrrp 2 slave
Router(config-vrrp-slave)# follow m1
```

Note Before configuring a subordinate group to inherit its state from a specified group, the group must be configured with the **session name** command on another vrrp group.

Related Commands

Command	Description
accept-mode, on page 534	Disable the installation of routes for the Virtual Router Redundancy Protocol (VRRP) virtual addresses.

subordinate primary virtual IPv4 address(vrrp)

To configure the primary virtual IPv4 address for the subordinate group, use the **subordinate primary virtual IPv4 address** command in the VRRP slave submode.

address *ip-address*

Syntax Description

ip-address	IP address of the Hot Standby router interface.

Command Default

None

Command Modes

VRRP slave submode configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
vrrp	read, write

Example

This example shows how to configure the primary virtual IPv4 address for the subordinate group.

```
Router# configure
Router(config)# router vrrp
Router(config-vrrp)# interface tenGigE 0/4/0/4
Router(config-vrrp-if)# address-family ipv4
Router(config-vrrp-address-family)# vrrp 2 slave
Router(config-vrrp-slave)# address 192.168.10.4
```

Related Commands

Command	Description
accept-mode, on page 534	Disable the installation of routes for the Virtual Router Redundancy Protocol (VRRP) virtual addresses.

subordinate secondary virtual IPv4 address(vrrp)

To configure the secondary virtual IPv4 address for the subordinate group, use the **subordinate secondary virtual IPv4 address** command in the VRRP slave submode.

address *ip-address* **secondary**

Syntax Description

ip-address	IP address of the Hot Standby router interface.
secondary	Sets the secondary hot standby IP address.

Command Default

None

Command Modes

VRRP slave submode configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

Before configuring secondary virtual IPv4 address, the primary virtual IPv4 address for the subordinate group must be configured.

Task ID

Task ID	Operation
vrrp	read, write

Example

This example shows how to configure the secondary virtual IPv4 address for the subordinate group.

```
Router# configure
Router(config)# router vrrp
Router(config-vrrp)# interface tenGigE 0/4/0/4
Router(config-vrrp-if)# address-family ipv4
Router(config-vrrp-address-family)# vrrp 2 slave
Router(config-vrrp-slave)# address 192.168.10.4 secondary
```

Related Commands

Command	Description
accept-mode, on page 534	Disable the installation of routes for the Virtual Router Redundancy Protocol (VRRP) virtual addresses.

snmp-server traps vrrp events

To enable the Simple Network Management Protocol (SNMP) server notifications (traps) available for VRRP, use the **snmp-server traps vrrp events command** in XR Config mode. To disable all available VRRP SNMP notifications, use the **no** form of this command.

snmp-server traps vrrp events
no snmp-server traps vrrp events

Syntax Description

events	Specifies all VRRP SNMP server traps.

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to enable snmpserver notifications for VRRP:

```
RP/0/RP0/CPU0:routerrouter(config)# snmp-server traps vrrp events
```

track object(vrrp)

To enable tracking of a named object with the specified decrement, use the **track object** command in VRRP virtual router submode. To remove the tracking, use the **no** form of this command.

track object *name*[*priority-decrement*]
no track object *name*[*priority-decrement*]

Syntax Description

object *name*	Object tracking. Name of the object to be tracked.
priority-decrement	(Optional) Amount by which the VRRP priority for the router is decremented when the interface goes down (or comes back up). Range is 1 to 255.

Command Default

The default priority-decrement is 10.

Command Modes

VRRP virtual router configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
vrrp	read, write

Example

This example shows how to configure object tracking under the VRRP virtual router submode.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router vrrp
RP/0/RP0/CPU0:router(config-vrrp)# interface tenGigE 0/4/0/4
RP/0/RP0/CPU0:router(config-vrrp-if)# address-family ipv4
RP/0/RP0/CPU0:router(config-vrrp-ipv4)# vrrp 1
RP/0/RP0/CPU0:router(config-vrrp-virtual-router)# track object t1 2
RP/0/RP0/CPU0:router(config-vrrp-virtual-router)#
```

Related Commands

Command	Description
accept-mode, on page 534	Disable the installation of routes for the Virtual Router Redundancy Protocol (VRRP) virtual addresses.

unicast-peer

To enable IPv4 and IPv6 layer 3 unicast transport on Virtual Router Redundancy Protocol (VRRP), use the command in VRRP virtual router submode. To disable unicast transport, use the **no** form of this command.

unicast-peer { *ipv4-address* | *ipv6-link-local-addres* }

Syntax Description

ipv4-address	IPv4 address
ipv6-link-local-address	IPv6 link-local address

Command Default

VRRP transmits multicast traffic.

Command Modes

VRRP virtual router configuration

Command History

Release	Modification
Release 7.11.1	This command was introduced.

Usage Guidelines

You can configure the unicast-peer command only once, allowing for the participation of only two physical routers in a unicast VRRP session.

When you configure the unicast-peer command, the router neither sends nor receives multicast packets

Task ID

Task ID	Operation
vrrp	read,write

Example

This example shows how to configure IPv4 Layer 3 unicast transport on VRRP.

```
Router(config)# router vrrp
Router(config-vrrp)# interface GigabitEthernet0/0/0/0
Router(config-vrrp-if)# address-family ipv4
Router(config-vrrp-address-family)# vrrp 1

Router(config-vrrp-virtual-router)# address 10.0.1.100

Router(config-vrrp-virtual-router)# unicast-peer 10.0.1.1
```

This example shows how to configure IPv6 Layer 3 unicast transport on VRRP.

```
Router(config)# router vrrp
Router(config-vrrp)# interface GigabitEthernet0/0/0/0
Router(config-vrrp-if)# address-family ipv6
Router(config-vrrp-address-family)# vrrp 2

Router(config-vrrp-virtual-router)# unicast-peer FE80::260:3EFF:FE11:6770
```

vrrp

To enable Virtual Router Redundancy Protocol (VRRP) virtual router mode, use the **vrrp** command in address-family mode. To terminate VRRP virtual router mode, use the **no** form of this command.

vrrp *vrid* **version** *version-no*
novrrp *vrid* **version** *version-no*

Syntax Description

vrid	(Optional) Virtual router identifier, which is the number identifying the virtual router for which status is displayed. The virtual router identifier is configured with the vrrp ipv4 command. Range is 1 to 255.
version *version-no*	The VRRP version number. Range is 2-3. **Note** The **version** keyword is available only for the ipv4 address family. By default, version is set to 3 for IPv6 address families.

Command Default

None.

Command Modes

address-family

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
vrrp	read, write

Example

The following example shows how to enable VRRP virtual router mode:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# router vrrp
RP/0/RP0/CPU0:router(config-vrrp)# interface tenGigE 0/4/0/4
RP/0/RP0/CPU0:router(config-vrrp-if)# address-family ipv4
RP/0/RP0/CPU0:router(config-vrrp-address-family)# vrrp 3 version 2
RP/0/RP0/CPU0:router(config-vrrp-virtual-router)#
```

Related Commands

Command	Description
interface (VRRP), on page 549	Enables VRRP interface configuration mode.

vrrp preempt

VRRP preempt is enabled by default. This means, a VRRP router with higher priority than the current IP address owner router will take over as new IP address owner router. To disable this feature, use the **preempt disable** command. To delay preemption, so that the higher priority router waits for a period of time before taking over, use the **preempt delay** command. To restore the default behavior (preempt enabled with no delay), use the **no** form of the command.

preempt {**delay** *seconds* | **disable**}
no preempt {**delay** *seconds* | **disable**}

Syntax Description

delay *seconds*	Specifies the number of seconds the router delays before issuing an advertisement claiming virtual IP address ownership to be the IP address owner router. Range is 1 to 3600 seconds (1 hour).
disable	Disables preemption.

Command Default

VRRP preempt is enabled.

seconds : 0 (no delay)

Command Modes

VRRP virtual router

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

By default , the router being configured with this command takes over as new IP address owner router for the virtual router if it has a higher priority than the current IP address owner router. You can configure a delay, which causes the VRRP router to wait the specified number of seconds before issuing an advertisement claiming virtual IP address ownership to be the IP address owner router.



Note The router that is the virtual IP address owner preempts, regardless of the setting of this command.

Task ID

Task ID	Operations
vrrp	read, write

Examples

The following example shows how to configure the router to preempt the current IP address owner router when its priority of 200 is higher than that of the current IP address owner router. If the router preempts the current IP address owner router, it waits 15 seconds before issuing an advertisement claiming that it is the new IP address owner router.

```
Router(config)# router vrrp
Router(config-vrrp)# interface TenGigE 0/3/0/0
Router(config-vrrp-if)# address-family ipv4
Router(config-vrrp-address-family)# vrrp 1 version 3
Router(config-vrrp-virtual-router)# preempt delay 15
Router(config-vrrp-virtual-router)# priority 200
```

Related Commands

Command	Description
vrrp priority, on page 570	Sets the priority of the virtual router.

vrrp priority

To set the priority of the virtual router, use the **priority** command in VRRP virtual router submode. To remove the priority of the virtual router, use the **no** form of this command.

priority *priority*
nopriority *priority*

Syntax Description

priority	Priority of the virtual router. Range is 1 to 254.

Command Default

priority : 100

Command Modes

VRRP virtual router

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

Use this command to control which router becomes the IP address owner router. This command is ignored while the router is the virtual IP address owner.

Task ID

Task ID	Operations
vrrp	read, write

Examples

The following example shows how to configure the router with a priority of 254:

```
Router(config)# router vrrp
Router(config-vrrp)# interface TenGigE 0/3/0/0
Router(config-vrrp-if)# address-family ipv4
Router(config-vrrp-address-family)# vrrp 1 version 3
Router(config-vrrp-virtual router)# priority 254
```

Related Commands

Command	Description
vrrp preempt, on page 568	Controls which router becomes the IP address owner router.

vrrp text-authentication

To configure the simple text authentication used for Virtual Router Redundancy Protocol (VRRP) packets received from other routers running VRRP, use the **text-authentication** command in VRRP virtual router submode. To disable VRRP authentication, use the **no** form of this command.

text-authentication *string*
no text-authentication [*string*]

Syntax Description

string	Authentication string (up to eight alphanumeric characters) used to validate incoming VRRP packets.

Command Default

No authentication of VRRP messages occurs.

Command Modes

VRRP virtual router

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

When a VRRP packet arrives from another router in the VRRP group, its authentication string is compared to the string configured on the local system. If the strings match, the message is accepted. If they do not match, the packet is discarded.

All routers within the group must be configured with the same authentication string.

Note Plain text authentication is not meant to be used for security. It simply provides a way to prevent a misconfigured router from participating in VRRP.

Task ID

Task ID	Operations
vrrp	read, write

Examples

The following example shows how to configure an authentication string of x30dn78k:

```
RP/0/RP0/CPU0:router(config)# router vrrp
RP/0/RP0/CPU0:router(config-vrrp)# interface TenGigE 0/3/0/0
RP/0/RP0/CPU0:router(config-vrrp-if)# address-family ipv4
RP/0/RP0/CPU0:router(config-vrrp-address-family)# vrrp 1 version 2
RP/0/RP0/CPU0:router(config-vrrp-virtual-router)# text-authentication x30dn78k
```

Note Text authentication is only valid for VRRP version 2 routers.

vrrp timer

To configure the interval between successive advertisements by the IP address owner router in a Virtual Router Redundancy Protocol (VRRP) virtual router, use the **timer** command in VRRP virtual router submode. To restore the default value, use the **no** form of this command.

timer [**msec**] *interval* [**force**]
no timer [**msec**] *interval* [**force**]

Syntax Description

msec	(Optional) Changes the unit of the advertisement time from seconds to milliseconds. Without this keyword, the advertisement interval is in seconds. Range is 20 to 3000 milliseconds.
interval	Time interval between successive advertisements by the IP address owner router. The unit of the interval is in seconds, unless the **msec** keyword is specified. Range is 1 to 255 seconds.
force	(Optional) Forces the configured value to be used. This keyword is required if milliseconds is specified.

Command Default

interval:1 second

Command Modes

VRRP virtual router

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
vrrp	read, write

Examples

The following example shows how to configure the IP address owner router to send advertisements every 4 seconds:

```
Router(config)# router vrrp
Router(config-vrrp)# interface TenGigE 0/3/0/0
Router(config-vrrp-if)# address-family ipv4
Router(config-vrrp-address-family)# vrrp 1 version 3
Router(config-vrrp-virtual-router)# timer 4
```

vrrp track interface

To configure the Virtual Router Redundancy Protocol (VRRP) to track an interface, use the **track interface** command in VRRP virtual router submode. To disable the tracking, use the **no** form of this command.

track interface *type interface-path-id* [*priority-decrement*]
no track interface *type interface-path-id* [*priority-decrement*]

Syntax Description

vrid	Virtual router identifier, which is the number identifying the virtual router to which tracking applies.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
priority-decrement	(Optional) Amount by which the priority for the router is decremented (or incremented) when the tracked interface goes down (or comes back up). Decrements can be set to any value between 1 and 254. Default value is 10.

Command Default

The default decrement value is 10. Range is 1 to 254.

Command Modes

VRRP virtual router

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

The **vrrp track interface** command ties the priority of the router to the availability of its interfaces. It is useful for tracking interfaces that are not configured for VRRP. Only IP interfaces are tracked. A tracked interface is up if IP on that interface is up. Otherwise, the tracked interface is down.

You can configure VRRP to track an interface that can alter the priority level of a virtual router for a VRRP virtual router. When the IP protocol state of an interface goes down or the interface has been removed from the router, the priority of the backup virtual router is decremented by the value specified in the *priority-decrement* argument. When the IP protocol state on the interface returns to the up state, the priority is restored.

Task ID

Task ID	Operations
vrrp	read, write

Examples

In the following example, 10-Gigabit Ethernet interface 0/3/0/0 tracks interface 0/3/0/3 and 0/3/0/2. If one or both of these two interfaces go down, the priority of the router decreases by 10 (default priority decrement) for each interface. The default priority decrement is changed using the *priority-decrement* argument. In this example, because the default priority of the virtual router is 100, the priority becomes 90 when one of the tracked interfaces goes down and the priority becomes 80 when both go down. See the **priority** command for details on setting the priority of the virtual router.

```
RP/0/RP0/CPU0:router(config)# router vrrp
RP/0/RP0/CPU0:router(config-vrrp)# interface TenGigE 0/3/0/0
RP/0/RP0/CPU0:router(config-vrrp-if)# address-family ipv4
RP/0/RP0/CPU0:router(config-vrrp-address-family)# vrrp 1 version 3
RP/0/RP0/CPU0:router(config-vrrp-virtual-router)# track interface TenGigE 0/3/0/3
RP/0/RP0/CPU0:router(config-vrrp-virtual-router)# track interface TenGigE 0/3/0/2
```

Related Commands

Command	Description
vrrp priority, on page 570	Sets the priority of the virtual router.