Cisco ASR 9000 Series Aggregation Services Router Broadband Network Gateway Command Reference, Release 5.1.x

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

Text Part Number: OL-30344-01

© Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Preface xi

Changes to This Document xi

Obtaining Documentation and Submitting a Service Request xi

CHAPTER 1

BNG AAA Commands 1

accounting aaa list 3

accounting aaa list type service 5

aaa accounting service 7

aaa accounting subscriber 9

aaa accounting system rp-failover 11

aaa attribute format 13

aaa authentication subscriber 16

aaa authorization subscriber 18

aaa group server radius (BNG) 20

aaa intercept 22

aaa radius attribute 23

aaa service-accounting 25

aaa server radius dynamic-author 27

aaa radius attribute nas-port-type 29

radius-server attribute 31

radius-server dead-criteria 33

radius-server deadtime (BNG) 35

radius-server disallow null-username 37

radius-server host (BNG) 38

radius-server ipv4 dscp 41

radius-server key (BNG) 42

radius-server load-balance 44

radius-server retransmit (BNG) 46
radius-server source-port 48
radius-server timeout (BNG) 49
radius-server vsa attribute ignore unknown 50
radius-server throttle 51
radius source-interface (BNG) 53
show aaa trace 55
show radius (BNG) 57
show radius server-groups detail 60
statistics period service-accounting 62

CHAPTER 2 ACL and ABF Commands 65
ipv4 access-group (BNG) 66
ipv4 access-list (BNG) 69
ipv6 access-group (BNG) 71
ipv6 access-list (BNG) 73

CHAPTER 3 Address Pool Service Commands 77
address-range 78
exclude 80
network (BNG) 82
prefix-length 84
prefix-range 86
pool vrf 88
pool ipv4 90
pool ipv6 92
utilization-mark 94
show pool ipv4 name 96
show pool ipv6 name 100
show pool vrf 107

CHAPTER 4 Control Policy Commands 111
activate 112
authenticate (BNG) 114
authorize 116

class-map type control subscriber 118
deactivate 120
event 122
match (class-map) 124
policy-map type control subscriber 126
policy-map type pbr 128
service-policy type control subscriber 130
show class-map 132
show policy-map 134

CHAPTER 5 BNG DHCP Commands 137
address-pool 139
aftr-name 140
broadcast-flag policy check (BNG) 141
class 143
dhcp ipv4 (BNG) 145
dhcp ipv6 (BNG) 146
dhcpv6 address-pool 147
dhcpv6 delegated-prefix-pool 149
dns-server (BNG) 150
domain-name (DHCP IPv6 pool-BNG) 152
framed-prefix-pool 154
helper-address (BNG) 155
interface (DHCP-BNG) 157
interface subscriber-pppoe profile 159
lease 160
match option 162
match vrf 164
prefix-pool 165
profile (BNG) 166
relay information authenticate (BNG) 168
relay information check (BNG) 170
relay information option (BNG) 172
relay information option allow-untrusted (BNG) 174
relay information policy (BNG) 176

relay option remote-id 178
limit lease per-circuit-id 180
limit lease per-remote-id 182
limit lease per-interface 184
lease proxy client-lease-time 186
show dhcp ipv4 proxy binding 188
show dhcp ipv4 proxy interface (BNG) 191
show dhcp ipv4 proxy profile 193
show dhcp ipv4 proxy statistics 195
show dhcp ipv6 proxy binding (BNG) 197
show dhcp ipv6 proxy interface (BNG) 199
show dhcp ipv6 proxy profile 201
show dhcp ipv6 proxy statistics 203
show dhcp ipv6 server binding 205
show dhcp ipv6 server interface 208
show dhcp ipv6 server profile 210
show dhcp ipv6 server statistics 212

CHAPTER 6 Dynamic Template Commands 215
dynamic-template 216
dynamic-template type ipsubscriber 218
dynamic-template type ppp 220
dynamic-template type service 222
monitor-session (interface-dynamic-template-BNG) 224
service-policy (BNG) 226
test radius coa activate 228
timeout idle 230
vrf (dynamic-template-BNG) 232

CHAPTER 7 Excessive Punt Flow Trap Commands 235
lpts punt excessive-flow-trap 236
lpts punt excessive-flow-trap non-subscriber-interfaces 238
lpts punt excessive-flow-trap penalty-rate 239
lpts punt excessive-flow-trap penalty-timeout 241
lpts punt excessive-flow-trap subscriber-interfaces 243

show lpts punt excessive-flow-trap 244
show lpts punt excessive-flow-trap information 247
show lpts punt excessive-flow-trap interface 250
show lpts punt excessive-flow-trap protocol 253

CHAPTER 8 IPoE Commands 255
initiator dhcp 256
initiator unclassified-source 258
ipsubscriber interface 260
ipsubscriber l2-connected 262
ipsubscriber routed 264
ipsubscriber session-limit 266
show ipsubscriber access-interface 268
show ipsubscriber interface 271
show ipsubscriber summary 275

CHAPTER 9 IPv4 and IPv6 Commands 279
ipv4 mtu (BNG) 280
ipv4 unnumbered (point-to-point -BNG) 282
ipv4 unreachables disable (BNG) 284
ipv4 verify unicast source reachable-via (BNG) 286
ipv6 enable (BNG) 288
ipv6 mtu (BNG) 290
ipv6 unreachables disable (BNG) 292
show ipv4 interface (BNG) 294
show ipv4 traffic (BNG) 298
show ipv6 interface (BNG) 301
show ipv6 neighbors (BNG) 305
show ipv6 neighbors summary (BNG) 311
show ipv6 traffic (BNG) 313

CHAPTER 10 Multicast Commands 317
router igmp vrf 318
igmp accounting 319
igmp explicit-tracking 320

igmp query-interval 322
igmp query-max-response-time 324
multicast (BNG) 326
unicast-qos-adjust 328
show igmp unicast-qos-adjust statistics 330
show igmp vrf (BNG) 333
clear igmp unicast-qos-adjust 335

CHAPTER 11 Neighbor Discovery Commands 337
ipv6 nd dad attempts (BNG) 338
ipv6 nd framed-prefix-pool 341
ipv6 nd managed-config-flag (BNG) 342
ipv6 nd ns-interval (BNG) 344
ipv6 nd nud-enable 346
ipv6 nd other-config-flag (BNG) 347
ipv6 nd ra-initial 349
ipv6 nd ra-interval (BNG) 351
ipv6 nd ra-lifetime (BNG) 353
ipv6 nd ra-unicast 355
ipv6 nd reachable-time (BNG) 356
ipv6 nd suppress-cache-learning 358
ipv6 nd suppress-ra (BNG) 359

CHAPTER 12 BNG PPP Commands 361
ppp authentication (BNG) 362
ppp chap 365
ppp ipcp 367
ppp lcp 369
ppp max-bad-auth (BNG) 371
ppp max-configure (BNG) 373
ppp max-failure (BNG) 375
ppp ms-chap 377
ppp timeout 379
show ppp interfaces (BNG) 381
show ppp statistics 389

show ppp summary 392

CHAPTER 13 PPPoE LAC-Specific Commands 395

l2tp-class 396

l2tp reassembly 398

process-failures switchover 399

redundancy (BNG) 401

session-limit (BNG) 402

template (BNG) 404

tunnel 406

vpdn 408

vpn 410

show l2tpv2 412

show l2tpv2 redundancy 414

show l2tpv2 redundancy mirroring 416

show vpdn 418

show vpdn redundancy 420

show vpdn redundancy mirroring 422

CHAPTER 14 PPPoE Commands 425

pado delay 426

pado delay circuit-id 428

pado delay remote-id 430

pado delay service-name 432

pppoe bba-group 434

pppoe enable bba-group 437

pppoe sessions limit 439

pppoe sessions throttle 442

clear pppoe statistics 444

show pppoe interfaces 446

show pppoe limits 448

show pppoe statistics 452

show pppoe summary 455

show pppoe throttles 457

CHAPTER 15 QOS Commands 461

qos account 462

qos output minimum-bandwidth 464

service-policy (QoS-BNG) 466

service-policy (interface-BNG) 468

show qos inconsistency (BNG) 470

show qos interface (BNG) 473

show qos shared-policy-instance (BNG) 478

show qos summary (BNG) 481

CHAPTER 16 Subscriber Commands 483

subscriber session limit 484

show subscriber database 486

show subscriber feature accounting 491

show subscriber manager sadb 493

show subscriber manager statistics 495

show subscriber running-config 498

show subscriber session 500

clear subscriber session 504

Preface

The Preface contains these topics:

- Changes to This Document, page xi
- Obtaining Documentation and Submitting a Service Request, page xi

Changes to This Document

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

Table 1: Changes to This Document

Revision	Date	Change Summary
OL-30344-02	January 2014	Republished with documentation updates for Cisco IOS XR Release 5.1.1 features.
OL-30344-01	September 2013	Initial release of this document.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

BNG AAA Commands

This module describes the Cisco IOS XR software commands used to configure the AAA commands for Broadband Network Gateway (BNG) on the Cisco ASR 9000 Series Router. For details regarding the related configurations, refer to the *Cisco ASR 9000 Series Aggregation Services Router Broadband Network Gateway Configuration Guide*.

- accounting aaa list, page 3
- accounting aaa list type service, page 5
- aaa accounting service, page 7
- aaa accounting subscriber, page 9
- aaa accounting system rp-failover, page 11
- aaa attribute format, page 13
- aaa authentication subscriber, page 16
- aaa authorization subscriber, page 18
- aaa group server radius (BNG), page 20
- aaa intercept, page 22
- aaa radius attribute, page 23
- aaa service-accounting, page 25
- aaa server radius dynamic-author, page 27
- aaa radius attribute nas-port-type, page 29
- radius-server attribute, page 31
- radius-server dead-criteria, page 33
- radius-server deadtime (BNG), page 35
- radius-server disallow null-username, page 37
- radius-server host (BNG), page 38
- radius-server ipv4 dscp, page 41
- radius-server key (BNG), page 42

- radius-server load-balance, page 44
- radius-server retransmit (BNG), page 46
- radius-server source-port, page 48
- radius-server timeout (BNG), page 49
- radius-server vsa attribute ignore unknown, page 50
- radius-server throttle, page 51
- radius source-interface (BNG), page 53
- show aaa trace, page 55
- show radius (BNG), page 57
- show radius server-groups detail, page 60
- statistics period service-accounting, page 62

accounting aaa list

To configure the subscriber accounting feature, use the **accounting aaa list** command in the dynamic template configuration mode. To disable this feature, use the **no** form of this command.

accounting aaa list {*method_list_name*| **default**} **type session** {**dual-stack-delay** *time*| **periodic-interval** *time*}

no accounting aaa list {*method_list_name*| **default**} **type session** {**dual-stack-delay** *time*| **periodic-interval** *time*}

Syntax Description

method_list_name	Specifies the preconfigured method list name.
default	Specifies the default method list.
type	Specifies the type of accounting performed.
session	Applies the accounting to a session.
dual-stack-delay	Specifies the dual stack set delay wait in seconds.
time	Specifies the value of the dual stack delay time in seconds. The value ranges from 1-30.
periodic-interval	Specifies the periodic accounting interval in minutes.
time	Specifies the value of the periodic accounting interval in minutes. The value ranges from 1-65535.

Command Default

None

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Use the **dynamic-template** command to enter dynamic template configuration mode.

Task ID

Task ID	Operation
config-services	read, write

Examples

This is an example of configuring **accounting aaa list** command for periodic accounting interval of 456 minutes:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template
RP/0/RSP0/CPU0:router(config-dynamic-template)# type service s1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# accounting aaa list l1 type session
periodic-interval 456
```

Related Commands

Command	Description
dynamic-template, on page 216	Enables the dynamic template configuration mode.
dynamic-template type ppp, on page 220	Enables the ppp dynamic template type.
dynamic-template type ipsubscriber, on page 218	Enables the ipsubscriber dynamic template type.

accounting aaa list type service

To configure the service accounting feature, use the **accounting aaa list type service** command in the dynamic template configuration mode. To disable this feature, use the **no** form of this command.

accounting aaa list {*method_list_name*| **default**} **type service** [**periodic-interval** *time*]

no accounting aaa list {*method_list_name*| **default**} **type service** [**periodic-interval** *time*]

Syntax Description

method_list_name	Specifies the pre-configured method list name.
default	Specifies the default method list.
type	Specifies the type of accounting performed.
service	Applies the accounting to a service.
periodic-interval	Specifies the periodic accounting interval in minutes.
time	Value of the periodic accounting interval in minutes. The range is from 1 to 65535.

Command Default

None

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

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

Use the **dynamic-template** command to enter dynamic template configuration mode.

Task ID

Task ID	Operation
config-services	read, write

Examples

This is an example of configuring service accounting for periodic accounting interval of 600 minutes:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template
RP/0/RSP0/CPU0:router(config-dynamic-template)# type service s1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# accounting aaa list l1 type service
periodic-interval 600
```

Related Commands

Command	Description
dynamic-template, on page 216	Enables the dynamic template configuration mode.
dynamic-template type service, on page 222	Specifies the service template type for a group of subscribers or services.

aaa accounting service

To create an accounting list for service accounting, use the **aaa accounting service** command in global configuration mode or administration configuration mode. To disable the service authentication method, use the **no** form of this command.

aaa accounting service {*list_name*| **default**} {**broadcast group** {*group_name*| **radius**}| **group** {*group_name*| **radius**}}

no aaa accounting subscriber {*list_name*| **default**} {**broadcast group** {*group_name*| **radius**}| **group** {*group_name*| **radius**}}

Syntax Description

default	Uses the listed authentication methods that follow this keyword as the default list of methods for authentication.
list-name	Represents the character string of the list name for AAA authentication.
broadcast	Specifies the broadcast accounting for the service.
group	Specifies the server-group.
group_name	Specifies the server group name.
radius	Specifies the list of all RADIUS hosts.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
aaa	read, write

Examples

This is an example of configuring the **aaa accounting service** command for the grpFR server group:

```
RP/0/RSP0/CPU0:router(config)# aaa accounting service default group grpFR
```

Related Commands

Command	Description
aaa accounting subscriber, on page 9	Creates an accounting list for subscriber accounting.

aaa accounting subscriber

To create an accounting list for subscriber accounting, use the **aaa accounting subscriber** command in global configuration mode or administration configuration mode. To disable this accounting list for subscriber accounting, use the **no** form of this command.

aaa accounting subscriber {*list_name*| **default**} {**broadcast group** {*group_name*| **radius**}| **group** {*group_name*| **radius**}}

no aaa accounting subscriber {*list_name*| **default**} {**broadcast group** {*group_name*| **radius**}| **group** {*group_name*| **radius**}}

Syntax Description

default	Uses the listed authentication methods that follow this keyword as the default list of methods for authentication.
list-name	Represents the character string for the list name for AAA authentication.
broadcast	Specifies the broadcast accounting for subscriber.
group	Specifies the server-group.
group_name	Specifies the server group name.
radius	Specifies the list of all RADIUS hosts.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
aaa	read, write

Examples

This is an example of configuring the **aaa accounting subscriber** command for sg1 server group:

```
RP/0/RSP0/CPU0:router(config)# aaa accounting subscriber sub1 broadcast group radius group
 sg1
```

Related Commands

Command	Description
aaa accounting system rp-failover, on page 11	Creates an accounting list for system events.

aaa accounting system rp-failover

To create an accounting list to send rp-failover or rp-switchover start or stop accounting messages, use the **aaa accounting system rp-failover** command in global configuration mode. To disable the system accounting for rp-failover, use the **no** form of this command.

aaa accounting system rp-failover {*list_name* {**start-stop| stop-only**}| **default** {**start-stop| stop-only**}}

no aaa accounting system rp-failover {*list_name* {**start-stop| stop-only**}| **default** {**start-stop| stop-only**}}

Syntax Description

list_name	Specifies the accounting list name.
default	Specifies the default accounting list.
start-stop	Enables the start and stop records.
stop-only	Enables the stop records only.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
aaa	read, write

Examples

This is an example of configuring the **aaa accounting system rp-failover** command for default accounting list:

```
RP/0/RSP0/CPU0:router(config)# aaa accounting system rp-failover default start-stop none
```

Related Commands

Command	Description
aaa attribute format, on page 13	Create an AAA attribute format name.

aaa attribute format

To create an AAA attribute format name and to enter the configuration ID format sub mode, use the **aaa attribute format** command in global configuration mode. To disable this AAA attribute format, use the **no** form of this command.

aaa attribute format *format_name* [**circuit-id[plus][mac-address| remote-id]** [**separator** *separator*] | **format-string** [**length** *length*] {*string* [*Identity-Attribute*]} | **mac-address [plus][circuit-id | remote-id][separator** *separator*] | **remote-id [plus][circuit-id | mac-address][separator** *separator*] | **username-strip**{**prefix-delimiter**| **suffix-delimiter**} {*delimiter*}]

no aaa attribute format *format_name*

Syntax Description

format_name	Specifies the name of the format.
circuit-id	Specifies the construction of the AAA attribute format name for subscribers based on the circuit-ID.
format-string	Specifies the extended string format of the AAA attribute format name.
string	Specifies the regular ASCII characters that includes conversion specifiers. The value is enclosed in double quotes.
Identity-Attribute	Identifies a session. For more information about the syntax for the router, use the question mark (?) online help function.
length	Specifies the length of the formatted attribute string.
length	Length of the formatted string, in integer. The range is from 1 to 253.
mac-address	Specifies the construction of the AAA attribute format name for subscribers based on the mac-address. The MAC address must be in the form of three 4-digit values (12 digits in dotted decimal notation).
remote-id	Specifies the construction of the AAA attribute format name for subscribers based on the remote-ID.
plus	Specifies the use of additional identifiers.
separator	Specifies the separator to be used between keys.
separator	Separator to be used between keys, default is a semicolon.

username-strip	Configures a network access server (NAS) to strip both suffixes and/or prefixes from the username before forwarding the username to the remote RADIUS server.
prefix-delimiter	Enables prefix stripping and specifies the character that will be recognized as a prefix delimiter.
suffix-delimiter	Enables suffix stripping and specifies the character that will be recognized as a suffix delimiter.
Delimiter	Suffix or prefix delimiter.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.
Release 4.2.1	The support for **format-string** keyword was added.

Usage Guidelines

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

Task ID

Task ID	Operation
aaa	read, write

Examples

This is an example of configuring the **aaa attribute format** command in the global configuration mode:

```
RP/0/RSP0/CPU0:router(config)# aaa attribute format form1
RP/0/RSP0/CPU0:router(config-id-format)# format-string "%s%s"
RP/0/RSP0/CPU0:router(config-id-format)# username-strip prefix-delimiter @
```

Related Commands

Command	Description
aaa accounting subscriber, on page 9	Creates an accounting list for subscriber accounting.

aaa authentication subscriber

To create a method list for subscriber authentication, use the **aaa authentication subscriber** command in global configuration mode. To disable this subscriber authentication method, use the **no** form of this command.

aaa authentication subscriber {*list_name*| **default**} **group** {*server_group_name*| **radius**}

no aaa authentication subscriber {*list_name*| **default**} **group** {*server_group_name*| **radius**}

Syntax Description

default	Uses the listed authentication methods that follow this keyword as the default list of methods for authentication.
list-name	Represents the character string for the list name for AAA authentication.
group	Specifies the server-group.
radius	Specifies the list of all RADIUS hosts.
server_group_name	Specifies the server group name.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
aaa	read, write

Examples

This is an example of configuring the **aaa authentication subscriber** command in the global configuration mode:

```
RP/0/RSP0/CPU0:router(config)# aaa authentication subscriber sub1 group sg1 group sg2
```

Related Commands

Command	Description
aaa authorization subscriber, on page 18	Creates authorization-related configurations

aaa authorization subscriber

To create authorization-related configurations, use the **aaa authorization subscriber** command in global configuration mode. To disable this subscriber authorization method, use the **no** form of this command.

aaa authorization subscriber {*list_name*| **default**} **group** {*server_group_name*| **radius**}

no aaa authorization subscriber {*list_name*| **default**} **group** {*server_group_name*| **radius**}

Syntax Description

default	Uses the listed authentication methods that follow this keyword as the default list of methods for authentication.
list-name	Represents the character string for the list name for AAA authorization.
group	Specifies the server-group.
radius	Specifies the list of all RADIUS hosts.
server_group_name	Specifies the server group name.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
aaa	read, write

Examples

This is an example of configuring the **aaa authorization subscriber** command in the global configuration mode:

```
RP/0/RSP0/CPU0:router(config)# aaa authorization subscriber sub1 group sg1 group sg2
```

Related Commands

Command	Description
aaa authentication subscriber, on page 16	Creates a method list for subscriber authentication.

aaa group server radius (BNG)

To configure a group server radius, use the **aaa group server radius** command in global configuration mode. To disable this AAA group server radius, use the **no** form of this command.

aaa group server radius *sever_group_name* [**accounting| authorization| deadtime| load-balance| server| server-private| source-interface| throttle| vrf**]

no aaa group server radius *sever_group_name* [**accounting| authorization| deadtime| load-balance| server| server-private| source-interface| throttle| vrf**]

Syntax Description

server_group_name	Specifies the AAA group server RADIUS name.
accounting	Specifies a RADIUS attribute filter for accounting.
authorization	Specifies a RADIUS attribute filter for authorization.
deadtime	Specifies the time in minutes after which a RADIUS server will be marked up after it has gone dead.
load-balance	Specifies the radius load-balancing options.
server	Specifies the RADIUS server.
server-private	Specifies the RADIUS server.
source-interface	Specifies interface for source address in RADIUS packet.
throttle	Specifies RADIUS throttling options.
vrf	Specifies the VRF to which the server group belongs.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
ip-services	read, write

Examples

This is an example of configuring the **aaa group server radius** command in the global configuration mode:

```
RP/0/RSP0/CPU0:router(config)#aaa group server radius SG1
RP/0/RSP0/CPU0:router(config-sg-radius)#server 99.1.1.10 auth-port 1812 acct-port 1813
RP/0/RSP0/CPU0:router(config-sg-radius)#throttle access 10 access-timeout 5 accounting 5
```

aaa intercept

To enable RADIUS-based Lawful Intercept (LI) feature on a router, use the **aaa intercept** command in global configuration mode. To disable RADIUS-based Lawful Intercept feature, use the **no** form of this command.

aaa intercept

no aaa intercept

Syntax Description

This command has no keywords or arguments.

Command Default

RADIUS-based Lawful Intercept feature is not enabled.

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

Use the **aaa intercept** command to enable a RADIUS-Based Lawful Intercept solution on your router. Intercept requests are sent (through Access-Accept packets or CoA-Request packets) to the network access server (NAS) or the Layer 2 Tunnel Protocol (L2TP) access concentrator (LAC) from the RADIUS server. All data traffic going to, or from, a PPP or L2TP session is passed to a mediation device.

Task ID

Task ID	Operation
aaa	read, write
li	read

Examples

This example shows how to configure **aaa intercept** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa intercept
```

aaa radius attribute

To configure a format e encode string for particular interface or NAS-Port type and to create an AAA radius attribute format configuration, use the **aaa radius attribute** command in global configuration mode. To disable this AAA Radius attribute, use the **no** form of this command.

aaa radius attribute {**called-station-id** {**format** *format_name*| **type** *value*}| **calling-station-id** {**format** *format_name*| **type** *value*}| **nas-port** {**format e** *format_name*| **type** *value*}| **nas-port-id** {**format e** *format_name*| **type** *value*}}

no aaa radius attribute {**called-station-id** {**format** *format_name*| **type** *value*}| **calling-station-id** {**format** *format_name*| **type** *value*}| **nas-port** {**format e** *format_name*| **type** *value*}| **nas-port-id** {**format e** *format_name*| **type** *value*}}

Syntax Description

called-station-id	Specifies the AAA nas-port attribute.
calling-station-id	Specifies the AAA nas-port attribute.
nas-port	Specifies the AAA nas-port attribute.
nas-port-id	Specifies the AAA nas-port-id attribute.
format	Specifies the AAA nas-port attribute format.
e	Specifies the AAA format type.
format_name	Specifies a 32 character string representing the format to be used.
type	Specifies the AAA nas-port attribute format.
value	Specifies the Nas-Port-Type value to apply format string on. The nas port value ranges from 0-44.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
ip-services	read, write

Examples

This is an example of configuring the **aaa radius attribute** command in the global configuration mode:

```
RP/0/RSP0/CPU0:router(config)# aaa radius attribute format e red type 40
```

aaa service-accounting

To set accounting parameters for service, use the **aaa service-accounting** command in global configuration mode or administration configuration mode. To disable this behavior, use the **no** form of this command.

aaa service-accounting [**extended** | **brief**]

no aaa service-accounting [**extended** | **brief**]

Syntax Description

extended	Sends extended service accounting records.
brief	Sends brief service accounting records.

Command Default

The default setting is **extended**.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

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

The **extended** keyword allows to report all the subscriber accounting identities and state attributes within all the service accounting records. While, the **brief** keyword allows to report only brief information about service accounting records without any parent accounting record details.

Task ID

Task ID	Operation
aaa	read, write

Examples

This example shows how to set service accounting parameters to send brief information about service accounting records:

```
RP/0/RSP0/CPU0:router(config)# aaa service-accounting brief
```

Related Commands

Command	Description
aaa accounting subscriber, on page 9	Creates an accounting list for subscriber accounting.
aaa accounting service, on page 7	Creates an accounting list for service accounting.

aaa server radius dynamic-author

To configure radius dynamic author server, use the**aaa server radius dynamic-author** command in global configuration mode or administration configuration mode. To disable this subscriber authentication method, use the **no** form of this command.

aaa server radius dynamic-author {**auth-type** {**all**| **any**| **session-key**}| **client** *hostname*| **ignore** {**server-key**| **session-key**}| **port** *port_number*| **server-key** {**0**| **7**| **line_number**}}

no aaa server radius dynamic-author

Syntax Description

auth-type	Represents the COA client authentication type.
all	Represents all the COA client authentication type.
any	Represents any COA client authentication type.
session-key	Specifies that the session-key could be ignored.
client	Represents the COA client configuration.
ignore	Specifies the ignore options.
port	Specifies the COA server port to listen on.
server-key	Sets the shared secret to verify client COA requests.
port_number	Represents the port number and the value ranges from 1000 to 5000.
0	Specifies that the unencrypted key will follow.
7	Specifies that the encrypted key will follow.
line_number	Represents the unencrypted (cleartext) key.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.
Release 4.2.1	The support for the keywords, **auth-key** and **ignore {session-key}** were removed.

Usage Guidelines

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

Task ID

Task ID	Operation
aaa	read, write

Examples

```
RP/0/RSP0/CPU0:router(config)# aaa server radius dynamic-author ignore server-key
```

Related Commands

Command	Description
show radius (BNG), on page 57	Displays all trace data for AAA sub-system.
show aaa trace, on page 55	Displays the tunnel-related information.

aaa radius attribute nas-port-type

To configure the AAA RADIUS attribute nas-port-type for a physical interface or a VLAN sub-interface, use the **aaa radius attribute nas-port-type** command in the interface configuration mode. To remove the configuration of nas-port-type from the interface or VLAN sub-interface, use the **no** form of this command.

aaa radius attribute nas-port-type {*value* | *string*}

no aaa radius attribute nas-port-type

Syntax Description

value	The nas-port-type value for the interface or VLAN sub-interface. The range is from 0 to 44.
string	The nas-port-type name for the interface or VLAN sub-interface.

Command Default

None

Command Modes

Interface or VLAN sub-interface configuration

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

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

The permissible values for nas-port-type within the given range are 0 - 6, 9, 15 and 30 - 44.

Task ID

Task ID	Operation
aaa	read, write

Examples

This example shows how to configure the AAA RADIUS attribute, **nas-port-type** for each physical interface :

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitEthernet 0/0/0/0
RP/0/RSP0/CPU0:router(config-if)# aaa radius attribute nas-port-type 15
```

Related Commands

Command	Description
aaa radius attribute, on page 23	Configures a format e encode string for particular interface or NAS-Port type.

radius-server attribute

To customize the selected radius attributes, use the **radius-server attribute** command in the global configuration mode. To disable the Radius server attribute, use the **no** form of this command.

radius-server attribute list *list_name* [**attribute** {*list*| **vendor-id** *value*}]

no radius-server attribute list *list_name* [**attribute** {*list*| **vendor-id** *value*}]

Syntax Description

list	Specifies a list of attributes that are used in conjunction with server-groups to accept or reject a list of attributes.
list_name	Specifies the list name.
attribute	Specifies a list of Radius attributes.
list	Specifies the list of comma-delimited Radius attributes.
vendor-id	Specifies the vendor-id of the RADIUS attribute.
value	Specifies the vendor-id value. The value ranges from 0 to 429496729.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
aaa	read, write

Examples This is an example of configuring the **radius-server attribute** command in the global configuration mode:

```
RP/0/RSP0/CPU0:router(config)# radius-server attribute list list1
RP/0/RSP0/CPU0:router(config-attribute-filter)# attribute list_1
RP/0/RSP0/CPU0:router(config-attribute-filter)# radius-server attribute vendor-id 429
```

radius-server dead-criteria

To configure the dead server detection criteria for a configured RADIUS server, use the **radius-server dead-criteria** command in the global configuration mode. To disable the Radius server dead-criteria, use the **no** form of this command.

radius-server dead-criteria {**time** *value*| **tries** *number_of_tries*}

no radius-server dead-criteria {**time** *value*| **tries** *number_of_tries*}

Syntax Description

time	Specifies the minimum time that must elapse since a response was received from this RADIUS server.
value	Specifies the time in seconds. The value ranges from 1 to 120.
tries	Specifies the minimum number of transmissions (original attempts plus retransmits) to this RADIUS server.
number_of_tries	Specifies the number of tries. The range is from 1 to 100.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
aaa	read, write

Examples This is an example of configuring the **radius-server dead-criteria** command with 100s time and 34 tries:

```
RP/0/RSP0/CPU0:router(config)#radius-server dead-criteria time 100
RP/0/RSP0/CPU0:router(config)#radius-server dead-criteria tries 34
```

radius-server deadtime (BNG)

To improve RADIUS response times when some servers are unavailable and cause the unavailable servers to be skipped immediately, use the **radius-server deadtime** command. To set deadtime to 0, use the **no** form of this command.

radius-server deadtime *value*

no radius-server deadtime *value*

Syntax Description

value	Length of time, in minutes, for which a RADIUS server is skipped over by transaction requests, up to a maximum of 1440 (24 hours). The range is from 1 to 1440. The default value is 0.

Command Default

Dead time is set to 0.

Command Modes

Global configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.2.0	This command was supported on BNG.

Usage Guidelines

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

A RADIUS server marked as dead is skipped by additional requests for the duration of minutes unless all other servers are marked dead and there is no rollover method.

Task ID

Task ID	Operations
aaa	read, write

Examples

This example specifies five minutes of deadtime for RADIUS servers that fail to respond to authentication requests for the **radius-server deadtime** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server deadtime 5
```

radius-server disallow null-username

To drop radius access-requests that has blank or no username, use the **radius-server disallow null-username** command in the global configuration mode. To disable the Radius server disallow null-username, use the **no** form of this command.

radius-server disallow null-username

no radius-server disallow null-username

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
aaa	read, write

Examples

This is an example of configuring the **radius-server disallow null-username** command in the global configuration mode:

```
RP/0/RSP0/CPU0:router(config)#radius-server disallow null-username
```

radius-server host (BNG)

To specify a RADIUS server host, use the **radius-server host** command in global configuration mode. To delete the specified RADIUS host, use the **no** form of this command.

radius-server host *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

no radius-server host *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]

Syntax Description

ip-address	IP address of the RADIUS server host.
auth-port *port-number*	(Optional) Specifies the User Datagram Protocol (UDP) destination port for authentication requests; the host is not used for authentication if set to 0. If unspecified, the port number defaults to 1645.
acct-port *port-number*	(Optional) Specifies the UDP destination port for accounting requests; the host is not used for accounting if set to 0. If unspecified, the port number defaults to 1646.
timeout *seconds*	(Optional) The time interval (in seconds) that the router waits for the RADIUS server to reply before retransmitting. This setting overrides the global value of the **radius-server timeout** command. If no timeout value is specified, the global value is used. Enter a value in the range from 1 to 1000. Default is 5.
retransmit *retries*	(Optional) The number of times a RADIUS request is re-sent to a server, if that server is not responding or is responding slowly. This setting overrides the global setting of the **radius-server retransmit** command. If no retransmit value is specified, the global value is used. Enter a value in the range from 1 to 100. Default is 3.
key *string*	(Optional) Specifies the authentication and encryption key used between the router and the RADIUS server. This key overrides the global setting of the **radius-server key** command. If no key string is specified, the global value is used. The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host** command syntax. This is because the leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

Command Default

No RADIUS host is specified; use global **radius-server** command values.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.2.0	This command was supported on BNG.

Usage Guidelines

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

You can use multiple **radius-server host** commands to specify multiple hosts. The Cisco IOS XR software searches for hosts in the order in which you specify them.

If no host-specific timeout, retransmit, or key values are specified, the global values apply to each host.

Task ID

Task ID	Operations
aaa	read, write

Examples

This example shows how to establish the host with IP address 172.29.39.46 as the RADIUS server, use ports 1612 and 1616 as the authorization and accounting ports, set the timeout value to 6, set the retransmit value to 5, and set “rad123” as the encryption key, matching the key on the RADIUS server:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server host 172.29.39.46 auth-port 1612 acct-port
1616 timeout 6 retransmit 5 key rad123
```

To use separate servers for accounting and authentication, use the zero port value as appropriate.

Related Commands

Command	Description
aaa accounting subscriber	Creates a method list for accounting.
aaa authentication subscriber	Creates a method list for authentication.
aaa authorization subscriber	Creates a method list for authorization.
radius-server key (BNG), on page 42	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
radius-server retransmit (BNG), on page 46	Specifies how many times Cisco IOS XR software retransmits packets to a server before giving up.

Command	Description
radius-server timeout (BNG), on page 49	Sets the interval a router waits for a server host to reply.

radius-server ipv4 dscp

To mark the dscp bit for the ipv4 packets, use the **radius-server ipv4 dscp** command in the global configuration mode. To disable the Radius server IPv4 dscp, use the **no** form of this command.

radius-server ipv4 dscp *value*

no radius-server ipv4 dscp *value*

Syntax Description

value	Specifies the differentiated services codepoint value. The value ranges from 1 to 63.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
aaa	read, write

Examples

This is an example of configuring the **radius-server ipv4 dscp** command in the global configuration mode:

```
RP/0/RSP0/CPU0:router(config)#radius-server ipv4 dscp 34
```

radius-server key (BNG)

To set the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon, use the **radius-server key** command. To disable the key, use the **no** form of this command.

radius-server key {**0** *clear-text-key*| **7** *encrypted-key*| *clear-text-key*}

no radius-server key

Syntax Description

0 *clear-text-key*	Specifies an unencrypted (cleartext) shared key.
7 *encrypted-key*	Specifies a encrypted shared key.
clear-text-key	Specifies an unencrypted (cleartext) shared key.

Command Default

The authentication and encryption key is disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.2.0	This command was supported on BNG.

Usage Guidelines

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

The key entered must match the key used on the RADIUS server. All leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

Task ID

Task ID	Operations
aaa	read, write

Examples

This example shows how to set the cleartext key to “samplekey”:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server key 0 samplekey
```

This example shows how to set the encrypted shared key to “anykey”:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server key 7 anykey
```

radius-server load-balance

To configure the RADIUS load-balancing options, use the **radius-server load-balance** command in the global configuration mode. To disable the Radius server load-balance, use the **no** form of this command.

radius-server load-balance method least-outstanding [**batch-size** *value*| **ignore-preferred-server**]

no radius-server load-balance method least-outstanding

Syntax Description

method	Specifies the method by which the next host will be picked.
least-outstanding	Picks the server with the least transactions outstanding.
batch-size	Specifies the batch size for the selection of the server.
value	Specifies the batch size value. The value ranges from 1 to 1500. The default is 25.
ignore-preferred-server	Disables the preferred server for this server group.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
aaa	read, write

Examples

This is an example of configuring the **radius-server load-balance** command in the global configuration mode:

```
RP/0/RSP0/CPU0:router(config)#radius-server load-balance method lead-outstanding batch-size
 25
RP/0/RSP0/CPU0:router(config)#radius-server load-balance method lead-outstanding batch-size
 ignore-preferred-server
```

radius-server retransmit (BNG)

To specify the number of times the Cisco IOS XR software retransmits a packet to a server before giving up, use the **radius-server retransmit** command. The **no** form of this command sets it to the default value of 3 .

radius-server retransmit {*retries* **disable**}

no radius-server retransmit {*retries* **disable**}

Syntax Description

retries	Maximum number of retransmission attempts. The range is from 1 to 100. Default is 3.
disable	Disables the radius-server transmit command.

Command Default

The RADIUS servers are retried three times, or until a response is received.

Command Modes

Global configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.2.0	This command was supported on BNG.

Usage Guidelines

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

The RADIUS client tries all servers, allowing each one to time out before increasing the retransmit count.

Task ID

Task ID	Operations
aaa	read, write

Examples

This example shows how to specify a retransmit counter value of five times:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server retransmit 5
```

Related Commands

Command	Description
radius-server key (BNG), on page 42	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.

radius-server source-port

To configure the NAS to use a total of 50 ports as the source ports for sending out RADIUS requests, use the **radius-server source-port** command in the global configuration mode. To disable the Radius server source-port, use the **no** form of this command.

radius-server source-port extended

no radius-server source-port extended

Syntax Description

extended	Specifies that the source-port can be extended to 50.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

Having 200 source ports allows up to 256*200 authentication and accounting requests to be outstanding at one time. During peak call volume, typically when a router first boots or when an interface flaps, the extra source ports allow sessions to recover more quickly on large-scale aggregation platforms.

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

Task ID

Task ID	Operations
aaa	read, write

Examples

This is an example of configuring the **radius-server source-port** command in the global configuration mode:

```
RP/0/RSP0/CPU0:router(config)#radius-server source-port extended
```

radius-server timeout (BNG)

To set the interval for which a router waits for a server host to reply before timing out, use the **radius-server timeout** command. To restore the default, use the **no** form of this command.

radius-server timeout *seconds*

no radius-server timeout

Syntax Description

seconds	Number that specifies the timeout interval, in seconds. Range is from 1 to 1000.

Command Default

The default radius-server timeout value is 5 seconds.

Command Modes

Global configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.2.0	This command was supported on BNG.

Usage Guidelines

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

Use the **radius-server timeout** command to set the number of seconds a router waits for a server host to reply before timing out.

Task ID

Task ID	Operations
aaa	read, write

Examples

This example shows how to change the interval timer to 10 seconds:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server timeout 10
```

radius-server vsa attribute ignore unknown

To specify the unknown vsa ignore configuration for RADIUS server, use the **radius-server vsa attribute ignore unknown** command in the global configuration mode. To disable this feature, use the **no** form of this command.

radius-server vsa attribute ignore unknown

no radius-server vsa attribute ignore unknown

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
aaa	read, write

Examples

This is an example of configuring the **radius-server vsa attribute ignore unknown** command in the global configuration mode:

```
RP/0/RSP0/CPU0:router(config)#radius-server vsa attribute ignore unknown
```

radius-server throttle

To configure RADIUS throttling options for access and accounting to flow control the number of access and accounting requests sent to a RADIUS server, use the **radius-server throttle** command in the global configuration mode. To disable the radius server throttle, use the **no** form of this command.

radius-server throttle {**access** *value* {**access-timeout** *time*| **accounting** *value*}| **accounting** *acc_value*}

no radius-server throttle {**access** *value* {**access-timeout** *time*| **accounting** *value*}| **accounting** *acc_value*}

Syntax Description

access	Controls the number of access requests sent to a radius server.
value	Specifies the number of outstanding access requests after which throttling should be performed. The value ranges from 0 to 65535 and the preferred value 100.
access-timeout	Specifies the number of timeouts exceeding which a throttled access request is dropped.
time	Specifies the number of timeouts for a transaction. The default value is 3.
accounting	Controls the number of accounting requests sent to a radius server.
acc_value	Specifies the number of outstanding accounting transactions after which throttling should be performed. The value ranges from 0 to 65535 and the preferred value 100.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.2.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
aaa	read, write

Examples

This is an example of configuring the **radius-server throttle** command in the global configuration mode:

```
RP/0/RSP0/CPU0:router(config)# radius-server throttle access 10 access-timeout 5 accounting
 10
```

radius source-interface (BNG)

To force RADIUS to use the IP address of a specified interface or subinterface for all outgoing RADIUS packets, use the **radius source-interface** command. To prevent only the specified interface from being the default and not from being used for all outgoing RADIUS packets, use the **no** form of this command.

radius source-interface *interface* [**vrf** *vrf_name*]

no radius source-interface *interface*

Syntax Description

interface-name	Name of the interface that RADIUS uses for all of its outgoing packets.
vrf *vrf-id*	Specifies the name of the assigned VRF.

Command Default

If a specific source interface is not configured, or the interface is down or does not have an IP address configured, the system selects an IP address.

Command Modes

Global configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.2.0	This command was supported on BNG.

Usage Guidelines

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

Use the **radius source-interface** command to set the IP address of the specified interface or subinterface for all outgoing RADIUS packets. This address is used as long as the interface or subinterface is in the up state. In this way, the RADIUS server can use one IP address entry for every network access client instead of maintaining a list of IP addresses.

The specified interface or subinterface must have an IP address associated with it. If the specified interface or subinterface does not have an IP address or is in the down state, then RADIUS reverts to the default. To avoid this, add an IP address to the interface or subinterface or bring the interface to the up state.

The **radius source-interface** command is especially useful in cases in which the router has many interfaces or subinterfaces and you want to ensure that all RADIUS packets from a particular router have the same IP address.

Task ID

Task ID	Operations
aaa	read, write

Examples

This example shows how to make RADIUS use the IP address of subinterface s2 for all outgoing RADIUS packets:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius source-interface Loopback 10 vrf vrf-1
```

show aaa trace

To display all trace data for AAA sub-system, use the **show aaa trace** command in the EXEC mode.

show aaa trace [**basic**| **errors**| **file**| **func**| **hexdump**| **job**| **last**| **location**| **reverse**| **stats**| **tailf**| **unique**| **usec**| **verbose**| **wide**| **wrapping**]

Syntax Description

basic	Displays the data for AAA basic events.
errors	Displays the data for AAA client library errors.
file	Displays the specific file.
func	Displays the data for AAA function.
hexdump	Displays the traces in hexadecimal.
job	Displays the job ID.
last	Displays the last n entries.
location	Displays the card location.
reverse	Displays the latest traces first.
stats	Displays the statistics.
tailf	Displays the new traces as they were added.
unique	Displays the unique entries with counts.
verbose	Displays the internal debugging information.
wrapping	Displays the wrapping entries.
|	Displays the output modifiers.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
aaa	read

Examples

This is the sample output of the **show aaa trace** command:

```
RP/0/RSP0/CPU0:router# show aaa trace func
Tue Jan 15 07:59:10.381 UTC
4 wrapping entries (1088 possible, 64 allocated, 0 filtered, 4 total)
Jan 15 06:11:00.958 aaa/func 0/RSP0/CPU0 t5  ENTERING aaa_connect2
Jan 15 06:11:00.962 aaa/func 0/RSP0/CPU0 t5  ENTERING get_unique_context
Jan 15 06:11:00.963 aaa/func 0/RSP0/CPU0 t5  EXITTING get_unique_context
Jan 15 06:11:00.963 aaa/func 0/RSP0/CPU0 t5  EXITTING aaa_connect2
```

show radius (BNG)

To display the tunnel-related information, use the **show radius** command in the EXEC mode.

show radius [**accounting**| **authentication**| **dead-criteria**| **double-dip**| **location**| **server-groups**]

Syntax Description

accounting	Displays the RADIUS accounting data.
authentication	Displays the RADIUS authentication data.
dead-criteria	Displays the RADIUS dead-server detection criteria.
double-dip	Displays the RADIUS double-dip data.
location	Specifies the RADIUS instance location.
server-groups	Displays the RADIUS server group information.
|	Displays the output modifiers.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	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.

Task ID

Task ID	Operation
aaa	read

Examples

This is the sample output of the **show radius** command:

```
RP/0/RSP0/CPU0:router#show radius | file tftp: vrf vrf1 |
```

The show radius output is as follows:

```
Wed Mar  7 19:22:40.392 IST
Global dead time: 0 minute(s)
Number of Servers:2

Server: 10.1.0.3/1645/1646  is UP
  Total Deadtime: 0s Last Deadtime: 0s
  Timeout: 5 sec, Retransmit limit: 3
  Quarantined: No
  Authentication:
    1 requests, 0 pending, 0 retransmits
    1 accepts, 0 rejects, 0 challenges
    0 timeouts, 0 bad responses, 0 bad authenticators
    0 unknown types, 0 dropped, 50 ms latest rtt
    Throttled: 0 transactions, 0 timeout, 0 failures
    Estimated Throttled Access Transactions: 0
    Maximum Throttled Access Transactions: 0

    Automated TEST Stats:
        0 requests, 0 timeouts, 0 response, 0 pending
  Accounting:
    1 requests, 0 pending, 0 retransmits
    1 responses, 0 timeouts, 0 bad responses
    0 bad authenticators, 0 unknown types, 0 dropped
    189 ms latest rtt
    Throttled: 0 transactions, 0 timeout, 0 failures
    Estimated Throttled Accounting Transactions: 0
    Maximum Throttled Accounting Transactions: 0

    Automated TEST Stats:
        0 requests, 0 timeouts, 0 response, 0 pending

Server: 1.1.1.1/1645/1646  is UP
  Total Deadtime: 0s Last Deadtime: 0s
  Timeout: 5 sec, Retransmit limit: 3
  Quarantined: No
  Authentication:
    0 requests, 0 pending, 0 retransmits
    0 accepts, 0 rejects, 0 challenges
    0 timeouts, 0 bad responses, 0 bad authenticators
    0 unknown types, 0 dropped, 0 ms latest rtt
    Throttled: 0 transactions, 0 timeout, 0 failures
    Estimated Throttled Access Transactions: 0
    Maximum Throttled Access Transactions: 0

    Automated TEST Stats:
        0 requests, 0 timeouts, 0 response, 0 pending
  Accounting:
    0 requests, 0 pending, 0 retransmits
    0 responses, 0 timeouts, 0 bad responses
    0 bad authenticators, 0 unknown types, 0 dropped
    0 ms latest rtt
    Throttled: 0 transactions, 0 timeout, 0 failures
    Estimated Throttled Accounting Transactions: 0
    Maximum Throttled Accounting Transactions: 0

    Automated TEST Stats:
        0 requests, 0 timeouts, 0 response, 0 pending

RP/0/RSP0/CPU0:router# show rad server-groups SG1

Server group 'SG1' has 1 server(s)
  VRF  (id 0x0)
  Dead time: 0 minute(s) (inherited from global)
```

```
  Contains 1 server(s)
Server 10.1.0.3/1645/1646
  Authentication:
    1 requests, 0 pending, 0 retransmits
    1 accepts, 0 rejects, 0 challenges
    0 timeouts, 0 bad responses, 0 bad authenticators
    0 unknown types, 0 dropped, 50 ms latest rtt
    Throttled: 0 transactions, 0 timeout, 0 failures
    Estimated Throttled Access Transactions: 0
    Maximum Throttled Access Transactions: 0

    Automated TEST Stats:
        0 requests, 0 timeouts, 0 response, 0 pending
  Accounting:
    1 requests, 0 pending, 0 retransmits
    1 responses, 0 timeouts, 0 bad responses
    0 bad authenticators, 0 unknown types, 0 dropped
    189 ms latest rtt
    Throttled: 0 transactions, 0 timeout, 0 failures
    Estimated Throttled Accounting Transactions: 0
    Maximum Throttled Accounting Transactions: 0

    Automated TEST Stats:
        0 requests, 0 timeouts, 0 response, 0 pending
```

This table describes the significant fields shown in the display.

Table 2: show radius Field Descriptions

Field	Description
Server	Server IP address/UDP destination port for authentication requests/UDP destination port for accounting requests.
Timeout	Number of seconds the router waits for a server host to reply before timing out.
Retransmit limit	Number of times the Cisco IOS XR software searches the list of RADIUS server hosts before giving up.
Deadtime	Length of time in minutes for a RADIUS server to remain marked dead.

show radius server-groups detail

To display the detailed summary of the RADIUS server group information, use the **show radius server-groups detail** command in the EXEC mode.

show radius server-groups *server_group_name* **detail**

Syntax Description

server_group_name	Specifies the name of the RADIUS server group.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
aaa	read

Examples

This is sample output of the **show radius server-groups detail** command:

```
RP/0/RSP0/CPU0:router# show radius server-groups SG1 detail
Wed Jan 18 06:04:59.432 EST

Server group 'SG1' has 1 server(s)
  VRF  (id 0x0)
  Dead time: 0 minute(s) (inherited from global)
  Contains 1 server(s)
Server 99.0.0.10/1812/1813
  Authentication:
    100 requests, 0 pending, 0 retransmits
    100 accepts, 0 rejects, 0 challenges
    0 timeouts, 0 bad responses, 0 bad authenticators
    0 unknown types, 0 dropped, 0 ms latest rtt
    Throttled: 0 transactions, 0 timeout, 0 failures
    Estimated Throttled Access Transactions: 0
```

```
    Maximum Throttled Access Transactions: 0

    Automated TEST Stats:
        0 requests, 0 timeouts, 0 response, 0 pending
```

This table describes the significant fields shown in the display.

Table 3: show radius Field Descriptions

Field	Description
Server	Server IP address/UDP destination port for authentication requests/UDP destination port for accounting requests.
Deadtime	Length of time in minutes for a RADIUS server to remain marked dead.
Authentication	Specifies the authentication details.
Automated TEST Stats	Specifies the total time taken for sending requests, total timeouts, and the response time.

statistics period service-accounting

To set collection period for statistics collectors, use the **statistics period service-accounting** command in global configuration mode or administration configuration mode. To disable this behavior, use the **no** form of this command.

statistics period service-accounting {*period*| **disable**}

no statistics period service-accounting {*period*| **disable**}

Syntax Description

period	Collection period in seconds. The range is from 30 to 3600. The default is 900.
disable	Disables periodic statistics collection.

Command Default

Default collection period is 900 seconds.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
diag	read, write

Examples

This example shows how to change the collection period or polling interval for statistics collector:

```
RP/0/RSP0/CPU0:router(config)# statistics period service-accounting 2000
```

Related Commands

Command	Description
aaa accounting subscriber, on page 9	Creates an accounting list for subscriber accounting.
aaa accounting service, on page 7	Creates an accounting list for service accounting.

ACL and ABF Commands

This module describes the Cisco IOS XR software commands used to configure the ACL and ABF commands for Broadband Network Gateway (BNG) on the Cisco ASR 9000 Series Router. For details regarding the related configurations, refer to the *Cisco ASR 9000 Series Aggregation Services Router Broadband Network Gateway Configuration Guide*.

- ipv4 access-group (BNG), page 66
- ipv4 access-list (BNG), page 69
- ipv6 access-group (BNG), page 71
- ipv6 access-list (BNG), page 73

ipv4 access-group (BNG)

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

ipv4 access-group *access-list-name* {**common** *acl-p* {[*acl1* **ingress [hardware-count] [interface-statistics]**]| **ingress**}| *acl1* {**ingress**| **egress**} **[hardware-count] [interface-statistics]**}

no ipv4 access-group *access-list-name* {**common** *acl-p* {[*acl1* **ingress [hardware-count] [interface-statistics]**]| **ingress**}| *acl1* {**ingress**| **egress**} **[hardware-count] [interface-statistics]**}

Syntax Description

access-list-name	The name of the ipv4 access list as specified by the ipv4 access-list command.
common	The name of the common ACL. Common ACL is only supported on the ingress direction.
ingress	Filters on inbound packets.
egress	Filters on outbound packets.
hardware-count	(Optional) Specifies to access a group's hardware counters.
interface-statistics	(Optional) Specifies per-interface statistics in the hardware. Not available for common ACL.

Command Default

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

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 4.1.1	This command was introduced.
Release 4.2.0	This command was supported in the dynamic template configuration mode for BNG.

Usage Guidelines

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

Use the **ipv4 access-group** command to control access to an interface. To remove the specified access group, use the **no** form of the command. Use the *access-list-name* argument to specify a particular IPv4 access list.

Use the **ingress** keyword to filter on inbound packets or the egress keyword to filter on outbound packets. Use the *hardware-count* argument to enable hardware counters for the access group.

Permitted packets are counted only when hardware counters are enabled using the hardware-count argument. Denied packets are counted whether hardware counters are enabled or not.

To enter the dynamic template configuration mode, run **dynamic-template** command in the global configuration mode.

Note Under the dynamic template configuration mode, only the **egress** and **ingress** keywords are displayed.

Note For packet filtering applications using the ipv4/ipv6 access-group command, packet counters are maintained in hardware for each direction. If an access group is used on multiple interfaces in the same direction, then packets are counted for each interface that has the hardware-count argument enabled.

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.

By default, the unique or per-interface ACL statistics are disabled.

Task ID

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

Examples

This is an example of the show access-lists command:

```
RP/0/RSP0/CPU0:router# show access-lists
ipv4 access-list acl-common
 10 permit ipv4 host 205.205.205.1 host 200.175.175.1 log-input
 15 deny ipv4 any host 200.175.175.1
 20 permit ipv4 host 205.205.205.1 host 201.175.175.1 log-input
 25 deny ipv4 any host 201.175.175.1
 30 permit ipv4 host 205.205.205.1 host 202.175.175.1 log-input
 35 deny ipv4 any host 202.175.175.1
ipv4 access-list acl-unique1
 10 permit ipv4 host 205.205.205.1 host 203.175.175.1 log-input
```

```
 15 deny ipv4 any host 203.175.175.1

 20 permit ipv4 any any

ipv4 access-list ssm-acl

 10 permit ipv4 232.0.0.0 0.255.255.255 any log
```

This is an example of a configured IPv4 ACL in the dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv4 access-group a1 egress
```

ipv4 access-list (BNG)

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

ipv4 access-list *name*

no ipv4 access-list *name*

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

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.3.0	This command was supported in BNG.

Usage Guidelines

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

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 **resequence access-list ipv4** command if you want 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.

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:

```
RP/0/RSP0/CPU0:router(config)# ipv4 access-list Internetfilter
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 10 permit 192.168.34.0 0.0.0.255
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 20 permit 172.16.0.0 0.0.255.255
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 30 permit 10.0.0.0 0.255.255.255
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 39 remark Block BGP traffic from 172.16 net.
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 40 deny tcp host 172.16.0.0 eq bgp host
192.168.202.203 range 1300 1400
```

ipv6 access-group (BNG)

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**| **egress**} **[interface-statistics]**

no ipv6 access-group *access-list-name* {**ingress**| **egress**} **[interface-statistics]**

Syntax Description

access-list-name	Name of an IPv6 access list as specified by an **ipv6 access-list** command.
ingress	Filters on inbound packets.
egress	Filters on outbound packets.
interface-statistics	(Optional) Specifies per-interface statistics in the hardware.

Command Default

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

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.3.0	Support for IPv6 ACL on L2 transport interface was added.

Usage Guidelines

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

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

Use the **ipv6 access-group** command to control access to an interface. To remove the specified access group, use the **no** form of the command. Use the *access-list-name* to specify a particular IPv6 access list. Use the**ingress** keyword to filter on inbound packets or the **egress** keyword to filter on outbound packets.

Filtering of MPLS packets through common ACL and interface ACL is not supported.

Note For packet filtering applications using the **ipv6 access-group** command, packet counters are maintained in hardware for each direction. If an access group is used on multiple interfaces in the same direction, then packets are counted for each interface.

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 a rate-limited Internet Control Message Protocol (ICMP) host unreachable message.

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

By default, the unique or per-interface ACL statistics are disabled.

Task ID

Task ID	Operations
acl	read, write
ipv6	read, write

Examples

This example shows how to apply filters on packets inbound and outbound from GigabitEthernet interface 0/2/0/2:

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/2
RP/0/RSP0/CPU0:router(config-if)# ipv6 access-group p-in-filter ingress
RP/0/RSP0/CPU0:router(config-if)# ipv6 access-group p-out-filter egress
```

This example shows how to apply filters on packets inbound and outbound from GigabitEthernet interface 0/2/0/2:

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/2
RP/0/RSP0/CPU0:router(config-if)# ipv6 access-group p-in-filter ingress
RP/0/RSP0/CPU0:router(config-if)# ipv6 access-group p-out-filter egress
```

This example shows how to apply per-interface statistics in the hardware:

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/2
RP/0/RSP0/CPU0:router(config-if)# ipv6 access-group p-in-filter ingress interface-statistics
```

ipv6 access-list (BNG)

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*

no ipv6 access-list *name*

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 3.7.2	This command was introduced.
Release 4.3.0	Support for IPv6 ACL on L2 transport interface was added.

Usage Guidelines

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

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 global configuration 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 outbound traffic on interface GigabitEthernet 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 GigabitEthernet 0/2/0/2. The second entry in the ACL permits all other traffic to exit out of interface GigabitEthernet 0/2/0/2. The second entry is necessary because an implicit deny all condition is at the end of each IPv6 ACL.

```
RP/0/RSP0/CPU0:router(config)# ipv6 access-list list2
RP/0/RSP0/CPU0:router(config-ipv6-acl)# 10 deny fec0:0:0:2::/64 any
RP/0/RSP0/CPU0:router(config-ipv6-acl)# 20 permit any any

RP/0/RSP0/CPU0:router# show ipv6 access-lists list2

ipv6 access-list list2
```

```
  10 deny ipv6 fec0:0:0:2::/64 any
  20 permit ipv6 any any

RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/2
RP/0/RSP0/CPU0:router(config-if)# ipv6 access-group list2 egress
```

Note IPv6 is automatically configured as the protocol type in **permit any any** and **deny any any** statements that are translated from global configuration 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).

Address Pool Service Commands

This chapter describes the Cisco IOS XR software Address Pool Service commands for Broadband Network Gateway (BNG). For details regarding related configurations, refer to the *Cisco ASR 9000 Series Aggregation Services Router Broadband Network Gateway Configuration Guide*.

- address-range, page 78
- exclude, page 80
- network (BNG), page 82
- prefix-length, page 84
- prefix-range, page 86
- pool vrf, page 88
- pool ipv4, page 90
- pool ipv6, page 92
- utilization-mark, page 94
- show pool ipv4 name, page 96
- show pool ipv6 name, page 100
- show pool vrf, page 107

address-range

To specify address range for allocation, use the **address-range** command in Pool IPv4 or IPv6 configuration submode. To remove the address range, use the **no** form of this command.

address-range *first_range last_range*

no address-range *first_range last_range*

Syntax Description

first_range	Specifies the first address in range from which the IP addresses can be assigned to clients.
last_range	Specifies the last address in range until which the IP addresses can be assigned to clients.

Command Default

None

Command Modes

Pool IPv4 configuration

Pool IPv6 configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.
Release 4.3.0	Support for **IPv6** was added.

Usage Guidelines

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

You should only specify the addresses that are assignable to clients in a particular subnet. The interface and broadcast addresses should not be included in the address-range configuration.

Use the **pool ipv4** command to enter IPv4 pool configuration submode and **pool ipv6** command to enter IPv6 pool configuration submode.

Multiple address-ranges are allowed within a pool.

Task ID

Task ID	Operation
ip-services	read, write

Examples

This is an example of configuring the **address-range** command for IPv4 in the global configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pool vrf vrf1 ipv4 pool2
RP/0/RSP0/CPU0:router(config-pool-ipv4)# address-range 11.11.11.11 14.14.14.14
```

This is an example of configuring the **address-range** command for IPv6 in the global configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pool vrf vrf1 ipv6 pool3
RP/0/RSP0/CPU0:router(config-pool-ipv6)# address-range 2001::1 2001::100
```

Related Commands

Command	Description
pool ipv4, on page 90	Enables distributed address pool service on ipv4.
pool vrf, on page 88	Enables distributed address pool service on vrf.
exclude, on page 80	Specifies a range of IP addresses that distributed address pool service should not assign to clients.

exclude

To specify a range of IPv4 or Pv6 addresses that distributed address pool service (DAPS) must not assign to clients, use the **exclude** command in Pool IPv4 or IPv6 configuration submode. To remove the excluded IP addresses, use the **no** form of this command.

exclude {*first_address*| *last_address*}

no exclude {*first_address*| *last_address*}

Syntax Description

first_address	Specifies the first address in the range that needs to be excluded for IPv4 and specifies the first address or prefix in the range for IPv6.
last_address	Specifies the last address in the range that needs to be excluded and specifies the last address or prefix in the range for IPv6.

Command Default

None

Command Modes

Pool IPv4 configuration

Pool IPv6 configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.
Release 4.3.0	Support for **IPv6** was added.

Usage Guidelines

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

Use the **pool ipv4** command to enter IPv4 pool configuration submode and **pool ipv6** command to enter IPv6 pool configuration submode.

The low IP address cannot overlap with the IP address of a reserved address command. Multiple exclude commands are allowed within a pool. To exclude a single address, <highIpAddress> can be omitted.

Note The **exclude** command can be configured along with the **network**, **address-range**, and the **prefix-range** commands.

Task ID

Task ID	Operation
ip-services	read, write

Examples

This is an example to configure the **exclude** command for IPv4:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pool vrf vrf1 ipv4 pool2
RP/0/RSP0/CPU0:router(config-pool-ipv4)# exclude 10.10.10.1 10.10.10.10
```

This is an example to configure the **exclude** command for IPv6:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pool vrf vrf1 ipv6 pool3
RP/0/RSP0/CPU0:router(config-pool-ipv6)# exclude 2001::1
```

Related Commands

Command	Description
pool ipv4, on page 90	Enables distributed address pool service on IPv4.
pool vrf, on page 88	Enables distributed address pool service on vrf.
network (BNG), on page 82	Specifies a set of addresses or prefixes inside a subnet.

network (BNG)

To specify a set of addresses or prefixes inside a subnet, use the **network** command in Pool IPv4 or IPv6 configuration submode. To remove the addresses or prefixes, use the **no** form of this command.

network {*IPv4_subnet/length* [**default-router** *default-router-address*]| *IPv6_subnet/length*}

no network {*IPv4_subnet/length* [**default-router** *default-router-address*]| *IPv6_subnet/length*}

Syntax Description

IPv4_subnet	Specifies the decimal representation of the IPv4 subnet mask.
IPv6_subnet	Specifies the hexadecimal value for the IPv6 subnet mask.
length	Specifies the length of the prefix. **Note** The prefix length must be a maximum of 16 bit more than the subnet mask.
default-router	(Optional) Specifies the default-gateway address for the subnet.
default-router-address	IPv4 address of the default-gateway.

Command Default

None

Command Modes

Pool IPv4 configuration

Pool IPv6 configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.
Release 4.3.0	Support for **IPv6** was added.
Release 5.1	Support for IPv4 **default-router** was added.

Usage Guidelines

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

Use the **pool ipv4** command to enter IPv4 pool configuration submode and **pool ipv6** command to enter IPv6 pool configuration submode.

The **prefix-length** command must be configured whenever the **network** command is used. The **prefix-length** must be configured to 128 to signify singleton addresses and a smaller value to signify IPv6 prefixes. The number of addresses or prefixes that can be allocated by DAPS can become huge when this command is used. The prefix-length command should be configured to a number that limits the number of addresses or prefixes for each pool to 64K.

The prefix is written as the first address of a network, followed by a slash character (/) , and ends with the bit-length of the prefix. For example, 192.168.1.0/24 is the prefix of the IPv4 network starting at the given address, having 24 bits allocated for the network prefix, and the remaining 8 bits reserved for host addressing. The IPv6 address specification 2001:db8::/32 is a large network with 2 ^{96} addresses, having a 32-bit routing prefix. In IPv4 the routing prefix is also specified in the form of the subnet mask, which is expressed in quad-dotted decimal representation like an address. For example, 255.255.255.0 is the network mask for the 192.168.1.0/24 prefix.

The **default-router** option is supported only for IPv4 pools. The configured default-gateway address is automatically excluded from allocation to clients, if the address is within the subnet range.

Task ID

Task ID	Operation
ip-services	read, write

Examples

This is an example of configuring the **network** command for IPv4:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pool vrf vrf1 ipv4 pool2
RP/0/RSP0/CPU0:router(config-pool-ipv4)# network 11.11.11.0/24 default-router 11.11.11.11
```

This is an example of configuring the **network** command for IPv6:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pool vrf vrf1 ipv6 pool3
RP/0/RSP0/CPU0:router(config-pool-ipv6)# network 10:1:1::/50
```

Related Commands

Command	Description
pool ipv4, on page 90	Enables distributed address pool service on ipv4.
pool vrf, on page 88	Enables distributed address pool service on vrf.
prefix-length, on page 84	Specifies the length of the prefix that is assigned to the client.

prefix-length

To specify the length of the prefix that is assigned to the client, use the **prefix-length** command in IPv6 configuration submode. To remove the length of the prefix, use the **no** form of this command.

prefix-length *prefix_length*

no prefix-length *prefix_length*

Syntax Description

prefix_length	Specifies the length of the prefix.

Command Default

None

Command Modes

Pool IPv6 configuration

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

Use the **pool ipv6** command to enter ipv6 pool configuration submode.

The **prefix-length** command under the pool ensures all the prefixes (described in the **prefix-range** section) in the pool have the same length. The **prefix-length** command must be configured when the **network** and the **prefix-length** commands are used.

Task ID

Task ID	Operation
ip-services	read, write

Examples

This is an example of configuring the **prefix-length** command in the IPv6 configuration submode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pool vrf vrf1 ipv6 pool3
RP/0/RSP0/CPU0:router(config-pool-ipv6)# prefix-length 50
```

Related Commands

Command	Description
pool ipv4, on page 90	Enables distributed address pool service on ipv4.
pool vrf, on page 88	Enables distributed address pool service on vrf.
network (BNG), on page 82	Specifies a set of addresses or prefixes inside a subnet.

prefix-range

To specify a range of IPv6 address prefixes, use the **prefix-range** command in IPv6 configuration submode. To remove the range of prefixes, use the **no** form of this command.

prefix-range {*first_ipv6_range*| *last_ipv6_range*}

no prefix-range {*first_ipv6_range*| *last_ipv6_range*}

Syntax Description

first_ipv6_range	Specifies the first IPv6 in the prefix range.
last_ipv6_range	Specifies the last IPv6 in the prefix range.

Command Default

None

Command Modes

Pool IPv6 configuration

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

Use the **pool ipv6** command to enter IPv6 pool configuration submode.

Multiple prefix-ranges are allowed within a pool. The length of the prefix in any pool is the same for all prefix's and this is imposed by the **prefix-length** command. The **prefix-length** has to be mandatorily configured whenever **prefix-range** is configured.

Task ID

Task ID	Operation
ip-services	read, write

Examples

This is an example of configuring the **prefix-range** command in IPv6 configuration submode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pool vrf vrf1 ipv6 pool3
RP/0/RSP0/CPU0:router(config-pool-ipv6)# prefix-range 1001:1:1:1:: 1001:1:1:10::
```

Related Commands

Command	Description
pool ipv4, on page 90	Enables distributed address pool service on ipv4.
pool vrf, on page 88	Enables distributed address pool service on vrf.
prefix-length, on page 84	Specifies the length of the prefix that is assigned to the client.

pool vrf

To enable distributed address pool service on a vrf and to enter the corresponding configuration submode, use the **pool vrf** command in the global configuration mode. To disable this feature, use the **no** form of this command.

pool vrf {*vrf_name*| **all**} {**ipv4**| *pool_name*| **ipv6**| *pool_name*}

no pool vrf {*vrf_name*| **all**} {**ipv4**| *pool_name*| **ipv6**| *pool_name*}

Syntax Description

vrf_name	Specifies the name of the vrf.
ipv4	Specifies IPv4 pool name. Each pool must have a unique name across all VRFs.
ipv6	Specifies IPv6 pool name. Each pool must have a unique name across all VRFs.
pool_name	Specifies the name of the pool for IPv4 or IPv6.
all	Specifies the global pool.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.
Release 4.3.0	Support for **IPv6** was added.

Usage Guidelines

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

Use the **pool ipv4** command to enter IPv4 pool configuration submode and **pool ipv6** command to enter IPv6 pool configuration submode.

Note Each pool must have a unique name across all VRFs. For example, pool1 can not be created in both vrf1 and vrf2.

Some pools can be associated with all the VRFs and these pools are configured with the **all** keyword.

Task ID

Task ID	Operation
ip-services	read, write

Examples

This is an example of configuring the **pool vrf** command for IPv4 in the global configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pool vrf vrf1 ipv4 pool2
RP/0/RSP0/CPU0:router(config-pool-ipv4)#
```

This is an example of configuring the **pool vrf** command for IPv6 in the global configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pool vrf vrf1 ipv6 pool3
RP/0/RSP0/CPU0:router(config-pool-ipv6)#
```

Related Commands

Command	Description
pool ipv4, on page 90	Enables distributed address pool service on IPv4.
pool ipv6, on page 92	Enables distributed address pool service on IPv6.

pool ipv4

To enable distributed address pool service on IPv4 and to enter the pool IPv4 configuration submode, use the **pool ipv4** command in the global configuration mode. To disable this feature, use the **no** form of this command.

pool ipv4 *pool_name*

no pool ipv4 *pool_name*

Syntax Description

pool_name	Specifies the name of the IPv4 pool.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Use the **pool ipv4** command to enter IPv4 pool configuration submode.

Task ID

Task ID	Operation
ip-services	read, write

Examples

This is an example of configuring the **pool ipv4** command in the global configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pool ipv4 pool1
RP/0/RSP0/CPU0:router(config-pool-ipv4)# address-range 10.10.10.1 10.10.10.254
```

Related Commands

Command	Description
pool vrf, on page 88	Enables distributed address pool service on vrf.

Command	Description
exclude, on page 80	Specifies a range of IP addresses that distributed address pool service should not assign to clients.
address-range, on page 78	Specifies a range of IP addresses.

pool ipv6

To enable distributed address pool service on IPv6 and to enter the IPv6 pool configuration submode, use the **pool ipv6** command in the global configuration mode. To disable this feature, use the **no** form of this command.

pool ipv6 *pool_name*

no pool ipv6 *pool_name*

Syntax Description

pool_name	Specifies the IPv6 pool name.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

Use the **pool ipv6** command to enter IPv6 pool configuration submode.

Task ID

Task ID	Operation
ip-services	read, write

Examples

This is an example of configuring the **pool ipv6** command in the global configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pool ipv6 p6 prefix-length 45
RP/0/RSP0/CPU0:router(config-pool-ipv6)#
```

Related Commands

Command	Description
pool vrf, on page 88	Enables distributed address pool service on vrf.

utilization-mark

To specify a utilization threshold, use the **utilization-mark** command in Pool IPv4 or IPv6 configuration submode. To remove the utilization threshold, use the **no** form of this command.

utilization-mark {**high**| *high_value*| **low**| *low_value*}

no utilization-mark {**high**| *high_value*| **low**| *low_value*}

Syntax Description

high	Specifies the high mark in the threshold value.
high_value	Specifies the numerical value as percentage, for the low mark in the threshold.
low	Specifies the low mark in the threshold value.
low_value	Specifies the numerical value as percentage, for the low mark in the threshold.

Command Default

None

Command Modes

Pool IPv4 configuration

Pool IPv6 configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.
Release 4.3.0	Support for **IPv6** was added.

Usage Guidelines

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

Use the **pool ipv4** command to enter IPv4 pool configuration submode and **pool ipv6** command to enter IPv6 pool configuration submode.

When the utilization threshold is reached, a LOG_WARNING message is logged with syslog facility. The high and low values are entered as percentages between 0 and 100. The utilization is defined as the # allocated addresses or # total addresses.

Task ID

Task ID	Operation
ip-services	read, write

Examples

This is an example of configuring the **utilization-mark** command in Pool IPv4 configuration submode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pool vrf vrf1 ipv4 pool2
RP/0/RSP0/CPU0:router(config-pool-ipv4)# utilization-mark high 90 low 10
```

This is an example of configuring the **utilization-mark** command in Pool IPv6 configuration submode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pool vrf vrf1 ipv6 pool3
RP/0/RSP0/CPU0:router(config-pool-ipv6)# utilization-mark high 70 low 40
```

Related Commands

Command	Description
pool ipv4, on page 90	Enables distributed address pool service on ipv4.
pool vrf, on page 88	Enables distributed address pool service on vrf.
exclude, on page 80	Specifies a range of IP addresses that distributed address pool service should not assign to clients.

show pool ipv4 name

To display the status of an IPv4 pool, use the **show pool ipv4 name** command in the EXEC mode.

show pool ipv4 name *pool_name*{**location| verbose|** }

Syntax Description

pool_name	Specifies the name of the IPv4 pool.
location	Specifies the location of the IPv4 pool.
verbose	Displays all allocations for the pools.
|	Specifies the output modifiers.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	This command was introduced.
Release 4.3.0	Support for **IPv6** was added.

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.

Use the**pool ipv4** command to enter Pool IPv4 configuration submode.

Task ID

Task ID	Operation
ip-services	read

Examples

This is the sample output of the **show pool ipv4 name** command:

```
RP/0/RSP0/CPU0:router# show pool ipv4 name POOL1

              Pool POOL1 Allocations
-----------------------------------------------------
```

```
VRF: default
Pool Id: 30
Pool Scope: VRF Specific Pool
Prefix Length: 32

Used:           100
Excl:             0
Free:          7900
Total:         8000

Utilization:    1%

Range List:
-----------
Range Start        :  12.0.0.2
Range End          :  12.0.31.65
Used Addresses     :  100
Excluded Addresses :  0
Free Addresses     :  7900

RP/0/RSP0/CPU0:router# show pool ipv4 name POOL1 verbose

              Pool POOL1 Allocations
--------------------------------------------------
VRF: default
Pool Id: 30
Pool Scope: VRF Specific Pool
Prefix Length: 32

Used:           100
Excl:             0
Free:          7900
Total:         8000

Utilization:    1%

Range List:
-----------
Range Start        :  12.0.0.2
Range End          :  12.0.31.65
Used Addresses     :  100
Excluded Addresses :  0
Free Addresses     :  7900

In-Use Address List:
   12.0.0.2  PPP
   12.0.0.3  PPP
   12.0.0.4  PPP
   12.0.0.5  PPP
   12.0.0.6  PPP
   12.0.0.7  PPP
   12.0.0.8  PPP
   12.0.0.9  PPP
   12.0.0.10  PPP
   12.0.0.11  PPP
   12.0.0.12  PPP
   12.0.0.13  PPP
   12.0.0.14  PPP
   12.0.0.15  PPP
   12.0.0.16  PPP
   12.0.0.17  PPP
   12.0.0.18  PPP
   12.0.0.19  PPP
   12.0.0.20  PPP
   12.0.0.21  PPP
   12.0.0.22  PPP
   12.0.0.23  PPP
   12.0.0.24  PPP
   12.0.0.25  PPP
   12.0.0.26  PPP
   12.0.0.27  PPP
   12.0.0.28  PPP
   12.0.0.29  PPP
```

```
12.0.0.30  PPP
12.0.0.31  PPP
12.0.0.32  PPP
12.0.0.33  PPP
12.0.0.34  PPP
12.0.0.35  PPP
12.0.0.36  PPP
12.0.0.37  PPP
12.0.0.38  PPP
12.0.0.39  PPP
12.0.0.40  PPP
12.0.0.41  PPP
12.0.0.42  PPP
12.0.0.43  PPP
12.0.0.44  PPP
12.0.0.45  PPP
12.0.0.46  PPP
12.0.0.47  PPP
12.0.0.48  PPP
12.0.0.49  PPP
12.0.0.50  PPP
12.0.0.51  PPP
12.0.0.52  PPP
12.0.0.53  PPP
12.0.0.54  PPP
12.0.0.55  PPP
12.0.0.56  PPP
12.0.0.57  PPP
12.0.0.58  PPP
12.0.0.59  PPP
12.0.0.60  PPP
12.0.0.61  PPP
12.0.0.62  PPP
12.0.0.63  PPP
12.0.0.64  PPP
12.0.0.65  PPP
12.0.0.66  PPP
12.0.0.67  PPP
12.0.0.68  PPP
12.0.0.69  PPP
12.0.0.70  PPP
12.0.0.71  PPP
12.0.0.72  PPP
12.0.0.73  PPP
12.0.0.74  PPP
12.0.0.75  PPP
12.0.0.76  PPP
12.0.0.77  PPP
12.0.0.78  PPP
12.0.0.79  PPP
12.0.0.80  PPP
12.0.0.81  PPP
12.0.0.82  PPP
12.0.0.83  PPP
12.0.0.84  PPP
12.0.0.85  PPP
12.0.0.86  PPP
12.0.0.87  PPP
12.0.0.88  PPP
12.0.0.89  PPP
12.0.0.90  PPP
12.0.0.91  PPP
12.0.0.92  PPP
12.0.0.93  PPP
12.0.0.94  PPP
12.0.0.95  PPP
12.0.0.96  PPP
12.0.0.97  PPP
12.0.0.98  PPP
12.0.0.99  PPP
12.0.0.100  PPP
12.0.0.101  PPP
```

This table describes the significant fields shown in the display.

Table 4: show pool ipv4 name Field Descriptions

Field	Description
VRF	Specifies the VRF the pool is associated with.
Pool ID	The unique pool ID of a specific pool.
Pool Scope	Pool scope belongs to the VRF specific pool.
Prefix Length	Length of the prefix specified.

Related Commands

Command	Description
pool vrf, on page 88	Enables distributed address pool service on vrf.
pool ipv4, on page 90	Enables distributed address pool service on ipv4.
exclude, on page 80	Specifies a range of IP addresses that distributed address pool service should not assign to clients.
address-range, on page 78	Specifies a range of IP addresses.

show pool ipv6 name

To show the status of an IPv6 pool, use the **show pool ipv6 name** command in the EXEC mode.

show pool ipv6 name *pool_name*{**location| verbose|** }

Syntax Description

pool_name	Specifies the name of the IPv6 pool.
location	Specifies the location of the IPv6 pool.
verbose	Displays all allocations for the pools.
|	Specifies the output modifiers.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.3.0	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.

Use the**pool ipv6** command to enter Pool IPv6 configuration submode.

Task ID

Task ID	Operation
ip-services	read

Examples

This is the sample output for the **show pool ipv6 name** command:

```
RP/0/RSP0/CPU0:router# show pool ipv4 name POOL_A6_i_1
                Pool POOL_A6_i_1 Allocations
-------------------------------------------------
VRF: vrf1
Pool Id: 1
Pool Scope: VRF Specific Pool
```

```
Prefix Length: 128

Used:         15797
Excl:             0
Free:           203
Total:        16000

Utilization:    98%

Range List:
-----------
Range Start        :  19::2
Range End          :  19::3e81
Used Addresses     :  15797
Excluded Addresses :  0
Free Addresses     :  203

RP/0/RSP0/CPU0:router# show pool ipv6 name POOL_A6_i_1 verbose

              Pool POOL_A6_i_1 Allocations
--------------------------------------------------
VRF: vrf1
Pool Id: 1
Pool Scope: VRF Specific Pool
Prefix Length: 128

Used:         15797
Excl:             0
Free:           203
Total:        16000

Utilization:    98%

Range List:
-----------
Range Start        :  19::2
Range End          :  19::3e81
Used Addresses     :  15797
Excluded Addresses :  0
Free Addresses     :  203

In-Use Address List:
   19::2  DHCPV6
   19::3  DHCPV6
   19::4  DHCPV6
   19::5  DHCPV6
   19::6  DHCPV6
   19::7  DHCPV6
   19::8  DHCPV6
   19::9  DHCPV6
   19::a  DHCPV6
   19::b  DHCPV6
   19::c  DHCPV6
   19::d  DHCPV6
   19::e  DHCPV6
   19::f  DHCPV6
   19::10  DHCPV6
   19::11  DHCPV6
   19::12  DHCPV6
   19::13  DHCPV6
   19::14  DHCPV6
   19::15  DHCPV6
   19::16  DHCPV6
   19::17  DHCPV6
   19::18  DHCPV6
   19::19  DHCPV6
   19::1a  DHCPV6
   19::1b  DHCPV6
   19::1c  DHCPV6
   19::1d  DHCPV6
   19::1e  DHCPV6
   19::1f  DHCPV6
   19::20  DHCPV6
```

```
19::21  DHCPV6
19::22  DHCPV6
19::23  DHCPV6
19::24  DHCPV6
19::25  DHCPV6
19::26  DHCPV6
19::27  DHCPV6
19::28  DHCPV6
19::29  DHCPV6
19::2a  DHCPV6
19::2b  DHCPV6
19::2c  DHCPV6
19::2d  DHCPV6
19::2e  DHCPV6
19::2f  DHCPV6
19::30  DHCPV6
19::31  DHCPV6
19::32  DHCPV6
19::33  DHCPV6
19::34  DHCPV6
19::35  DHCPV6
19::36  DHCPV6
19::37  DHCPV6
19::38  DHCPV6
19::39  DHCPV6
19::3a  DHCPV6
19::3b  DHCPV6
19::3c  DHCPV6
19::3d  DHCPV6
19::3e  DHCPV6
19::3f  DHCPV6
19::40  DHCPV6
19::41  DHCPV6
19::42  DHCPV6
19::43  DHCPV6
19::44  DHCPV6
19::45  DHCPV6
19::46  DHCPV6
19::47  DHCPV6
19::48  DHCPV6
19::49  DHCPV6
19::4a  DHCPV6
19::4b  DHCPV6
19::4c  DHCPV6
19::4d  DHCPV6
19::4e  DHCPV6
19::4f  DHCPV6
19::50  DHCPV6
19::51  DHCPV6
19::52  DHCPV6
19::53  DHCPV6
19::54  DHCPV6
19::55  DHCPV6
19::56  DHCPV6
19::57  DHCPV6
19::58  DHCPV6
19::59  DHCPV6
19::5a  DHCPV6
19::5b  DHCPV6
19::5c  DHCPV6
19::5d  DHCPV6
19::5e  DHCPV6
19::5f  DHCPV6
19::60  DHCPV6
19::61  DHCPV6
19::62  DHCPV6
19::63  DHCPV6
19::64  DHCPV6
19::65  DHCPV6
19::66  DHCPV6
19::67  DHCPV6
19::68  DHCPV6
19::69  DHCPV6
```

```
19::6a  DHCPV6
19::6b  DHCPV6
19::6c  DHCPV6
19::6d  DHCPV6
19::6e  DHCPV6
19::6f  DHCPV6
19::70  DHCPV6
19::71  DHCPV6
19::72  DHCPV6
19::73  DHCPV6
19::74  DHCPV6
19::75  DHCPV6
19::76  DHCPV6
19::77  DHCPV6
19::78  DHCPV6
19::79  DHCPV6
19::7a  DHCPV6
19::7b  DHCPV6
19::7c  DHCPV6
19::7d  DHCPV6
19::7e  DHCPV6
19::7f  DHCPV6
19::80  DHCPV6
19::81  DHCPV6
19::82  DHCPV6
19::83  DHCPV6
19::84  DHCPV6
19::85  DHCPV6
19::86  DHCPV6
19::87  DHCPV6
19::88  DHCPV6
19::89  DHCPV6
19::8a  DHCPV6
19::8b  DHCPV6
19::8c  DHCPV6
19::8d  DHCPV6
19::8e  DHCPV6
19::8f  DHCPV6
19::90  DHCPV6
19::91  DHCPV6
19::92  DHCPV6
19::93  DHCPV6
19::94  DHCPV6
19::95  DHCPV6
19::96  DHCPV6
19::97  DHCPV6
19::98  DHCPV6
19::99  DHCPV6
19::9a  DHCPV6
19::9b  DHCPV6
19::9c  DHCPV6
19::9d  DHCPV6
19::9e  DHCPV6
19::9f  DHCPV6
19::a0  DHCPV6
19::a1  DHCPV6
19::a2  DHCPV6
19::a3  DHCPV6
19::a4  DHCPV6
19::a5  DHCPV6
19::a6  DHCPV6
19::a7  DHCPV6
19::a8  DHCPV6
19::a9  DHCPV6
19::aa  DHCPV6
19::ab  DHCPV6
19::ac  DHCPV6
19::ad  DHCPV6
19::ae  DHCPV6
19::af  DHCPV6
19::b0  DHCPV6
19::b1  DHCPV6
19::b2  DHCPV6
```

```
19::b3  DHCPV6
19::b4  DHCPV6
19::b5  DHCPV6
19::b6  DHCPV6
19::b7  DHCPV6
19::b8  DHCPV6
19::b9  DHCPV6
19::ba  DHCPV6
19::bb  DHCPV6
19::bc  DHCPV6
19::bd  DHCPV6
19::be  DHCPV6
19::bf  DHCPV6
19::c0  DHCPV6
19::c1  DHCPV6
19::c2  DHCPV6
19::c3  DHCPV6
19::c4  DHCPV6
19::c5  DHCPV6
19::c6  DHCPV6
19::c7  DHCPV6
19::c8  DHCPV6
19::c9  DHCPV6
19::ca  DHCPV6
19::cb  DHCPV6
19::cc  DHCPV6
19::cd  DHCPV6
19::ce  DHCPV6
19::cf  DHCPV6
19::d0  DHCPV6
19::d1  DHCPV6
19::d2  DHCPV6
19::d3  DHCPV6
19::d4  DHCPV6
19::d5  DHCPV6
19::d6  DHCPV6
19::d7  DHCPV6
19::d8  DHCPV6
19::d9  DHCPV6
19::da  DHCPV6
19::db  DHCPV6
19::dc  DHCPV6
19::dd  DHCPV6
19::de  DHCPV6
19::df  DHCPV6
19::e0  DHCPV6
19::e1  DHCPV6
19::e2  DHCPV6
19::e3  DHCPV6
19::e4  DHCPV6
19::e5  DHCPV6
19::e6  DHCPV6
19::e7  DHCPV6
19::e8  DHCPV6
19::e9  DHCPV6
19::ea  DHCPV6
19::eb  DHCPV6
19::ec  DHCPV6
19::ed  DHCPV6
19::ee  DHCPV6
19::ef  DHCPV6
19::f0  DHCPV6
19::f1  DHCPV6
19::f2  DHCPV6
19::f3  DHCPV6
19::f4  DHCPV6
19::f5  DHCPV6
19::f6  DHCPV6
19::f7  DHCPV6
19::f8  DHCPV6
19::f9  DHCPV6
19::fa  DHCPV6
19::fb  DHCPV6
```

```
19::fc  DHCPV6
19::fd  DHCPV6
19::fe  DHCPV6
19::ff  DHCPV6
19::100  DHCPV6
19::101  DHCPV6
19::102  DHCPV6
19::103  DHCPV6
19::104  DHCPV6
19::105  DHCPV6
19::106  DHCPV6
19::107  DHCPV6
19::108  DHCPV6
19::109  DHCPV6
19::10a  DHCPV6
19::10b  DHCPV6
19::10c  DHCPV6
19::10d  DHCPV6
19::10e  DHCPV6
19::10f  DHCPV6
19::110  DHCPV6
19::111  DHCPV6
19::112  DHCPV6
19::113  DHCPV6
19::114  DHCPV6
19::115  DHCPV6
19::116  DHCPV6
19::117  DHCPV6
19::118  DHCPV6
19::119  DHCPV6
19::11a  DHCPV6
19::11b  DHCPV6
19::11c  DHCPV6
19::11d  DHCPV6
19::11e  DHCPV6
```

This table describes the significant fields shown in the display.

Table 5: show pool ipv6 name Field Descriptions

Field	Description
VRF	Specifies the VRF the pool is associated with.
Pool ID	The unique pool ID of a specific pool.
Pool Scope	Pool scope belongs to the VRF specific pool.
Prefix Length	Length of the prefix specified.

Related Commands

Command	Description
pool vrf, on page 88	Enables distributed address pool service on vrf.
pool ipv6, on page 92	Enables distributed address pool service on ipv6.
exclude, on page 80	Specifies a range of IP addresses that distributed address pool service should not assign to clients.
address-range, on page 78	Specifies a range of IP addresses.

show pool vrf

To show the status of VRF pool, use the **show pool vrf** command in the EXEC mode.

show pool vrf *vrf_name*{**ipv4**|**ipv6**}

Syntax Description

vrf_name	Specifies the vrf name.
all	Displays all vrfs.
ipv4	Specifies the IPv4 pool.
ipv6	Specifies the IPv6 pool.
|	Specifies the output modifiers.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	This command was introduced.
Release 4.3.0	Support for **IPv6** was added.

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.

Use the **pool ipv4** command to enter IPv4 pool configuration submode and **pool ipv6** command to enter IPv6 pool configuration submode.

Task ID

Task ID	Operation
ip-services	read

Examples

This is the sample output of the **show pool vrf** command for IPv4:

```
RP/0/RSP0/CPU0:router# show pool vrf vrf1 ipv4

                  Allocation Summary
-----------------------------------------------------

Used: 0
Excl: 0
Free: 254
Total: 254
Utilization: 0%


 Pool Name    Pool ID      VRF      Used    Excl    Free   Total
-----------  ---------  ---------  ------  ------  ------ -------
     test1      4        vrf2          0       0    254    254
```

This is the sample output of the **show pool vrf** command for IPv6:

```
RP/0/RSP0/CPU0:router# show pool vrf vrf1 ipv6


                Allocation Summary
-----------------------------------------------------

Used: 2
Excl: 0
Free: 31999
Total: 32001
Utilization: 0%


 Pool Name    Pool ID      VRF      Used    Excl    Free   Total
-----------  ---------  ---------  ------  ------  ------ -------
POOL_A6_i_1      1        vrf1           1       0  15999  16000
POOL_P6_i_2      2        vrf1           1       0  15999  16000
      test      0        vrf1           0       0      1      1
```

This table describes the significant fields shown in the display.

Table 6: show pool ipv4 name Field Descriptions

Field	Description
VRF	Specifies the VRF the pool is associated with.
Pool ID	The unique pool ID of a specific pool.
Pool Name	The name of the IPv6 pool.

Related Commands

Command	Description
pool vrf, on page 88	Enables distributed address pool service on vrf.
pool ipv4, on page 90	Enables distributed address pool service on ipv4.

Command	Description
exclude, on page 80	Specifies a range of IP addresses that distributed address pool service should not assign to clients.
address-range, on page 78	Specifies a range of IP addresses.

Control Policy Commands

This module describes the Cisco IOS XR software commands used to configure the Control Policy commands for Broadband Network Gateway (BNG) on the Cisco ASR 9000 Series Router. For details regarding the related configurations, refer to the *Cisco ASR 9000 Series Aggregation Services Router Broadband Network Gateway Configuration Guide*.

- activate, page 112
- authenticate (BNG), page 114
- authorize, page 116
- class-map type control subscriber, page 118
- deactivate, page 120
- event, page 122
- match (class-map), page 124
- policy-map type control subscriber, page 126
- policy-map type pbr, page 128
- service-policy type control subscriber, page 130
- show class-map, page 132
- show policy-map, page 134

activate

To activate the dynamic template mode in the class map sub-configuration mode, use the **activate** command in the global configuration mode. To disable this feature, use the **no** form of this command.

activate dynamic-template *name* **aaa list** {*list_name*| **default**}

no activate

Syntax Description

dynamic-template	Specifies the actions related to dynamic templates.
name	Specifies the name of the dynamic template.
aaa	Specifies the AAA parameters.
list	Specifies the AAA method list that identifies the radius server from which to acquire the service definition.
default	Specifies the default AAA method list.
list_name	(Optional) Specifies the name of the AAA method list. If provided, the template is downloaded from radius. If not provided, then the template is expected to be locally configured.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
qos	read, write

Examples

This is an example of configuring the **activate** command in the global configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# policy-map type control subscriber PL1
RP/0/RSP0/CPU0:router(config-pmap)# event session-activate match-first
RP/0/RSP0/CPU0:router(config-pmap-e)# class type control subscriber CL2
RP/0/RSP0/CPU0:router(config-pmap-c)# 1 activate dynamic-template DL1 aaa list default
```

Related Commands

Command	Description
deactivate, on page 120	Deactivates the dynamic template mode in the class map sub-configuration mode.

authenticate (BNG)

To authenticate and specify the AAA method list that authentication should be made with in the class map sub-configuration mode, use the **authenticate** command in the global configuration mode. To disable the AAA method list authentication, use the **no** form of this command.

authenticate aaa list{*list_name*| **default**}

no authenticate

Syntax Description

aaa	Specifies the AAA parameters.
list	Specifies AAA method list that authentication should be made with.
default	Specifies the default AAA method list.
list_name	Specifies the name of the AAA method list.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
qos	read, write

Examples

This is an example of configuring the **authenticate** command in the global configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# policy-map type control subscriber PL1
RP/0/RSP0/CPU0:router(config-pmap)# event session-start match-first
```

```
RP/0/RSP0/CPU0:router(config-pmap-e)# class type control subscriber CL2
RP/0/RSP0/CPU0:router(config-pmap-c)# 1 authenticate aaa list default
```

authorize

To authenticate and specify the AAA method list that authorization should be made with in the class map sub-configuration mode, use the **authorize** command in the global configuration mode. To disable the AAA method list authorization, use the **no** form of this command.

authorize aaa list{*list_name*| **default**} {**format** *format_name* } | **identifier** {**circuit-id**| **remote-id**| **source-address-ipv4**| **source-address-mac**| **username**} {**password** | {**use-from-line**| *password*}}

no authorize

Syntax Description

aaa	Specifies the AAA parameters.
list	Specifies AAA method list that authorization should be made with.
default	Specifies the default AAA method list.
list_name	Specifies the name of the AAA method list.
format	Specifies an authorize format name.
format_name	Specifies to use format_name, which was defined using CLI 'aaa attribute format'. The result of format is used as user name in authorization request.
password	Specifies a password to be used for AAA request.
use-from-line	Specifies the line from which the password needs to be used.
password	Specifies a clear text password.
identifier	Specifies an authorize identifier.
circuit-id	Specifies to use circuit-id as the username in authorize request.
remote-id	Specifies to use remote-id as the username in authorize request. .
source-address-ipv4	Specifies to use source-address-ipv4 as the username in authorize request.
source-address-mac	Specifies to use source-address-mac as the username in authorize request.
username	Specifies an authorize username.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
qos	read, write

Examples

This is an example of configuring the **authorize** command in the global configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# policy-map type control subscriber PL1
RP/0/RSP0/CPU0:router(config-pmap)# event session-start match-first
RP/0/RSP0/CPU0:router(config-pmap-e)# class type control subscriber CL2
RP/0/RSP0/CPU0:router(config-pmap-c)# 1 authorize aaa list default password DdjkkWE
```

class-map type control subscriber

To determine the list of actions to be executed for the class and to enter the class-map configuration mode, use the **class-map type control subscriber** command in global configuration mode. To disable the class map type control subscriber and exit the class-map configuration mode, use the **no** form of this command.

class-map type control subscriber { **match-all** | **match-any** } *class-map name*

no class-map type control subscriber { **match-all** | **match-any** } *class-map name*

Syntax Description

class-map name	Specifies the class map name.
match-all	Configures the match all criteria for this class.
match-any	Configures the match any criteria for this class.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

Use the **class-map type control subscriber** command to enter class-map configuration mode.

Task ID

Task ID	Operation
qos	read, write

Examples

This is an example of configuring the **class-map type control subscriber** command in global configuration mode:

```
RP/0/RSP0/CPU0:router(config)# class-map type control subscriber match-any class1
RP/0/RSP0/CPU0:router(config-cmap)# match protocol ppp
RP/0/RSP0/CPU0:router(config-cmap)# end-class-map
```

Related Commands

Command	Description
policy-map type control subscriber, on page 126	Enables the policy-map.
event, on page 122	Enables the event in a policy-map.

deactivate

To deactivate the dynamic template mode, use the **deactivate** command in the class map sub-configuration mode. To disable this feature, use the **no** form of this command.

deactivate dynamic-template *name* **aaa list** {*list_name*| **default**}

no deactivate

Syntax Description

dynamic-template	Specifies the actions related to dynamic templates.
name	Specifies the name of the dynamic template.
aaa	Specifies the AAA parameters.
list	Specifies AAA method list that authentication should be made with.
default	Specifies the default AAA method list.
list_name	Specifies the name of the AAA method list.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
qos	read, write

Examples

This is an example of configuring the **deactivate** command in the class map sub-configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# policy-map type control subscriber PL1
RP/0/RSP0/CPU0:router(config-pmap)# event session-start match-first
RP/0/RSP0/CPU0:router(config-pmap-e)# class type control subscriber CL2
RP/0/RSP0/CPU0:router(config-pmap-c)# 1 deactivate dynamic-template DL1 aaa list default
```

Related Commands

Command	Description
activate, on page 112	Activates the dynamic template mode in the class map sub-configuration mode.

event

To configure a policy event, use the **event** command in policy-map configuration mode. To disable an event and exit the policy-map configuration mode, use the **no** form of this command.

event { **account-logoff** | **account-logon** | **authentication-failure** | **authentication-no-response** | **authorization-failure** | **authorization-no-response** | **idle-timeout** | **service-start** | **service-stop** | **session-activate** | **session-start** | **session-stop** | **timer-expiry** }

no event { **account-logoff** | **account-logon** | **authentication-failure** | **authentication-no-response** | **authorization-failure** | **authorization-no-response** | **idle-timeout** | **service-start** | **service-stop** | **session-activate** | **session-start** | **session-stop** | **timer-expiry** }

Syntax Description

account-logoff	Specifies an account logoff event.
account-logon	Specifies an account logon event.
authentication-failure	Specifies an authentication failure event.
authentication-no-response	Specifies an authentication no response event.
authorization-failure	Specifies an authorization failure event.
authorization-no-response	Specifies an authorization no response event.
idle-timeout	Specifies an idle timeout event.
service-start	Specifies a service start event.
service-stop	Specifies a service stop event.
session-activate	Specifies session activate event.
session-start	Specifies session start event.
session-stop	Specifies session start event.
timer-expiry	Specifies the timer expiry event.

Command Default

None

Command Modes

Policy-map configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.
Release 5.1	The **idle-timeout** event was added.

Usage Guidelines

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

Use the **policy-map type control subscriber** command to enter policy-map configuration mode.

For **idle-timeout** event, you can configure the policy action as **monitor** under the idle timeout event for a subscriber policy, to prevent the termination of the session.

Task ID

Task ID	Operation
qos	read, write

Examples

This example shows how to configure the **event** command in policy configuration mode:

```
RP/0/RSP0/CPU0:router(config)# policy-map type control subscriber pol1
RP/0/RSP0/CPU0:router(config-pmap)# event session-start match-first
RP/0/RSP0/CPU0:router(config-pmap-e)# class type control subscriber ip_dhcp do-until-failure
RP/0/RSP0/CPU0:router(config-cmap-c)# 1 activate dynamic-template ip_temp
RP/0/RSP0/CPU0:router(config-cmap-c)# 10 authorize aaa list default identifier format
dhcp_id_format password xya
RP/0/RSP0/CPU0:router(config-cmap-c)# end-policy-map
```

This example shows how to configure the **idle-timeout** event in policy configuration mode, with the action as **monitor** for the subscriber policy:

```
RP/0/RSP0/CPU0:router(config)# policy-map type control subscriber pol1
RP/0/RSP0/CPU0:router(config-pmap)# event idle-timeout
RP/0/RSP0/CPU0:router(config-pmap-e)# class type control subscriber ip_dhcp
RP/0/RSP0/CPU0:router(config-cmap-c)# 1 monitor
```

Related Commands

Command	Description
class-map type control subscriber, on page 118	Enables the class-map.
policy-map type control subscriber, on page 126	Enables the policy-map.

match (class-map)

To configure match criteria for the corresponding class, use the **match** command in class-map configuration mode. To disable the match feature and exit the policy-map configuration mode, use the **no** form of this command.

match {**authen-status**| {**authenticated**| **unauthenticated**}| **domain**| *domain_name*| {**format**| *format_name*}| **regexp**| *string*| **not**| **protocol**| {**ppp**| **dhcpv4**}| **source-address**| {**ipv4**| **mac**}| **timer**| *string*| **regexp**| *string*| **username**}

no match {**authen-status**| {**authenticated**| **unauthenticated**}| **domain**| *domain_name*| {**format**| *format_name*}| **regexp**| *string*| **not**| **protocol**| {**ppp**| **dhcpv4**}| **source-address**| {**ipv4**| **mac**}| **timer**| *string*| **regexp**| *string*| **username**}

Syntax Description

authen-status	Specified the authentication status.
authenticated	Specified the authenticated status.
unauthenticated	Specified the unauthenticated status.
domain	Specifies the domain type.
domain_name	Specifies the name of the domain.
format	Specifies the format type.
format_name	Specifies the name of the format.
regexp	Specifies the regular expression.
string	Specifies the regular expression of a string.
not	Negates the match criteria.
protocol	Specifies the protocol type.
source-address	Specifies the source address.
timer	Specifies the timer.
username	Specifies the name of the user.

Command Default

None

Command Modes

Class-map configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

Use the **class-map type control subscriber** command to enter class-map configuration mode.

Task ID

Task ID	Operation
qos	read, write

Examples

This is an example of configuring the **class-map type control subscriber** command in the class-map configuration mode:

```
RP/0/RSP0/CPU0:router(config)# class-map type control subscriber CL1
RP/0/RSP0/CPU0:router(config-pmap)# match authen-status authenticated
RP/0/RSP0/CPU0:router(config-pmap-e)# match domain d1 format f1
RP/0/RSP0/CPU0:router(config-cmap-c)# match protocol ppp
RP/0/RSP0/CPU0:router(config-cmap-c)# match source-address ipv4 1.3.4.5 12.334.55.2
RP/0/RSP0/CPU0:router(config-cmap-c)# match timer time1
```

policy-map type control subscriber

To determine the list of events that are applicable to the subscriber lifecycle and to enter the policy-map configuration mode, use the **policy-map type control subscriber** command in global configuration mode. To disable the policy map type control subscriber and exit the policy-map configuration mode, use the **no** form of this command.

policy-map type control subscriber *policy-map name*

no policy-map type control subscriber *policy-map name*

Syntax Description

policy-map name	Represents the policy map name.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
qos	read, write

Examples

This is an example of configuring the **policy-map type control subscriber** command in the global configuration mode:

```
RP/0/RSP0/CPU0:router(config)# policy-map type control subscriber pol1
RP/0/RSP0/CPU0:router(config-cmap-c)# end-policy-map
```

Related Commands

Command	Description
class-map type control subscriber, on page 118	Enables the class-map.
event, on page 122	Enables the event in the policy-map.

policy-map type pbr

To create or modify a policy map of type policy based routing that can be attached to one or more interfaces, use the **policy-map type pbr** command in global configuration mode. To disable this feature, use the **no** form of this command.

policy-map type pbr *name*

no policy-map type pbr *name*

Syntax Description

policy-map name	Represents the policy map name.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
qos	read, write

Examples

This is an example of configuring the **policy-map type pbr** command in the global configuration mode:

```
RP/0/RSP0/CPU0:router(config)# policy-map type pbr pbr_policy
RP/0/RSP0/CPU0:router(config-pmap)# end-policy-map
```

Related Commands

Command	Description
class-map type control subscriber, on page 118	Enables the class-map.

Command	Description
event, on page 122	Enables the event in the policy-map.

service-policy type control subscriber

To associate a subscriber control service policy to the interface, use the **service-policy type control subscriber** command in interface configuration mode. To disable the service-policy type control subscriber, use the **no** form of this command.

service-policy type control subscriber *name*

no service-policy type control subscriber *name*

Syntax Description

name	Represents the policy map name.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
config-services	read, write

Examples

This is an example of configuring the **service-policy type control subscriber** command in interface configuration mode:

```
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether 344
RP/0/RSP0/CPU0:router(config-if)# service-policy type control subscriber sub1
```

Related Commands

Command	Description
class-map type control subscriber, on page 118	Enables the class-map.

Command	Description
event, on page 122	Enables the event in the policy-map.

show class-map

To show the class-map related information, use the **show class-map** command in the EXEC mode.

show class-map type control subscriber *name*

Syntax Description

type	Displays the type of classmap.
control	Displays all the control class maps.
subscriber	Displays all the subscriber control class maps.
name	Displays the class map name.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	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.

Task ID

Task ID	Operation
qos	read

Examples

This is a sample output of the **show class-map** command in the EXEC mode:

```
RP/0/RSP0/CPU0:router# show class-map type control subscriber PTA_CLASS
```

The show class-map output is as follows:

```
Wed Jan 23 08:55:15.027 GMT
1) ClassMap: PTA_CLASS    Type: subscriber_control
    Referenced by 1 Policymaps
```

This table describes the significant fields shown in the display.

Table 7: show class-map Field Descriptions

Field	Description
ClassMap	Specifies the class map name.
Type	Specifies the type of the class map.

Related Commands

Command	Description
class-map type control subscriber, on page 118	Determines the list of actions to be executed for the class and enters the class-map configuration mode.

show policy-map

To show the policy-map related information, use the **show policy-map** command in the EXEC mode.

show policy-map type control subscriber pmap-name *name*

Syntax Description

type	Displays the type of policy-map.
control	Displays the control type policy-map.
subscriber	Displays the subscriber control type policy-map.
pmap_name	Specifies the policy-map name.
name	Displays the policy map name.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	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.

Task ID

Task ID	Operation
qos	read

Examples

This is a sample output of the **show policy-map** command in the EXEC mode:

```
RP/0/RSP0/CPU0:router# show policy-map control subscriber pmap-name POLICY1
```

The show policy-map output is as follows:

```
Wed Jan 23 08:56:13.794 GMT
```

```
policy-map type control subscriber POLICY1
 event session-start match-all
  class type control subscriber PTA_CLASS do-all
   1 activate dynamic-template PPP_PTA_TEMPLATE
  !
 !
 end-policy-map
!
```

This table describes the significant fields shown in the display.

Table 8: show policy-map Field Descriptions

Field	Description
policy-map	Specifies the policy map name.
Type	Specifies the type of the class type control subscriber.

Related Commands

Command	Description
policy-map type control subscriber, on page 126	Determines the list of events that are applicable to the subscriber lifecycle and to enter the policy-map configuration mode.

BNG DHCP Commands

This module describes the Cisco IOS XR software commands used to configure the DHCP commands for Broadband Network Gateway (BNG) on the Cisco ASR 9000 Series Router. For details regarding the related configurations, refer to the *Cisco ASR 9000 Series Aggregation Services Router Broadband Network Gateway Configuration Guide*.

- address-pool, page 139
- aftr-name, page 140
- broadcast-flag policy check (BNG), page 141
- class, page 143
- dhcp ipv4 (BNG), page 145
- dhcp ipv6 (BNG), page 146
- dhcpv6 address-pool, page 147
- dhcpv6 delegated-prefix-pool, page 149
- dns-server (BNG), page 150
- domain-name (DHCP IPv6 pool-BNG), page 152
- framed-prefix-pool, page 154
- helper-address (BNG), page 155
- interface (DHCP-BNG), page 157
- interface subscriber-pppoe profile, page 159
- lease, page 160
- match option, page 162
- match vrf, page 164
- prefix-pool, page 165
- profile (BNG), page 166
- relay information authenticate (BNG), page 168
- relay information check (BNG), page 170

- relay information option (BNG), page 172
- relay information option allow-untrusted (BNG), page 174
- relay information policy (BNG), page 176
- relay option remote-id, page 178
- limit lease per-circuit-id, page 180
- limit lease per-remote-id, page 182
- limit lease per-interface, page 184
- lease proxy client-lease-time, page 186
- show dhcp ipv4 proxy binding, page 188
- show dhcp ipv4 proxy interface (BNG), page 191
- show dhcp ipv4 proxy profile, page 193
- show dhcp ipv4 proxy statistics, page 195
- show dhcp ipv6 proxy binding (BNG), page 197
- show dhcp ipv6 proxy interface (BNG), page 199
- show dhcp ipv6 proxy profile, page 201
- show dhcp ipv6 proxy statistics, page 203
- show dhcp ipv6 server binding, page 205
- show dhcp ipv6 server interface, page 208
- show dhcp ipv6 server profile, page 210
- show dhcp ipv6 server statistics, page 212

address-pool

To specify the name of an address pool by integrating the DHCPv6 sever with distributed address pool service (DAPS), use the **address-pool** command in the DHCP IPv6 server profile class configuration mode. To remove the address pool name, use the **no** form of this command.

address-pool *pool_name*

no address-pool *pool_name*

Syntax Description

pool_name	Specifies the name of a address pool.

Command Default

None

Command Modes

DHCP IPv6 server profile class configuration

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

To enter the DHCP IPv6 server profile configuration, enter **profile** *profile_name* **server** command in the DHCPv6 configuration mode.

To enter the DHCP IPv6 server profile class configuration, enter **class** *class_name* command in the DHCPv6 server profile configuration mode.

Task ID

Task ID	Operations
ip-services	read, write

Examples

This is an example of creating a address-pool name using the **address-pool** command:

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv6
RP/0/RSP0/CPU0:router(config-dhcpv6)# profile my_profile server
RP/0/RSP0/CPU0:router(config-dhcpv6-server-profile)# class class_dhcp
RP/0/RSP0/CPU0:router(config-dhcpv6-server-profile-class)# address-pool pool_addr
```

aftr-name

To set the Address Family Transition Router's (AFTR) name for Dual-stack Lite support, use the **aftr-name** command in DHCPv6 server profile configuration mode. To disable the AFTR-name, use the **no** form of this command.

aftr-name *aftr-name*

no aftr-name *aftr-name*

Syntax Description

aftr-name	Specifies the AFTR fully qualified domain name for the server profile.

Command Default

Dual-stack support is not enabled.

Command Modes

DHCPv6 server profile configuration

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
ip-services	read, write

Examples

This example shows how to configure the AFTR Fully Qualified Domain Name (FQDN) for a server profile:

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv6
RP/0/RSP0/CPU0:router(config-dhcpv6)# profile my_profile server
RP/0/RSP0/CPU0:router(config-dhcpv6-server-profile)# aftr-name aftr-server.example.com
```

broadcast-flag policy check (BNG)

To configure Dynamic Host Configuration Protocol (DHCP) IPv4 Relay to broadcast only BOOTREPLY packets if the DHCP IPv4 broadacst flag is set in the DHCP IPv4 header, use the **broadcast-flag policy check** command in DHCP IPv4 relay profile configuration submode or DHCP IPv4 server profile configuration submode. By default, the DHCP IPv4 Relay always broadcasts BOOTREPLY packets. To restore the default, use the **no** form of this command.

broadcast-flag policy { **check** | **unicast-always** }

no broadcast-flag policy { **check** | **unicast-always** }

Syntax Description

check	Checks the broadcast flag in packets.
unicast-always	Sets the broadcast-flag policy to unicast-always.

Command Default

Relay agent always broadcasts DHCP IPv4 packets to a client.

Command Modes

DHCP IPv4 relay profile configuration

DHCP IPv4 server profile

Command History

Release	Modification
Release 3.7.0	This command was introduced.
Release 4.2.0	This command was supported for BNG.
Release 5.1	The **unicast-always** keyword was added.

Usage Guidelines

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

Task ID

Task ID	Operations
ip-services	read, write

Examples

This an example of the **broadcast-flag policy check** command:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# profile client relay
RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# broadcast-flag policy check
```

This an example of the **broadcast-flag policy** command:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# profile TEST server
RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)# broadcast-flag policy unicast-always
```

Related Commands

Command	Description
dhcp ipv4 (BNG), on page 145	Enables DHCP for IPv4 and enters DHCP IPv4 configuration mode.
#unique_114	Configures the DHCP relay agent to relay packets to a specific DHCP server.
relay information check (BNG), on page 170	Configures a DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.
relay information option (BNG), on page 172	Enables the system to insert a DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.
relay information option allow-untrusted (BNG), on page 174	Configures the DHCP component to not drop BOOTREQUEST messages that have the relay information option set and the giaddr set to zero.
#unique_115	Configures how a relay agent processes BOOTREQUEST messages that already contain a relay information option.

class

To create a proxy profile class and to enter the proxy profile class sub configuration mode, use the **class** command in an appropriate configuration mode. To disable this feature and exit the profile mode, use the **no** form of this command.

class *class_name* {**helper-address**| **match**} {**address-pool**| **dns-server**| **domain-name**| **prefix-pool**}

no class *class_name*

Syntax Description

class_name	Specifies the class name.
helper-address	Specifies the server address to relay packets.
match	Inserts a match keyword.
address-pool	Specifies the name of the address pool
dns-server	Specifies the name of a dns server.
domain-name	Specifies the name of a domain.
prefix-pool	Specifies the name of the prefix pool.

Command Default

No class is specified.

Command Modes

DHCP IPv4 proxy profile configuration

DHCP IPv6 proxy profile configuration

DHCP IPv6 server profile configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.
Release 4.3.0	The support for IPv6 was added.

Usage Guidelines

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

The class submode is present in both DHCP IPv6 proxy profile configuration and DHCP IPv6 server profile configuration submodes. A class is associated with a match criterion, which is used to determine if the class is applied to a subscriber or not. The class name needs to be unique for the system.

Note The address-pool, dns-server, domain-name, and prefix-pool keywords appear only in the DHCP IPv6 server profile configuration mode. However, the helper-address keywords appears in both DHCP IPv4 proxy profile configuration and DHCP IPv6 proxy profile configuration modes.

Task ID

Task ID	Operation
ip-services	read, write

Examples

This example shows how to create a class in the DHCP IPv4 proxy profile configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# profile dhcp_profile proxy
RP/0/RSP0/CPU0:router(config-dhcpv4-proxy-profile)# class blue
```

This example shows how to create a class in the DHCP IPv6 proxy profile configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv6
RP/0/RSP0/CPU0:router(config-dhcpv6)# profile dhcp_profile1 proxy
RP/0/RSP0/CPU0:router(config-dhcpv4-proxy-profile)# class blue
```

This example shows how to create a class in the DHCP IPv6 server profile configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv6)# profile dhcp_profile2 server
RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)# class red
```

Related Commands

Command	Description
class-map type control subscriber, on page 118	This topic describes the class-map type control subscriber command.

dhcp ipv4 (BNG)

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

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.2.0	This command was supported for BNG.

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:

```
RP/0/RSP0/CPU0:router# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)#
```

dhcp ipv6 (BNG)

To enable Dynamic Host Configuration Protocol (DHCP) for IPv6 and to enter DHCP IPv6 configuration mode, use the **dhcp ipv6** command in global configuration mode. To disable the DHCP for IPv6, use the **no** form of this command.

dhcp ipv6

no dhcp ipv6

Syntax Description

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.3.0	This command was supported for BNG.

Usage Guidelines

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

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:

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv6
RP/0/RSP0/CPU0:router(config-dhcpv6)#
```

dhcpv6 address-pool

To specify addresses for DHCPv6 when Radius does not provide IPv6 address, use the **dhcpv6 address-pool** command in the dynamic template configuration mode. To remove the IPv6 address pool name for DHCPv6, use the **no** form of this command.

dhcpv6 address-pool *pool_name*

no dhcpv6 address-pool *pool_name*

Syntax Description

pool_name	Specifies the name of a IPv6 address pool name for DHCPv6.

Command Default

None

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

To enter the dynamic template configuration mode, enter **dynamic-template** command in the global configuration mode.

The IPv6 address pool is used for both PPPoE and IPoE subscribers.

Task ID

Task ID	Operations
config-services	read, write

Examples

This is an example of creating an IPv6 address pool for PPPoE subscribers using the **dhcpv6 address-pool** command:

```
RP/0/RSP0/CPU0:router(config)# dynamic-template
RP/0/RSP0/CPU0:router(config-dynamic-template)# type ppp my-ipv6-pppoe-tempate
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# dhcpv6 address-pool my-pppoe-addr-pool
```

This is an example of creating an IPv6 address pool for IPoE subscribers using the **dhcpv6 address-pool** command:

```
RP/0/RSP0/CPU0:router(config)# dynamic-template
RP/0/RSP0/CPU0:router(config-dynamic-template)# type ppp my-ipv6-tempate
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# dhcpv6 address-pool my-ipsub-addr-pool
```

dhcpv6 delegated-prefix-pool

To specify the default pool name for (IA-PD) prefix delegation when no pool name or prefix is provided by the Radius, use the **dhcpv6 delegated-prefix-pool** command in the dynamic template configuration mode. To remove the delegated prefix pool name, use the **no** form of this command.

dhcpv6 delegated-prefix-pool *pool_name*

no dhcpv6 delegated-prefix-pool *pool_name*

Syntax Description

pool_name	Specifies the name of a delegated prefix pool for DHCPv6.

Command Default

None

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

To enter the dynamic template configuration mode, enter **dynamic-template** command in the global configuration mode.

Task ID

Task ID	Operations
config-services	read, write

Examples

This is an example of creating a delegated prefix-pool name using the **dhcpv6 delegated-prefix-pool** command:

```
RP/0/RSP0/CPU0:router(config)# dynamic-template
RP/0/RSP0/CPU0:router(config-dynamic-template)# type ipsubscriber ipsub1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# dhcpv6 delegated-prefix-pool myPool
```

dns-server (BNG)

To specify the Domain Name System (DNS) IPv6 servers available to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **dns-server** command in an appropriate configuration mode. To remove the DNS server list, use the **no** form of this command.

dns-server *ipv6-address*

no dns-server *ipv6-address*

Syntax Description

ipv6-address	IPv6 address of a DNS server. This argument must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

When a DHCP for IPv6 pool is first created, no DNS IPv6 servers are configured.

Command Modes

DHCP IPv6 server profile configuration

DHCP IPv6 server profile class configuration

Command History

Release	Modification
Release 4.3.0	This command was supported in DHCP IPv6 server profile and class configuration mode in BNG.

Usage Guidelines

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

Multiple Domain Name System (DNS) server addresses can be configured by issuing this command multiple times. New addresses do not overwrite old addresses.

To enter the DHCP IPv6 server profile configuration, enter **profile** *profile_name* **server** command in the DHCPv6 configuration mode.

To enter the DHCP IPv6 server profile class configuration, enter **class** *class_name* command in the DHCPv6 server profile configuration mode.

Task ID

Task ID	Operations
ip-services	read, write

Examples

This is an example of setting the DNS address - 2001:db8:1203::1 and 2001:db8:1204::1 - using the **dns-server** command in the DHCP IPv6 server profile configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv6
RP/0/RSP0/CPU0:router(config-dhcpv6)# profile my_profile server
RP/0/RSP0/CPU0:router(config-dhcpv6-server-profile)# dns-server 2001:db8:1203::1 and
2001:db8:1204::1
```

This is an example of setting the DNS address - 2001:db8:1203::1 and 2001:db8:1204::1 - using the **dns-server** command in the DHCP IPv6 server profile class configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv6
RP/0/RSP0/CPU0:router(config-dhcpv6)# profile my_profile server
RP/0/RSP0/CPU0:router(config-dhcpv6-server-profile)# class proxy-red
RP/0/RSP0/CPU0:router(config-dhcpv6-server-profile-class)# dns-server 2001:db8:1203::1 and
 2001:db8:1204::1
```

domain-name (DHCP IPv6 pool-BNG)

To configure a domain name for a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **domain-name** command in an appropriate configuration mode. To remove the domain name, use the **no** form of this command.

domain-name *domain*

no domain-name

Syntax Description

domain	Specifies the domain name string to be used by the client.

Command Default

When a DHCP for IPv6 pool is first created, no domain name for clients is configured.

Command Modes

DHCP IPv6 server profile configuration

DHCP IPv6 server profile class configuration

Command History

Release	Modification
Release 4.3.0	This command was supported in DHCP IPv6 server profile and class configuration mode in BNG.

Usage Guidelines

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

Multiple Domain Name System (DNS) domain names can be configured by issuing the **domain-name** command multiple times. The new domain name does not overwrite existing domain names.

To enter the DHCP IPv6 server profile configuration, enter **profile** *profile_name* **server** command in the DHCPv6 configuration mode.

To enter the DHCP IPv6 server profile class configuration, enter **class** *class_name* command in the DHCPv6 server profile configuration mode.

The domain name is defined in DHCP IPv6 server profile and DHCP IPv6 server profile class configuration. If the same parameters are defined in the class scope, then the values defined in the class scope takes precedence.

Task ID

Task ID	Operations
ip-services	read, write

Examples

This is an example of setting the domain name using the **domain-name** command in the DHCP IPv6 server profile configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv6
RP/0/RSP0/CPU0:router(config-dhcpv6)# profile my_profile server
RP/0/RSP0/CPU0:router(config-dhcpv6-server-profile)# domain-name my.domain.com
```

This is an example of setting the domain name using the **domain-name** command in the DHCP IPv6 server profile class configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv6
RP/0/RSP0/CPU0:router(config-dhcpv6)# profile my_profile server
RP/0/RSP0/CPU0:router(config-dhcpv6-server-profile)# class proxy-red
RP/0/RSP0/CPU0:router(config-dhcpv6-server-profile-class)# domain-name my.domain.com
```

framed-prefix-pool

To specify the default pool name for ipv6 prefixes for assignment only from SLAAC (Stateless Address Auto-Configuration), use the **framed-prefix-pool** command in the dynamic template configuration mode. To remove the framed prefix pool name, use the **no** form of this command.

framed-prefix-pool *pool_name*

no framed-prefix-pool *pool_name*

Syntax Description

pool_name	Specifies the name of a prefix pool.

Command Default

None

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

To enter the dynamic template configuration mode, enter **dynamic-template** command in the global configuration mode.

The dynamic template configuration is used when Radius does not return pool name or prefix for the SLAAC.

Task ID

Task ID	Operations
config-services	read, write

Examples

This is an example of creating a framed prefix pool name using the **framed-prefix-pool** command:

```
RP/0/RSP0/CPU0:router(config)# dynamic-template
RP/0/RSP0/CPU0:router(config-dynamic-template)# type ipv6
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# framed-prefix-pool my-slaac-pool
```

helper-address (BNG)

To configure the Dynamic Host Configuration Protocol (DHCP) IPv4 and IPv6 relay agent to relay BOOTREQUEST packets to a specific DHCP server, use the **helper-address** command in an appropriate 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 and Pv6 address in four part, dotted decimal format.
giaddr *gateway-address*	Specifies the gateway address to use in packets relayed to server.

Command Default

Helper address is not configured.

Command Modes

DHCP IPv6 proxy profile class configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.2.0	This command was supported for BNG.
Release 4.3.0	The support for IPv6 was added in BNG.

Usage Guidelines

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

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 IPv6 proxy profile class configuration mode:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# dhcp ipv6
RP/0/RSP0/CPU0:router(config-dhcpv6)# profile myprofile proxy
RP/0/RSP0/CPU0:router(config-dhcpv4-proxy-profile)# class myclass
RP/0/RSP0/CPU0:router(config-dhcpv4-proxy-profile-class)#  helper-address vrf my-server-vrf
 1:1:1::1
```

Related Commands

Command	Description
dhcp ipv4 (BNG), on page 145	Enables Dynamic Host Configuration Protocol (DHCP) for IPv4 and enters DHCP IPv4 configuration mode.
relay information check (BNG), on page 170	Configures a DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.
relay information option (BNG), on page 172	Enables the system to insert a DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.
relay information option allow-untrusted (BNG), on page 174	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 (BNG), on page 176	Configures how a relay agent processes BOOTREQUEST messages that already contain a relay information option.

interface (DHCP-BNG)

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* {**server**| **relay**| **proxy**}

no interface *type interface-path-id* {**relay**| **proxy**| **server**}

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	Specifies a destination address.
proxy	Specifies the proxy and assigns option 82 to an interface.

Command Default

None

Command Modes

DHCP IPv6 configuration

Command History

Release	Modification
Release 4.3.0	The support for IPv6 was added in BNG.
Release 5.1	Support for **server** profile was added.

Task ID

Task ID	Operations
ip-services	read, write

Examples

This is an example of enabling the DHCP interface mode on a Packet over Sonet/SDH (POS) interface using the **interface** command:

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv6
RP/0/RSP0/CPU0: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:

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# interface POS 0/5/0/0 server profile TEST
```

Related Commands

Command	Description
dhcp ipv6 (BNG), on page 146	Enables Dynamic Host Configuration Protocol (DHCP) for IPv6 and enters DHCP IPv6 configuration mode.
dhcp ipv4 (BNG), on page 145	Enables Dynamic Host Configuration Protocol (DHCP) for IPv4 and enters DHCP IPv4 configuration mode.
show dhcp ipv6 interface	Displays DHCP for IPv6 interface information.

interface subscriber-pppoe profile

To enable the PPPoE subscribers to use a profile for all the PPPoE subscribers, use the **interface subscriber-pppoe profile** command in the DHCP IPv6 configuration mode. To disable this feature, use the **no** form of this command.

interface subscriber-pppoe profile *profile_name*

no interface subscriber-pppoe profile *profile_name*

Syntax Description

profile_name	Specifies the name of the profile.

Command Default

VRF is disabled.

Command Modes

DHCP IPv6 configuration

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
ip-services	read, write

Examples

This is an example for enabling PPPoE subscribers to use the "my-def-pppoe-green" profile for all the PPPoE subscribers using the **interface subscriber-pppoe profile** command:

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv6
RP/0/RSP0/CPU0:router(config-dhcpv6)#  interface subscriber-pppoe profile my-def-pppoe-green
```

lease

To set a client lease time on a per profile basis, use the **lease** command in DHCPv6 server profile configuration mode. To disable the client lease time, use the **no** form of this command.

lease {{*days*| *hours*| *minutes*}|**infinite** }

no lease {{*days*| *hours*| *minutes*}|**infinite** }

Syntax Description

days	Specifies the number of days for the lease time. The value ranges from 1 to 365.
hours	Specifies the number of hours for the lease time. The value ranges from 0 to 23.
minutes	Specifies the number of minutes for the lease time. The value ranges from 0 to 59.
infinite	Specifies an infinite amount of lease.

Command Default

Lawful intercept is not enabled.

Command Modes

DHCPv6 server profile configuration

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

The lease time is applied to the class only and not to the whole profile. When both profile and class lease times are present, then the class lease time is applied. The default lease time is 1 day, when no lease time configuration exists.

The lease time is specified in seconds or date format.

Task ID

Task ID	Operation
ip-services	read, write

Examples This example shows how to configure lease time for 1 day, 6 hours, and 0 minutes:

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv6
RP/0/RSP0/CPU0:router(config-dhcpv6)# profile my_profile server
RP/0/RSP0/CPU0:router(config-dhcpv6-server-profile)# lease 1 6 0
```

This example shows how to configure infinite amount of lease time:

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv6
RP/0/RSP0/CPU0:router(config-dhcpv6)# profile my_profile server
RP/0/RSP0/CPU0:router(config-dhcpv6-server-profile)# lease infinite
```

match option

To match the proxy with the configured pattern, use the **match option** command in the DHCP IPv4 proxy profile class configuration mode. To disable the match option, use the **no** form of the command.

match option {**124**| **125**| | **60**| **77**} **hex** *hex_string* **mask** *bit_mask_string*

no match option {**124**| **125**| | **60**| **77**} **hex** *hex_string* **mask** *bit_mask_string*

Syntax Description

124	Inserts option 124 vendor-identifying vendor class.
125	Inserts option 125 vendor-identifying vendor-specific info.
60	Inserts option 60 vendor class ID.
77	Inserts option 124 user class.
hex	Inserts a hex pattern.
hex_string	Specifies the hex pattern string.
mask	Inserts bit mask pattern.
bit_mask_string	Specifies the bit mask pattern string. The string pattern is between 0 and 4294967295.

Command Default

None

Command Modes

DHCP IPv4 proxy profile class configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
ip-services	read, write

Examples

This is an example of configuring the **match option** command in the DHCP IPv4 proxy profile class configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# profile dhcp_profile proxy
RP/0/RSP0/CPU0:router(config-dhcpv4-proxy-profile)# class blue
RP/0/RSP0/CPU0:router(config-dhcpv4-proxy-profile-class)# match option 124 hex hex_name
mask 3445
```

Related Commands

Command	Description
class, on page 143	Creates a proxy profile class and enters the proxy profile class sub configuration mode.

match vrf

To match class based on VRF name, use the **match vrf** command in the DHCP IPv4 proxy profile class configuration mode. To disable the match vrf, use the **no** form of the command.

match vrf *vrf_name*

no match vrf *vrf_name*

Syntax Description

vrf_name	Specifies the VRF name.

Command Default

None

Command Modes

DHCP IPv4 proxy profile class configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
ip-services	read, write

Examples

This is an example of configuring the **match vrf** command

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# profile dhcp_profile proxy
RP/0/RSP0/CPU0:router(config-dhcpv4-proxy-profile)# class blue
RP/0/RSP0/CPU0:router(config-dhcpv4-proxy-profile-class)# match vrf vrf1
```

Related Commands

Command	Description
match option, on page 162	Matches the proxy with the configured pattern.

prefix-pool

To specify the name of prefix pool by integrating the DHCPv6 sever with distributed address pool service (DAPS), use the **prefix-pool** command in the DHCP IPv6 server profile class configuration mode. To remove the prefix pool name, use the **no** form of this command.

prefix-pool *pool_name*

no prefix-pool *pool_name*

Syntax Description

pool_name	Specifies the name of a prefix pool.

Command Default

When a DHCP for IPv6 pool is first created, no DNS IPv6 servers are configured.

Command Modes

DHCP IPv6 server profile class configuration

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

To enter the DHCP IPv6 server profile configuration, enter **profile** *profile_name* **server** command in the DHCPv6 configuration mode.

To enter the DHCP IPv6 server profile class configuration, enter **class** *class_name* command in the DHCPv6 server profile configuration mode.

Task ID

Task ID	Operations
ip-services	read, write

Examples

This is an example of creating a prefix-pool name using the **prefix-pool** command:

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv6
RP/0/RSP0/CPU0:router(config-dhcpv6)# profile my_profile server
RP/0/RSP0/CPU0:router(config-dhcpv6-server-profile)# class class_dhcp
RP/0/RSP0/CPU0:router(config-dhcpv6-server-profile-class)# prefix-pool pool1
```

profile (BNG)

To specify a DHCP profile for the Dynamic Host Configuration Protocol (DHCP) IPv4 and IPv6 component and to enter the profile mode, use the **profile** command in DHCP IPv4 or DHCP IPv6 configuration submode. To disable a profile and exit the profile mode, use the **no** form of this command.

profile *profile_name* {**proxy** | **server** }

no profile *profile_name* **proxy**

Syntax Description

profile_name	Specifies the name of the profile that uniquely identifies the proxy or server.
proxy	Creates a DHCP proxy profile.
server	Creates a DHCP server profile.

Command Default

None

Command Modes

DHCP IPv4 configuration

DHCP IPv6 configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.
Release 4.3.0	Support was added for IPv6.

Usage Guidelines

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

Task ID

Task ID	Operations
ip-services	read, write

Examples

This example shows how to enable the dhcpv4 configuration mode and how to create a profile called dhcp_profile in the dhcpv4 configuration submode:

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# profile dhcp_profile proxy
RP/0/RSP0/CPU0:router(config-dhcpv4-proxy-profile)#
```

This example shows how to enable the dhcpv6 configuration mode and how to create a profile called dhcp_v6 in the dhcpv6 configuration submode:

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv6
RP/0/RSP0/CPU0:router(config-dhcpv6)# profile dhcp_v6 proxy
RP/0/RSP0/CPU0:router(config-dhcpv6-proxy-profile)#
```

relay information authenticate (BNG)

To specify relay agent information option to the policy plane for authentication purposes, use the **relay information authenticate** command in the DHCP IPv4 proxy profile configuration mode. To disable the relay option, use the **no** form of this command.

relay information authenticate {**received| inserted**}

no relay information authenticate {**received| inserted**}

Syntax Description

received	Authenticate using received relay agent information option.
inserted	Authenticate using inserted relay agent information option.

Command Default

None

Command Modes

DHCP IPv4 proxy profile configuration

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
ip-services	read, write

Examples

This example shows how to specify the received relay agent information option for authentication using the **relay information authenticate** command in DHCP IPv4 proxy profile configuration mode:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# profile myprofile proxy
RP/0/RSP0/CPU0:router(config-dhcpv4-proxy-profile)# relay information authenticate received
```

Related Commands

Command	Description
dhcp ipv4 (BNG), on page 145	Enables Dynamic Host Configuration Protocol (DHCP) for IPv4 and enters DHCP IPv4 configuration mode.
relay information check (BNG), on page 170	Configures a DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.
relay information option (BNG), on page 172	Enables the system to insert a DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.
relay information option allow-untrusted (BNG), on page 174	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 (BNG), on page 176	Configures how a relay agent processes BOOTREQUEST messages that already contain a relay information option.

relay information check (BNG)

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 3.7.2	This command was introduced.
Release 4.2.0	This command was supported for BNG.

Usage Guidelines

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

Task ID

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

Examples

This example shows how to use the **relay information check** command:

```
RP/0/RSP0/CPU0:router#config
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# profile client relay
RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# relay information check
```

Related Commands

Command	Description
dhcp ipv4 (BNG), on page 145	Enables DHCP for IPv4 and enters DHCP IPv4 configuration mode.
#unique_114	Configures the DHCP relay agent to relay packets to a specific DHCP Server.
profile (BNG)	Configures a relay profile for the DHCP IPv4 component.
relay information option (BNG), on page 172	Enables the system to insert a DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.
relay information option allow-untrusted (BNG), on page 174	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 (BNG)

To configure Dynamic Host Configuration Protocol (DHCP) IPv4 relay or DHCP snooping 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 or DHCP IPv4 profile snoop submode. 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 relay configuration

DHCP IPv4 profile snoop configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.2.0	This command was supported for BNG.

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.

If the **information option** command is enabled, DHCP snooping mode does not set the giaddr field in the DHCP packet.

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

Examples

This example shows how to use the **relay information option** command:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# profile client relay
RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# relay information option
```

Related Commands

Command	Description
dhcp ipv4 (BNG), on page 145	Enables DHCP for IPv4 and enters DHCP IPv4 configuration mode.
#unique_114	Configures the DHCP relay agent to relay packets to a specific DHCP Server.
relay information check (BNG), on page 170	Configures a DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.
relay information option allow-untrusted (BNG), on page 174	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 (BNG)

To configure the Dynamic Host Configuration Protocol (DHCP) IPv4 relay or DHCP snooping 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 or DHCP IPv4 profile snoop 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 relay configuration

DHCP IPv4 profile snoop configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.2.0	This command was supported for BNG.

Usage Guidelines

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

According to RFC 3046, relay agents (and servers) 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 the server or 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/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# profile client relay
RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# relay information option allow-untrusted
```

Related Commands

Command	Description
dhcp ipv4 (BNG), on page 145	Enables DHCP for IPv4 and enters DHCP IPv4 configuration mode.
#unique_114	Configures the DHCP relay agent to relay packets to a specific DHCP Server.
relay information check (BNG), on page 170	Configures a DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.
relay information option (BNG), on page 172	Enables the system to insert a DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.

relay information policy (BNG)

To configure how the Dynamic Host Configuration Protocol (DHCP) IPv4 relay processes BOOTREQUEST packets that already contain a relay information option, use the **relay information policy** command in DHCP IPv4 relay profile configuration submode. To restore the default relay information policy, use the **no** form of this command.

relay information policy {**drop**| **keep**| **encapsulate**}

no relay information policy {**drop**| **keep**| **encapsulate**}

Syntax Description

drop	Directs the DHCP IPv4 Relay to discard BOOTREQUEST packets with the existing relay information option.
keep	Directs the DHCP IPv4 Relay not to discard a BOOTREQUEST packet that is received with an existing relay information option and to keep the existing relay information option value.
encapsulate	Encapsulates the DHCP relay agent information option received from a prior relay agent in forwarded BOOTREQUEST messages.

Command Default

The DHCP IPv4 Relay does not discard a BOOTREQUEST packet that has an existing relay information option. The option and the existing relay information option value is replaced.

Command Modes

DHCP IPv4 relay profile configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.2.0	This command was supported for BNG.
Release 4.3.1	The **encapsulate** keyword was added.

Usage Guidelines

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

The **encapsulate** keyword allows the second relay agent to encapsulate option 82 information in a message received from the first relay agent, if it is also configured to add its own option 82 information. This configuration allows the DHCP server to use option 82 information from both relay agents.

Task ID

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

Examples

This is sample output from executing the **relay information policy** command:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# profile client relay
RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# relay information policy keep
```

This example shows how to encapsulate the DHCP relay agent information option:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# profile client relay
RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# relay information policy encapsulate
```

Related Commands

Command	Description
dhcp ipv4 (BNG), on page 145	Enables DHCP for IPv4 and enters DHCP IPv4 configuration mode.
helper-address (BNG), on page 155	Configures the DHCP relay agent to relay packets to a specific DHCP Server.
relay information check (BNG), on page 170	Configures a DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.
relay information option (BNG), on page 172	Enables the system to insert a DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.
relay information option allow-untrusted (BNG), on page 174	Configures the DHCP component to not drop BOOTREQUEST messages that have the relay information option set and the giaddr set to zero.

relay option remote-id

To identify the remote host end of the circuit in the DHCPv6 relay agents, use the **relay option remote-id** command in the DHCP IPv6 proxy profile configuration mode. To disable the relay option, use the **no** form of this command.

relay option remote-id *remote-id-string*

no relay option remote-id *remote_id*

Syntax Description

remote-id-string	(Optional) Specifies the string value for the remote-id.

Command Default

If the remote-id is not provided during configuration, then the default value is used.

Command Modes

DHCP IPv4 proxy profile configuration

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

The **relay option remote-id** *remote-id* option is from the relay agent/proxy to the server. The option provides additional information to the DHCPv6 server. The server may use the information in the option to select parameters specific to particular users, hosts, or subscriber modems. The remote-id field is opaque to server and the server does not parse the value.

Task ID

Task ID	Operations
ip-services	read, write

Examples

This example shows how to set the remote-id value as "my-remote-id-12345" using the **relay option remote-id** command in DHCP IPv6 proxy profile configuration mode:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# dhcp ipv6
RP/0/RSP0/CPU0:router(config-dhcpv6)# profile myprofile proxy
RP/0/RSP0/CPU0:router(config-dhcpv4-proxy-profile)# relay option remote-id my-remote-id-12345
```

Related Commands

Command	Description
dhcp ipv4 (BNG), on page 145	Enables Dynamic Host Configuration Protocol (DHCP) for IPv4 and enters DHCP IPv4 configuration mode.
relay information check (BNG), on page 170	Configures a DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.
relay information option (BNG), on page 172	Enables the system to insert a DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.
relay information option allow-untrusted (BNG), on page 174	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 (BNG), on page 176	Configures how a relay agent processes BOOTREQUEST messages that already contain a relay information option.

limit lease per-circuit-id

To specify the lease limit each circuit id each interface, use the **limit lease per-circuit-id** command in the DHCP IPv4 sub configuration mode. To disable the lease per-circuit-id, use the **no** form of this command.

limit lease per-circuit-id *value*

no limit lease per-circuit-id *value*

Syntax Description

value	Specifies the limit up to which the lease value can be extended.

Command Default

None

Command Modes

DHCP IPv4 configuration

Command History

Release	Modification
Release 4.2.1	This command was introduced.

Usage Guidelines

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

Use the **dhcp ipv4** command to enter DHCP IPv4 configuration mode.

Task ID

Task ID	Operation
ip-services	read, write

Examples

This is an example of configuring the **limit lease per-circuit-id** command in the DHCP IPv4 sub configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# profile myproxyprofile proxy
RP/0/RSP0/CPU0:router(config-dhcpv4)# limit lease per-circuit-id 1000
```

Related Commands

Command	Description
dhcp ipv4 (BNG), on page 145	Enables the Dynamic Host Configuration Protocol (DHCP) for IPv4.

limit lease per-remote-id

To specify the lease limit per remote id each interface, use the **limit lease per-remote-id** command in the DHCP IPv4 sub configuration mode. To disable the lease per-remote-id, use the **no** form of this command.

limit lease per-remote-id *value*

no limit lease per-remote-id *value*

Syntax Description

value	Specifies the limit up to which the lease value can be extended.

Command Default

None

Command Modes

DHCP IPv4 configuration

Command History

Release	Modification
Release 4.2.1	This command was introduced.

Usage Guidelines

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

Use the **dhcp ipv4** command to enter DHCP IPv4 configuration mode.

Task ID

Task ID	Operation
ip-services	read, write

Examples

This is an example of configuring the **limit lease per-remote-id** command in the DHCP IPv4 sub configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# profile myproxyprofile proxy
RP/0/RSP0/CPU0:router(config-dhcpv4)# limit lease per-remote-id 1000
```

Related Commands

Command	Description
dhcp ipv4 (BNG), on page 145	Enables the Dynamic Host Configuration Protocol (DHCP) for IPv4.

limit lease per-interface

To specify the lease limit each interface, use the **limit lease per-interface** command in the DHCP IPv4 sub configuration mode. To disable the limit lease per-interface, use the **no** form of this command.

limit lease per-interface *value*

no limit lease per-interface *value*

Syntax Description

value	Specifies the limit up to which the lease value can be extended.

Command Default

None

Command Modes

DHCP IPv4 configuration

Command History

Release	Modification
Release 4.2.1	This command was introduced.

Usage Guidelines

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

Use the **dhcp ipv4** command to enter DHCP IPv4 configuration mode.

Task ID

Task ID	Operation
ip-services	read, write

Examples

This is an example of configuring the **limit lease per-interface** command in the DHCP IPv4 sub configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# profile myproxyprofile proxy
RP/0/RSP0/CPU0:router(config-dhcpv4)# limit lease per-interface 1000
```

Related Commands

Command	Description
dhcp ipv4 (BNG), on page 145	Enables the Dynamic Host Configuration Protocol (DHCP) for IPv4.

lease proxy client-lease-time

To specify the lease limit each circuit id each interface, use the **lease proxy client-lease-time** command in the DHCP IPv4 sub configuration mode. To disable the lease proxy client-lease-time, use the **no** form of this command.

lease proxy client-lease-time *value*

no lease proxy client-lease-time *value*

Syntax Description

value	Specifies the time in seconds for the lease proxy client. The minimum value of lease proxy client-time is 600 seconds.

Command Default

If you set the default (no), then the lease proxy gets disabled.

Command Modes

DHCP IPv4 configuration

Command History

Release	Modification
Release 4.2.1	This command was introduced.

Usage Guidelines

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

When the binding is created, the client-lease-time is cached on a per-binding basis, thus, the changes to the profile client-lease-time does not cause any impact to any existing bindings. However, changes are effective only for subsequently created bindings.

Task ID

Task ID	Operation
ip-services	read, write

Examples

This is an example of configuring the **lease proxy client-lease-time** command in the DHCP IPv4 sub configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# profile myproxyprofile proxy
RP/0/RSP0/CPU0:router(config-dhcpv4)# lease proxy client-lease-time 600
```

Related Commands

Command	Description
dhcp ipv4 (BNG), on page 145	Enables the Dynamic Host Configuration Protocol (DHCP) for IPv4.

show dhcp ipv4 proxy binding

To show information concerning DHCP client bindings for proxy, use the **show dhcp ipv4 proxy binding** command in the EXEC mode.

show dhcp ipv4 proxy binding [**circuit-id** *circuit_id_name*| **detail**| **interface**| *ipspecifier*| **location**| *locationspecifier*| **mac-address**| **remote-id**| **summary**]{**location**| **vrf**| *vrf_name*}

Syntax Description

circuit-id	Displays the DHCP IPv4 proxy client binding based on circuit ID.
circuit_id_name	Displays the name of the circuit ID.
detail	Displays detailed binding information for DHCP proxy.
interface	Specifies the interface based on which the DHCP bindings are filtered.
ipspecifier	Displays the name of the interface.
location	Specifies the node location of the DHCP proxy.
locationspecifier	Displays the name of the location.
mac-address	Displays detailed client binding information based on mac-address.
remote-id	Displays the DHCP IPv4 proxy client binding based on remote ID.
summary	Displays the summary binding information for proxy.
vrf	Displays the VRF information.
vrf_name	Displays the name of the VRF.
|	Displays the output modifiers.

Command Default

Displays brief information about all DHCP proxy client bindings.

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	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.

Task ID

Task ID	Operations
ip-services	read

Examples

This is the sample output of the **show dhcp ipv4 proxy binding** command:

```
RP/0/RSP0/CPU0:router# show dhcp ipv4 proxy binding
The show dhcp ipv4 proxy binding output is as follows:
                                                                        Lease

 MAC Address      IP Address      State    Remaining      Interface            VRF
Sublabel
--------------          --------------    ---------   ---------       --------------------
  ---------  ----------
0000.6602.0102    1.1.1.1             BOUND    3495         Gi0/1/0/0            default
  0x0


RP/0/RSP0/CPU0:router# show dhcp ipv4 proxy binding mac-address  0000.6602.0102
MAC Address:      0000.6602.0102
IP Address:       1.1.1.1
Profile:          foo
State:            BOUND
Proxy Lease:                    86400 secs (1d00h)
Proxy Lease Remaining:  85942 secs (23:52:22)
Client Lease:                    600 secs (00:10:00)
Client Lease Remaining: 442 secs (00:07:22)
Client ID:        00-00-66-02-01-02
Interface:        GigabitEthernet0/1/0/0.200
VLAN Id:      200
VRF:              default
Subscriber Label: 0x0

RP/0/RSP0/CPU0:router# show dhcp ipv4 proxy binding circuit-id CCCCCCCCCC
MAC Address:      0000.6602.0102
IP Address:       1.1.1.1
circuit-id:  CCCCCCCCCC
remote-id: RRRRRRRRRR
Profile:          foo
State:            BOUND
Proxy Lease:                    86400 secs (1d00h)
Proxy Lease Remaining:  85942 secs (23:52:22)
Client Lease:                    600 secs (00:10:00)
Client Lease Remaining: 442 secs (00:07:22)
Client ID:        00-00-66-02-01-02
Interface:        GigabitEthernet0/1/0/0.200
VLAN Id:      outer 200, inner 300
VRF:              default
Subscriber Label: 0x0

RP/0/RSP0/CPU0:router# show dhcp ipv4 proxy binding remote-id RRRRRRRRRR
MAC Address:      0000.6602.0102
IP Address:       1.1.1.1
Profile:          foo
circuit-id:  CCCCCCCCCC
remote-id: RRRRRRRRRR
State:            BOUND
```

```
Proxy Lease:                    86400 secs (1d00h)
Proxy Lease Remaining:  85942 secs (23:52:22)
Client Lease:                    600 secs (00:10:00)
Client Lease Remaining: 442 secs (00:07:22)
Client ID:         00-00-66-02-01-02
Interface:         GigabitEthernet0/1/0/0
VRF:               default
Subscriber Label: 0x0

RP/0/RSP0/CPU0:router# show dhcp ipv4 proxy binding detail
MAC Address:         ca01.3fcd.0000
VRF:                 default
IP Address:          10.10.10.6
Gateway IP Address: 0.0.0.0
Server IP Address:  11.11.11.3
ReceivedCircuit ID: -
InsertedCircuit ID: -
ReceivedRemote ID:  -
InsertedRemote ID:  -
Profile:             proxyProfile
State:               BOUND
Proxy Lease:                    86400 secs (1d00h)
Proxy Lease Remaining:  85942 secs (23:52:22)
Client Lease:                    600 secs (00:10:00)
Client Lease Remaining: 442 secs (00:07:22)
Client ID:           0x00-0x76-0x6C-0x61-0x6E-0x31-0x30-0x30
Interface:           GigabitEthernet0/1/0/0.100
VLAN:                None
Subscriber Label:   0x0

RP/0/RSP0/CPU0:router# show dhcp ipv4 proxy binding interface Gi0/1/0/0
                                                                    Lease

 MAC Address      IP Address      State    Remaining      Interface            VRF
Sublabel
--------------          ---------------     ---------   ---------       --------------------
  ---------  ----------
0000.6602.0102    1.1.1.1             BOUND    3495         Gi0/1/0/0            default
  0x0
```

Related Commands

Command	Description
dhcp ipv4 (BNG), on page 145	Enables the Dynamic Host Configuration Protocol (DHCP) for IPv4.
show dhcp ipv6 proxy binding (BNG), on page 197	Shows the client bindings for Dynamic Host Configuration Protocol (DHCP) proxy.

show dhcp ipv4 proxy interface (BNG)

To display the proxy interface information for Dynamic Host Configuration Protocol (DHCP) IPv4, use the **show dhcp ipv4 proxy interface** command in EXEC mode.

show dhcp ipv4 proxy interface [*interface-type interface-name*] **[detail]**

Syntax Description

interface-type	Type of the proxy interface.
interface-name	Name of the proxy interface.
detail	Displays the detailed information of proxy interface.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	This command was supported for BNG.

Usage Guidelines

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

Task ID

Task ID	Operation
ip-services	read

Examples

This is a sample output from the **show dhcp ipv4 proxy interface** command:

```
RP/0/RSP0/CPU0:router# show dhcp ipv4 proxy interface bundle-Ether 70.16 detail
Sat Jan  5 14:25:53.484 UTC

Interface:          Bundle-Ether70.16
VRF:                default
Mode:               Proxy
Profile Name:       proxy1
Lease Limit:        per circuit id from AAA 2

Lease Count Details:
```

```
Circuit id from AAA                                              Count
c2                                                               1
```

This table describes the significant fields shown in the display.

Table 9: show dhcp ipv4 proxy interface Command Field Descriptions

Field	Description
Lease Limit	Specifies the lease limit value sent from AAA server.
Count	Specifies the number of sessions on the router having the specific Circuit-ID received from the AAA server.

show dhcp ipv4 proxy profile

To display Dynamic Host Configuration Protocol (DHCP) proxy profile information, use the **show dhcp ipv4 proxy profile** command in the EXEC mode.

show dhcp ipv4 proxy profile {**name** | *profile_name* | }

Syntax Description

name	Displays the detailed proxy profile information.
profile_name	Specifies the profile name.
|	Displays the output modifiers.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

This command displays the proxy profiles created for DHCP IPv4.

Task ID

Task ID	Operations
ip-services	read

Examples

This is the sample output of the **show dhcp ipv4 proxy profile** command:

```
RP/0/RSP0/CPU0:router# show dhcp ipv4 proxy profile
```

The show dhcp ipv4 proxy profile output is as follows:

```
Wed Jan 23 17:05:49.760 IST

DHCP IPv4 Proxy Profiles
------------------------
```

```
DHCP_PROF_IPSUB
```

This table describes the significant fields shown in the display.

Table 10: show dhcp ipv4 proxy profile Field Descriptions

Field	Description
DHCP IPv4 Proxy Profiles	Specifies all the DHCP IPv4 proxy profiles.

show dhcp ipv4 proxy statistics

To display statistics for a specific bridge domain, use the **show dhcp ipv4 proxy statistics** command in the EXEC mode.

show dhcp ipv4 proxy statistics location |]

Syntax Description

location	Specifies the node information for dhcp ipv4 proxy.
|	Displays the output modifiers.

Command Default

Displays a table of DHCP proxy statistics.

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	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.

Task ID

Task ID	Operations
ip-services	read

Examples

This is the sample output of the **show dhcp ipv4 proxy statistics** command:

```
RP/0/RSP0/CPU0:router# show dhcp ipv4 proxy statistics
```

The show dhcp ipv4 proxy statistics output is as follows:

```
Wed Jan 23 17:07:12.386 IST

                  VRF                     |       RX       |       TX       |       DR
|
-------------------------------------------------------------------------------------------
default                                   |            0   |            0   |            0   |
**nVSatellite                             |            0   |            0   |            0   |
```

This table describes the significant fields shown in the display.

Table 11: show dhcp ipv4 proxy statistics Field Descriptions

Field	Description
VRF	Specifies the VRF in the DHCP proxy. The default is nVSatellite.

show dhcp ipv6 proxy binding (BNG)

To display the client bindings for Dynamic Host Configuration Protocol (DHCP) proxy, use the **show dhcp ipv6 proxy binding** command in EXEC mode.

show dhcp ipv6 proxy binding{**detail**| **duid**| **interface**| **interface-id**| **location**| **mac-address**| **remote-id**| **summary**| **vrf**}

Syntax Description

detail	Displays detailed bindings for proxy.
duid	Displays client bindings for DUID.
interface	Displays client bindings by Interface.
interface-id	Displays client bindings by Interface ID.
location	Specifies the node location.
mac-address	Displays detailed client binding information.
remote-id	Displays client binding by Remote ID.
summary	Displays summary bindings for proxy.
vrf	Displays client bindings by VRF name.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.1.1	This command was introduced.
Release 4.3.0	This command was supported for BNG.

Usage Guidelines

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

Task ID

Task ID	Operation
ip-services	read

Examples

This is a sample output from the **show dhcp ipv6 proxy binding** command:

```
RP/0/RSP0/CPU0:router# show dhcp ipv6 proxy binding

Summary:
  Total number of Proxy bindings = 1
Prefix: 2001::/60 (Gi0/0/0/1)
  DUID: 00030001ca004a2d0000
  IAID: 00020001
  lifetime: 2592000
  expiration: Nov 25 2010 16:47

RP/0/RSP0/CPU0:router# show dhcp ipv6 proxy binding summary

Total number of clients: 2

     STATE              |              COUNT             |
                        |     IA-NA     |    IA-PD       |
-------------------------------------------------------------
  INIT                  |            0  |            0   |
  SUB VALIDATING        |            0  |            0   |
  ADDR/PREFIX ALLOCATING|            0  |            0   |
  REQUESTING            |            0  |            0   |
  SESSION RESP PENDING  |            2  |            0   |
  ROUTE UPDATING        |            0  |            0   |
  BOUND                 |            0  |            0   |
```

show dhcp ipv6 proxy interface (BNG)

To display the proxy interface information for Dynamic Host Configuration Protocol (DHCP), use the **show dhcp ipv6 proxy interface** command in EXEC mode.

show dhcp ipv6 proxy interface {*type*| *interface-path-id*} {**location**| *location*}

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.
location	Displays the node location by Interface.
location	Displays the fully qualified location specification of an interface.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
ip-services	read

Examples

This is a sample output from the **show dhcp ipv6 proxy interface** command:

```
RP/0/RSP0/CPU0:router# show dhcp ipv6 proxy interface

Tue Sep  4 19:14:54.056 UTC
Codes: Amb - Ambiguous VLAN, B - Base, R - Relay, P - Proxy,
       SR - Server, S - Snoop, C - Client, INV - Invalid
       CID - Circuit Id, RID - Remote Id, INTF - Interface

Interface              Mode Profile Name                               Amb Lease Limit
-------------------------------------------------------------------------------------
BE1.100                P    pxy1                                       No  None
BE1.200                P    pxy1                                       No  None
BE1.250                P    pxy1                                       Yes None
BE1.400                P    pxy1                                       Yes None
```

show dhcp ipv6 proxy profile

To display the proxy profile information for Dynamic Host Configuration Protocol (DHCP) proxy, use the **show dhcp ipv6 proxy profile** command in EXEC mode.

show dhcp ipv6 proxy profile name *profile_name*{**location**| *location*}

Syntax Description

name	Displays the detailed proxy profile information for the profile.
profile_name	Specifies the name of the profile.
location	Displays the node location by Interface.
location	Displays the fully qualified location specification of an interface.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
ip-services	read

Examples

This is a sample output from the **show dhcp ipv6 proxy profile** command:

```
RP/0/RSP0/CPU0:router# show dhcp ipv6 proxy profile

Tue Sep  4 05:00:57.938 UTC

DHCP IPv6 Proxy Profiles
--------------------------
```

```
pxy1
pxy_pppoe1
pxy_pppoe2
```

show dhcp ipv6 proxy statistics

To display the statistics for Dynamic Host Configuration Protocol (DHCP) proxy, use the **show dhcp ipv6 proxy statistics** command in EXEC mode.

show dhcp ipv6 proxy statistics {**debug**| **location**| **vrf**}

Syntax Description

debug	Displays the debug statistics for the proxy.
location	Displays the node location for the proxy.
vrf	Displays the proxy statistics by VRF.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
ip-services	read

Examples

This is a sample output from the **show dhcp ipv6 proxy statistics** command:

```
RP/0/RSP0/CPU0:router# show dhcp ipv6 proxy statistics

Wed Sep  5 01:10:35.650 UTC

                  VRF                     |       RX       |       TX       |       DR
|
-------------------------------------------------------------------------------------------

 default                                  |           23   |           28   |            0
```

red	0	0	0
blue	0	0	0
green	6	0	0
orange	0	0	0
test_vrf	0	0	0
dhcpclient	0	0	0
dhcpserver	0	0	0

show dhcp ipv6 server binding

To display the client bindings for Dynamic Host Configuration Protocol (DHCP) server, use the **show dhcp ipv6 server binding** command in EXEC mode.

show dhcp ipv6 server binding{**detail**| **duid**| **interface**| **interface-id**| **location**| **mac-address**| **remote-id**| **summary**| **vrf**}

Syntax Description

detail	Displays detailed bindings for proxy.
duid	Displays client bindings for DUID.
interface	Displays client bindings by Interface.
interface-id	Displays client bindings by Interface ID.
location	Specifies the node location.
mac-address	Displays detailed client binding information.
remote-id	Displays client binding by Remote ID.
summary	Displays summary bindings for proxy.
vrf	Displays client bindings by VRF name.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
ip-services	read

Examples This is a sample output from the **show dhcp ipv6 server binding** command:

```
RP/0/RSP0/CPU0:router# show dhcp ipv6 server binding location 0/RSP0/CPU0
Summary:
Total number of clients: 3
  DUID  : 000300010000641e0103
  MAC Address: 0000.641e.0103
  Client Link Local: fe80::200:64ff:fe1e:103
  Sublabel: 0x82f
    IA ID: 0xb100
      STATE: BOUND
      IPv6 Prefix:  2004:4:4:6::/64 (Bundle-Ether2.3)
        lifetime  : 600 secs (00:10:00)
        expiration: 327 secs (00:05:27)
  DUID  : 000300010000641e0104
  MAC Address: 0000.641e.0104
  Client Link Local: fe80::200:64ff:fe1e:104
  Sublabel: 0x870
    IA ID: 0xb101
      STATE: BOUND
      IPv6 Prefix:  2004:4:4:a::/64 (Bundle-Ether2.3)
        lifetime  : 600 secs (00:10:00)
        expiration: 327 secs (00:05:27)
  DUID  : 000300010000641e0105
  MAC Address: 0000.641e.0105
  Client Link Local: fe80::200:64ff:fe1e:105
  Sublabel: 0x8b5
    IA ID: 0xb102
      STATE: BOUND
      IPv6 Prefix:  2004:4:4:b::/64 (Bundle-Ether2.3)
        lifetime  : 600 secs (00:10:00)
        expiration: 397 secs (00:06:37)

RP/0/RSP0/CPU0:router# show dhcp ipv6 server binding summary
Tue Sep  4 04:58:19.580 UTC

Total number of clients: 3

     STATE               |             COUNT             |
                         |     IA-NA     |     IA-PD     |
-------------------------------------------------------------
  INIT                   |            0  |            0  |
  SUB VALIDATING         |            0  |            0  |
  ADDR/PREFIX ALLOCATING |            0  |            0  |
  REQUESTING             |            0  |            0  |
  SESSION RESP PENDING   |            0  |            0  |
  ROUTE UPDATING         |            0  |            0  |
  BOUND                  |            0  |            3  |


RP/0/RSP0/CPU0:router#show dhcp ipv6 server binding detail
Tue Sep  4 04:59:41.765 UTC

Client Link Local:      fe80::200:64ff:fe1e:103
MAC Address:            0000.641e.0103
Profile:                test
Client DUID:            000300010000641e0103
Client Flag:            0x80080811
Subscriber VRF:         abc
Class Name:             -
Access Interface:       Bundle-Ether2.3
Access VRF:             abc
Subscriber Label:       0x82f
VLAN Id:                3
ReceivedRemote ID:      -
ReceivedInterface ID:   -
Prefix Pool Name:       p2
```

```
Address Pool Name:      -
  IA ID:                0xb100
    STATE:              BOUND
      IPv6 Prefix:      2004:4:4:6::/64 (Bundle-Ether2.3)
        lifetime:       600 secs (00:10:00)
        expiration:     515 secs (00:08:35)

Client Link Local:      fe80::200:64ff:fe1e:104
MAC Address:            0000.641e.0104
Profile:                test
Client DUID:            000300010000641e0104
Client Flag:            0x80080811
Subscriber VRF:         abc
Class Name:             -
Access Interface:       Bundle-Ether2.3
Access VRF:             abc
Subscriber Label:       0x870
VLAN Id:                3
ReceivedRemote ID:      -
ReceivedInterface ID:   -
Prefix Pool Name:       p2
Address Pool Name:      -
  IA ID:                0xb101
    STATE:              BOUND
      IPv6 Prefix:      2004:4:4:a::/64 (Bundle-Ether2.3)
        lifetime:       600 secs (00:10:00)
        expiration:     515 secs (00:08:35)

Client Link Local:      fe80::200:64ff:fe1e:105
MAC Address:            0000.641e.0105
Profile:                test
Client DUID:            000300010000641e0105
Client Flag:            0x80080811
Subscriber VRF:         abc
Class Name:             -
Access Interface:       Bundle-Ether2.3
Access VRF:             abc
Subscriber Label:       0x8b5
VLAN Id:                3
ReceivedRemote ID:      -
ReceivedInterface ID:   -
Prefix Pool Name:       p2
Address Pool Name:      -
  IA ID:                0xb102
    STATE:              BOUND
      IPv6 Prefix:      2004:4:4:b::/64 (Bundle-Ether2.3)
        lifetime:       600 secs (00:10:00)
        expiration:     585 secs (00:09:45)
```

show dhcp ipv6 server interface

To display the server interface information for Dynamic Host Configuration Protocol (DHCP), use the **show dhcp ipv6 server interface** command in EXEC mode.

show dhcp ipv6 server interface {*type*| *interface-path-id*} {**location**| *location*}

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 (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/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	Displays the node location by Interface.
location	Displays the fully qualified location specification of an interface.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
ip-services	read

Examples

This is a sample output from the **show dhcp ipv6 server interface** command:

```
RP/0/RSP0/CPU0:router# show dhcp ipv6 server interface bundle-Ether 2.3

Tue Sep  4 05:02:03.861 UTC

Interface:          Bundle-Ether2.3
VRF:                abc
Mode:               Server
Profile Name:       test
Lease Limit:        None
```

show dhcp ipv6 server profile

To display the server profile information for Dynamic Host Configuration Protocol (DHCP) server, use the **show dhcp ipv6 server profile** command in EXEC mode.

show dhcp ipv6 server profile name *profile_name*{**location**| *location*}

Syntax Description

name	Displays the detailed proxy profile information for the profile.
profile_name	Specifies the name of the profile.
location	Displays the node location by Interface.
location	Displays the fully qualified location specification of an interface.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
ip-services	read

Examples

This is a sample output from the **show dhcp ipv6 server profile** command:

```
RP/0/RSP0/CPU0:router# show dhcp ipv6 server profile name test

Tue Sep  4 05:00:57.938 UTC

Profile: test
DNS Addresses:None
```

```
Client Lease Time: 0 secs (00:00:00)
Framed Address Pool: p1
Delegated Prefix Pool: p2
Interface References:
Bundle-Ether2.3
```

show dhcp ipv6 server statistics

To display the statistics for Dynamic Host Configuration Protocol (DHCP) server, use the **show dhcp ipv6 server statistics** command in EXEC mode.

show dhcp ipv6 server statistics{**debug**| **location**| **vrf**}

Syntax Description

debug	Displays the debug statistics for the proxy.
location	Displays the node location for the proxy.
vrf	Displays the proxy statistics by VRF.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
ip-services	read

Examples

This is a sample output from the **show dhcp ipv6 server statistics** command:

```
RP/0/RSP0/CPU0:router# show dhcp ipv6 server statistics

  Tue Sep  4 19:13:47.472 UTC

                  VRF                     |       RX       |       TX       |       DR
|
-------------------------------------------------------------------------------------------

 default                                  |        10003   |        11651   |            3
```

```
|
 red                                 |           0   |           0   |           0
|
 blue                                |           0   |           0   |           0
|
 green                               |           0   |           0   |           0
|
 orange                              |           0   |           0   |           0
|
 test_vrf                            |           0   |           0   |           0
|
 dhcpclient                          |           0   |           0   |           0
|
 dhcpserver                          |           0   |           0   |           0
|
```

Dynamic Template Commands

This module describes the Cisco IOS XR software commands used to configure the Dynamic Template commands for Broadband Network Gateway (BNG) on the Cisco ASR 9000 Series Router. For details regarding the related configurations, refer to the *Cisco ASR 9000 Series Aggregation Services Router Broadband Network Gateway Configuration Guide*.

- dynamic-template, page 216
- dynamic-template type ipsubscriber, page 218
- dynamic-template type ppp, page 220
- dynamic-template type service, page 222
- monitor-session (interface-dynamic-template-BNG), page 224
- service-policy (BNG), page 226
- test radius coa activate, page 228
- timeout idle, page 230
- vrf (dynamic-template-BNG), page 232

dynamic-template

To group a set of configuration items that can be applied to a group of subscribers and to enter the dynamic-template configuration mode, use the **dynamic-template** command in the global configuration mode. To disable this feature and exit the dynamic-template configuration mode, use the **no** form of this command.

dynamic-template type {**ipsubscriber** *name*| **ppp** *name*| **service** *name*}

no dynamic-template

Syntax Description

type	Specifies the type of templates, for example, ppp or ipsubscriber or service.
name	Specifies the name of the dynamic template type.
ipsubscriber	Specifies the ipsubscriber dynamic template type.
ppp	Specifies the ppp dynamic template type.
service	Specifies the service dynamic template type.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

Use the **dynamic-template** command to enter dynamic template configuration mode.

Task ID

Task ID	Operation
config-services	read, write

Examples

This is an example of configuring the **dynamic-template** command in the global configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template
RP/0/RSP0/CPU0:router(config-dynamic-template)#
```

Related Commands

Command	Description
dynamic-template type ppp, on page 220	Enables the ppp dynamic template type.
dynamic-template type ipsubscriber, on page 218	Enables the ipsubscriber dynamic template type.
dynamic-template type service, on page 222	Enables the service dynamic template type.

dynamic-template type ipsubscriber

To group a set of configuration items that can be applied to a group of subscribers based on the ipsubscriber template type and to enter the dynamic-template configuration mode, use the **dynamic-template type ipsubscriber** command. To disable this feature and exit the dynamic-template configuration mode, use the **no** form of this command.

dynamic-template type ipsubscriber *template-name*

no dynamic-template type ipsubscriber *template-name*

Syntax Description

template-name	Specifies the dynamic template name.

Command Default

None

Command Modes

Dynamic template configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

Use the **dynamic-template** command to enter dynamic template configuration mode.

Task ID

Task ID	Operation
config-services	read, write

Examples

This is an example of configuring the **dynamic-template type ipsubscriber** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template
RP/0/RSP0/CPU0:router(config-dynamic-template)# type ipsubscriber ipsub1
```

Related Commands

Command	Description
dynamic-template, on page 216	Enables the dynamic template configuration mode.
dynamic-template type ppp, on page 220	Enables the ppp dynamic template type.

Command	Description
dynamic-template type service, on page 222	Enables the service dynamic template type.

dynamic-template type ppp

To group a set of configuration items that can be applied to a group of subscribers based on the ppp template type and to enter the dynamic-template configuration mode, use the **dynamic-template type ppp** command. To disable this feature and exit the dynamic-template configuration mode, use the **no** form of this command.

dynamic-template type ppp *template-name*

no dynamic-template type ppp *template-name*

Syntax Description

template-name	Specifies the dynamic template name.

Command Default

None

Command Modes

Dynamic template configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

Use the **dynamic-template** command to enter dynamic template configuration mode.

Task ID

Task ID	Operation
config-services	read, write

Examples

This is an example of configuring the **dynamic-template type ppp** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template
RP/0/RSP0/CPU0:router(config-dynamic-template)# type ppp p1
```

Related Commands

Command	Description
dynamic-template, on page 216	Enables the dynamic template configuration mode.
dynamic-template type ipsubscriber, on page 218	Enables the ipsubscriber dynamic template type.

Command	Description
dynamic-template type service, on page 222	Enables the service dynamic template type.

dynamic-template type service

To group a set of configuration items that can be applied to a group of subscribers based on the service template type and to enter the dynamic-template configuration mode, use the **dynamic-template type service** command. To disable this feature and exit the dynamic-template configuration mode, use the **no** form of this command.

dynamic-template type service *template-name*

no dynamic-template type service *template-name*

Syntax Description

template-name	Specifies the dynamic template name.

Command Default

None

Command Modes

Dynamic template configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

Use the **dynamic-template** command to enter dynamic template configuration mode.

Task ID

Task ID	Operation
config-services	read, write

Examples

This is an example of configuring the **dynamic-template type service** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template
RP/0/RSP0/CPU0:router(config-dynamic-template)# type service s1
```

Related Commands

Command	Description
dynamic-template, on page 216	Enables the dynamic template configuration mode.

Command	Description
dynamic-template type ppp, on page 220	Enables the ppp dynamic template type.
dynamic-template type ipsubscriber, on page 218	Enables the ipsubscriber dynamic template type.

monitor-session (interface-dynamic-template-BNG)

To associate a traffic mirroring session with a specific interface, use the **monitor-session** command in interface configuration mode or dynamic-template configuration mode. To remove the association between a traffic mirroring session and an interface, use the **no** form of this command.

monitor-session *session-name* [**direction** {**rx-only**| **tx-only**}]

no monitor-session *session-name* [**direction** {**rx-only**| **tx-only**}]

Syntax Description

session-name	Name of the monitor session to configure.
direction	Specifies that traffic replication is in only one direction.
rx-only	Specifies that only ingress traffic is replicated.
tx-only	Specifies that only egress traffic is replicated.

Command Default

Replicates both ingress and egress traffic.

Command Modes

Interface configuration

Dynamic template configuration (for BNG)

Command History

Release	Modification
Release 3.9.1	This command was introduced.
Release 4.0.0	The **acl** and **mirror first** keywords were added.
Release 5.1	The support for this command under dynamic-template configuration mode was added for BNG.

Usage Guidelines

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

Before you can associate a traffic mirroring session to a specific interface, you must define it using the **monitor-session** global configuration command. After the traffic mirroring session is defined, use the **monitor-session** interface configuration command or dynamic template configuration command to associate this session with a specific source interface. For BNG sessions, the subscriber is attached to the monitor session, only when the dynamic template is applied to the subscriber. When the session is associated, all

specified traffic on the interface is then replicated to the destination location defined in the monitor session configuration.

The **monitor-session** interface configuration command also enters monitor session configuration mode for you to configure additional features of the mirroring session.

Task ID

Task ID	Operations
interface	read, write
config-services	read, write

Examples

This example shows how to enter monitor session configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet0/0/0/11
RP/0/RSP0/CPU0:router(config-if)# l2transport
RP/0/RSP0/CPU0:router(config-if-l2)# monitor-session mon1
RP/0/RSP0/CPU0:router(config-if-mon)#
```

This example shows how to configure **monitor-session** command in the dynamic-template configuration mode for BNG:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp ppp_template
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# monitor-session mon1 direction rx-only

RP/0/RSP0/CPU0:router(config-dynamic-template-type)# acl
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# mirror first 100
```

service-policy (BNG)

To associate a service-policy to the dynamic template, use the **service-policy** command in the dynamic template configuration mode. To disable this feature, use the **no** form of this command.

service-policy {**input**| **output**| **type**} *service-policy_name* **[acct-stats]** [**merge** *seq_num*]

no service-policy

Syntax Description

input	Configures an ingress service-policy.
output	Configures an egress service-policy.
type	Creates the service policy for policy-based routing (PBR).
service-policy_name	Name of the service policy.
acct-stats	(Optional) Enables service accounting.
merge	(Optional) Enables the policy to be merged.
seq_num	Sequence number of the policy. Range is from 0 to 255.

Command Default

None

Command Modes

Dynamic template configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.
Release 4.3.0	Support was added for policy based routing.
Release 4.3.1	**acct-stats** and **merge** keywords were added to support service accounting and policy merge features.

Usage Guidelines

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

Use the **dynamic-template type ppp** command to enter the ppp dynamic template type configuration mode.

Task ID

Task ID	Operation
qos	read, write

Examples

This is an example of configuring the **service-policy** command in the dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# accounting aaa list default type session
 periodic-interval 60 dual-stack-delay 1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# service-policy input i1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# service-policy output o1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# service-policy type pbr pbr_policy
```

This example shows how to enable service accounting feature in the dynamic template configuration mode using **service-policy** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template type service s1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# accounting aaa list l1 type service
periodic-interval 500
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv4 access-group ACL1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# service-policy input QoS1 acct-stats
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# service-policy output QoS2 acct-stats
```

This example shows how to merge policy maps using **service-policy** command in the dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template type service MyService
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# service-policy input i1 merge 20
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# service-policy output o1 merge 30
```

Related Commands

Command	Description
dynamic-template, on page 216	Enables the dynamic template configuration mode.
dynamic-template type ppp, on page 220	Enables the ppp dynamic template type.
dynamic-template type ipsubscriber, on page 218	Enables the ipsubscriber dynamic template type.
accounting aaa list type service, on page 5	Configures service accounting feature.

test radius coa activate

To enable Traffic Mirroring, also known as Switch Port Analyzer (SPAN), on a BNG subscriber interface, use the **test radius coa activate** command in EXEC mode. To disable SPAN, use the **deactivate** form of this command.

test radius coa activate service *name* **acct-ses-id** *id*

test radius coa deactivate service *name* **acct-ses-id** *id*

Syntax Description

service	Specifies the service to be activated or de-activated.
name	Name of the service, which is same as the dynamic-template name.
acct-ses-id	Specifies the accounting session ID of the subscriber on which the template is to be activated or de-activated.
id	ID of the accounting session, in hexadecimal format .

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 5.1	This command was introduced.

Usage Guidelines

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

Configure monitor sessions (using **monitor-session** command in global configuration mode) and configure source interface attachment to a monitor session (using dynamic templates), as a pre-requisite for executing **test radius coa activate** command.

Task ID

Task ID	Operation
network	read, write

Examples

This example shows how to enable SPAN on BNG subscriber interface by associating a dynamic template with a specific subscriber :

```
RP/0/RSP0/CPU0:router# test radius coa activate acct-ses-id 0x00000001 service service1
```

This example shows how to disable SPAN on BNG subscriber interface by dis-associating a dynamic template with a specific subscriber :

```
RP/0/RSP0/CPU0:router# test radius coa deactivate acct-ses-id 0x00000001 service service1
```

Related Commands

Command	Description
monitor-session	Defines a traffic mirroring session and enters monitor session configuration mode.
monitor-session (interface-dynamic-template-BNG)	Associates a traffic mirroring session with a specific interface or dynamic template.
show monitor-session status	Displays status information about configured traffic mirroring sessions.
show monitor-session counters	Displays statistics regarding traffic mirroring sessions.
clear monitor-session counters	Clears the traffic mirroring session statistics.

timeout idle

To configure an idle timeout period for the IPoE and PPPoE subscriber sessions on BNG, use the **timeout idle** command in dynamic template type configuration mode. To disable this feature, use the **no** form of this command.

timeout idle *seconds* [**threshold** *rate*] [**traffic** {**both**| **inbound**| **outbound**}]

no timeout idle *seconds* [**threshold** *duration*] [**traffic** {**both**| **inbound**| **outbound**}]

Syntax Description

seconds	Idle timeout value for the subscriber sessions, in seconds. The range is from 60 to 4320000.
threshold	Configures a threshold to track the duration of session idleness.
duration	Duration of threshold, in minute(s) per packet. The range is from 1 to 10000. Default is 0. **Note** This value should be less than the idle timeout value.
traffic	Considers the direction of traffic while deriving the duration of session idleness. The default is inbound direction.
both	Considers inbound and outbound traffic while deriving the duration of session idleness.
inbound	Considers inbound traffic only while deriving the duration of session idleness.
outbound	Considers outbound traffic only while deriving the duration of session idleness.

Command Default

None

Command Modes

Dynamic template type configuration

Command History

Release	Modification
Release 4.2.1	This command was introduced.

Release	Modification
Release 5.1	The support for **threshold** and **traffic** keywords were added.

Usage Guidelines

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

In Cisco IOS XR software release 4.2.1, both the IPoE and PPPoE sessions are retained idle, when the idle timeout period expires. In Cisco IOS XR software release 4.2.3, only the IPoE sessions are terminated when the idle timeout period expires. Whereas, the PPPoE sessions are retained idle. From Cisco IOS XR software release 5.1.0 and later, both IPoE and PPPoE sessions are terminated on the expiry of the idle timeout period.

If packets sent or received by BNG, in the configured threshold interval is less than that threshold value, then that particular session is considered idle. For instance, if the **threshold** is configured as 2 packets/minute, and, if the number of packets received in every 2 minutes is only less than 2 (either 0 or 1), then that particular session is considered as idle. Whereas, if the number of packets received is 2 or above, then that session is considered as active.

By default, the sessions are disconnected if the **threshold** is not configured.

Task ID

Task ID	Operation
config-services	read, write

Examples

This example shows how to configure an idle timeout of 200 seconds, with a threshold of 2 minutes/packet and considering inbound and outbound traffic for determining the duration of session idleness:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp ppp1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# timeout idle 200 threshold 2 traffic
both
```

Related Commands

Command	Description
show subscriber feature accounting, on page 491	Displays the feature accounting information of the subscriber.

vrf (dynamic-template-BNG)

To set the vrf in which the interface operates, use the **vrf** command in the dynamic template type configuration mode. To disable the VRF, use the **no** form of this command.

vrf *vrf-name*

no vrf

Syntax Description

vrf_name	Specifies the name of the vrf.

Command Default

None

Command Modes

Dynamic template type configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

Use the **dynamic-template** command to enter dynamic template configuration mode.

Task ID

Task ID	Operation
config-services	read, write

Examples

This is an example of configuring the **vrf** command in the dynamic template type configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template
RP/0/RSP0/CPU0:router(config-dynamic-template)# type service s1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# vrf vrf1
```

Related Commands

Command	Description
dynamic-template, on page 216	Enables the dynamic template configuration mode.
dynamic-template type ppp, on page 220	Enables the ppp dynamic template type.

Command	Description
dynamic-template type ipsubscriber, on page 218	Enables the ipsubscriber dynamic template type.

Excessive Punt Flow Trap Commands

This module describes the Cisco IOS XR software commands used to configure the Excessive Punt Flow Trap commands for Broadband Network Gateway (BNG) on the Cisco ASR 9000 Series Router. For details regarding the related configurations, refer to the *Cisco ASR 9000 Series Aggregation Services Router Broadband Network Gateway Configuration Guide*.

- lpts punt excessive-flow-trap, page 236
- lpts punt excessive-flow-trap non-subscriber-interfaces, page 238
- lpts punt excessive-flow-trap penalty-rate, page 239
- lpts punt excessive-flow-trap penalty-timeout, page 241
- lpts punt excessive-flow-trap subscriber-interfaces, page 243
- show lpts punt excessive-flow-trap, page 244
- show lpts punt excessive-flow-trap information, page 247
- show lpts punt excessive-flow-trap interface, page 250
- show lpts punt excessive-flow-trap protocol, page 253

lpts punt excessive-flow-trap

To activate the Excessive Punt Flow Trap feature and to enter the control plane policer configuration mode, use the **lpts punt excessive-flow-trap** command in global configuration mode. To exit the control plane policer configuration mode and disable the Excessive Punt Flow Trap feature, use the **no** form of this command.

lpts punt excessive-flow-trap {**subscriber-interfaces**| **non-subscriber-interfaces**| **penalty-rate**| **penalty-timeout**}

no lpts punt excessive-flow-trap {**subscriber-interfaces**| **non-subscriber-interfaces**| **penalty-rate**| **penalty-timeout**}

Syntax Description

subscriber-interfaces	Enables the Excessive Punt Flow Trap for subscriber interfaces.
non-subscriber-interfaces	Enables the Excessive Punt Flow Trap for non-subscriber interfaces.
penalty-rate	Sets the penalty policing rate for a protocol.
penalty-timeout	Sets the penalty timeout for a protocol.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
config-services	read, write

Examples

This example shows how to enable the Excessive Punt Flow Trap feature in the global configuration mode:

```
RP/0/RSP0/CPU0:router(config)# lpts punt excessive-flow-trap
RP/0/RSP0/CPU0:router(config-control-plane-policer)#
```

Related Commands

Command	Description
show lpts punt excessive-flow-trap, on page 244	Displays the running configuration for the Excessive Punt Flow Trap feature.

lpts punt excessive-flow-trap non-subscriber-interfaces

To enable the Excessive Punt Flow Trap feature on non-subscriber interfaces, use the **lpts punt excessive-flow-trap non-subscriber-interfaces** command in global configuration mode. To disable the Excessive Punt Flow Trap feature on subscriber interfaces, use the **no** form of this command.

lpts punt excessive-flow-trap non-subscriber-interfaces

no lpts punt excessive-flow-trap non-subscriber-interfaces

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
config-services	read, write

Examples

This example shows how to enable the Excessive Punt Flow Trap feature on the non-subscriber interfaces in the global configuration mode:

```
RP/0/RSP0/CPU0:router(config)# lpts punt excessive-flow-trap non-subscriber-interfaces
RP/0/RSP0/CPU0:router(config)#
```

Related Commands

Command	Description
show lpts punt excessive-flow-trap, on page 244	Displays the running configuration for the Excessive Punt Flow Trap feature.

lpts punt excessive-flow-trap penalty-rate

To set the penalty policing rate for a protocol, use the **lpts punt excessive-flow-trap penalty-rate** command in global configuration mode. To restore the default penalty-rate, use the **no** form of this command.

lpts punt excessive-flow-trap penalty-rate{**trace**| **arp**| **icmp**| **dhcp**| **pppoe**| **ppp**| **igmp**| **ip**| **l2tp**| **all**| **interface**| **information**} *penalty_rate*

no punt excessive-flow-trap penalty-rate{**trace**| **arp**| **icmp**| **dhcp**| **pppoe**| **ppp**| **igmp**| **ip**| **l2tp**| **all**| **interface**| **information**}

Syntax Description

default	Sets the default penalty policing rate for all protocols.
arp	Sets the penalty policing rate for the ARP protocol.
icmp	Sets the penalty policing rate for the ICMP protocol.
dhcp	Sets the penalty policing rate for the DHCP protocol.
pppoe	Sets the penalty policing rate for the PPPoE protocol.
ppp	Sets the penalty policing rate for the PPP protocol.
igmp	Sets the penalty policing rate for the IGMP protocol.
ip	Sets the penalty policing rate for the IPv4 protocol.
l2tp	Sets the penalty policing rate for the L2TP protocol.

Command Default

The default *packets per seconds(pps)* is 10 pps.

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
config-services	read, write

Examples

This example shows how to set the penalty policing rate of 4 pps for the ARP protocol in the global configuration mode:

```
RP/0/RSP0/CPU0:router(config)# lpts punt excessive-flow-trap penalty-rate arp 4
RP/0/RSP0/CPU0:router(config)#
```

Related Commands

Command	Description
lpts punt excessive-flow-trap, on page 236	Enables the Excessive Punt Flow Trap feature.

lpts punt excessive-flow-trap penalty-timeout

To set the penalty timeout value for a protocol, use the **lpts punt excessive-flow-trap penalty-timeout** command in global configuration mode. To restore the default penalty timeout value, use the **no** form of this command.

lpts punt excessive-flow-trap penalty-timeout{**trace**| **arp**| **icmp**| **dhcp**| **pppoe**| **ppp**| **igmp**| **ip**| **l2tp**| **all**| **interface**| **information**} *timeout*

no lpts punt excessive-flow-trap penalty-timeout{**trace**| **arp**| **icmp**| **dhcp**| **pppoe**| **ppp**| **igmp**| **ip**| **l2tp**| **all**| **interface**| **information**}

Syntax Description

default	Sets the default penalty timeout for all protocols.
arp	Sets the penalty timeout for the ARP protocol.
icmp	Sets the penalty timeout for the ICMP protocol.
dhcp	Sets the penalty timeout for the DHCP protocol.
pppoe	Sets the penalty timeout for the PPPoE protocol.
ppp	Sets the penalty timeout for the PPP protocol.
igmp	Sets the penalty timeout for the IGMP protocol.
ip	Sets the penalty timeout for the IPv4 protocol.
l2tp	Sets the penalty timeout for the L2TP protocol.

Command Default

The default value in *minutes* is 15.

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
config-services	read, write

Examples

This example shows how to set the penalty timeout value of 70 minutes for the DHCP protocol in the global configuration mode:

```
RP/0/RSP0/CPU0:router(config)# lpts punt excessive-flow-trap penalty-timeout dhcp 70
RP/0/RSP0/CPU0:router(config)#
```

Related Commands

Command	Description
lpts punt excessive-flow-trap, on page 236	Enables the Excessive Punt Flow Trap feature.

lpts punt excessive-flow-trap subscriber-interfaces

To enable the Excessive Punt Flow Trap feature on subscriber interfaces, use the **lpts punt excessive-flow-trap subscriber-interfaces** command in global configuration mode. To disable the Excessive Punt Flow Trap feature on subscriber interfaces, use the **no** form of this command.

lpts punt excessive-flow-trap subscriber-interfaces

no lpts punt excessive-flow-trap subscriber-interfaces

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
config-services	read, write

Examples

This example shows how to enable the Excessive Punt Flow Trap feature for subscriber interfaces in the global configuration mode:

```
RP/0/RSP0/CPU0:router(config)# lpts punt excessive-flow-trap subscriber-interfaces
RP/0/RSP0/CPU0:router(config)#
```

Related Commands

Command	Description
show lpts punt excessive-flow-trap, on page 244	Displays the running configuration for the Excessive Punt Flow Trap feature.

show lpts punt excessive-flow-trap

To display the running configuration for the Excessive Punt Flow Trap feature, use the **show lpts punt excessive-flow-trap** command in the EXEC mode.

show lpts punt excessive-flow-trap {*protocol*| **interface**| *type*| *interface-path-id*| **information**}

Syntax Description

protocol	Enter the protocol type. • arp—Displays ARP bad actors. • icmp—Displays ICMP bad actors. • dhcp—Displays DHCP bad actors. • pppoe—Displays PPPoE bad actors. • ppp—Displays PPP bad actors. • igmp—Displays IGMP bad actors. • ipv4—Displays IPv4 bad actors. • l2tp—Displays L2TP bad actors. • all—Displays bad actors for all protocols.
interface	Displays the bad actors on an interface. For more information on the interface types, use the question mark (?) online help function.
type	Specifies the 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.
information	Displays the Excessive Punt Flow Trap feature information.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
lpts	read
basic-services	read, write

Examples

The **show running-config** output for the above **show lpts punt excessive-flow-trap** command is:

```
RP/0/RSP0/CPU0:router# show running-config lpts punt excessive-flow-trap
lpts punt excessive-flow-trap
 penalty-rate arp 15
 penalty-rate pppoe 25
 penalty-timeout arp 2
 non-subscriber-interfaces
```

This table describes the significant fields shown in the display.

Table 12: show lpts punt excessive-flow-trap Field Descriptions

Field	Description
penalty-rate	The penalty policing rate for a protocol. For arp the value is 15 and for pppoe the value is 2.
penalty-timeout	The penalty timeout value for a protocol. For arp the value is 2.

Related Commands

Command	Description
lpts punt excessive-flow-trap, on page 236	Enables the Excessive Punt Flow Trap feature.

show lpts punt excessive-flow-trap information

To display the Excessive Punt Flow Trap feature information, use the **show lpts punt excessive-flow-trap information** command in the EXEC mode.

show lpts punt excessive-flow-trap information

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
lpts	read
basic-services	read, write

Examples

This is an example of **show lpts punt excessive-flow-trap information** command with ARP and PPPoE protocols configured with non-default values:

```
RP/0/RSP0/CPU0:router# show lpts punt excessive-flow-trap information

------------------------------------------------------------
  Global Default Values -
         Police Rate: 10 pps
     Penalty Timeout: 15 mins

------------------------------------------------------------
              Police          Penalty
              Rate (pps)      Timeout (mins)
 Protocol   Default Config   Default Config   Punt Reasons
 --------   --------------   --------------   ----------------
 ARP           10     15        15      2     ARP
                                              Reverse ARP
```

```
                                                Dynamic ARP Inspection (DAI)

ICMP            10      -          15      -    ICMP
                                                ICMP-local
                                                ICMP-app
                                                ICMP-control
                                                ICMP-default

DHCP            10      -          15      -    DHCP Snoop Request
                                                DHCP Snoop Reply

PPPOE           10      25         15      -    PPP over Ethernet (PPPoE)
                                                PPPoE packets for RSP
                                                PPPoE packet/config mismatch
                                                PPPoE packet/config mismatch for RSP

PPP             10      -          15      -    Point-to-Point Protocol (PPP)
                                                PPP packets for RSP

IGMP            10      -          15      -    IGMP
                                                IGMP Snoop
                                                MLD Snoop

IPv4/v6         10      -          15      -    IP Subscriber (IPSUB)
                                                IPv4 options
                                                IPv4 FIB
                                                IPv4 TTL exceeded
                                                IPv4 fragmentation needed
                                                IPv4/v6 adjacency
                                                IPV4/v6 unknown IFIB
                                                UDP-known
                                                UDP-listen
                                                Generic Routing Encap (GRE) bad flags
                                                UDP-default
                                                TCP-known
                                                TCP-listen
                                                TCP-cfg-peer
                                                TCP-default
                                                Raw-listen
                                                Raw-default

L2TP            10      -          15      -    Layer 2 Tunneling Protocol, version 2 (L2TPv2)

                                                L2TPv2-default
                                                L2TPv2-known
                                                L2TPv3
```

The corresponding **show running-config** output for the above **show lpts punt excessive-flow-trap information** command is:

```
RP/0/RSP0/CPU0:router# show running-config lpts punt excessive-flow-trap
lpts punt excessive-flow-trap
 penalty-rate arp 15
 penalty-rate pppoe 25
 penalty-timeout arp 2
 non-subscriber-interfaces
```

This table describes the significant fields shown in the display.

Table 13: show lpts punt excessive-flow-trap information Field Descriptions

Field	Description
penalty-rate	The penalty policing rate for a protocol. For arp the value is 15 and for pppoe the value is 25.

Field	Description
penalty-timeout	The penalty timeout value for a protocol. For arp the value is 2.

Related Commands

Command	Description
lpts punt excessive-flow-trap, on page 236	Enables the Excessive Punt Flow Trap feature.

show lpts punt excessive-flow-trap interface

To display the penalty status of an interface for one or all protocols, use the **show lpts punt excessive-flow-trap interface** command in the EXEC mode.

show lpts punt excessive-flow-trap interface *type interface-path-id* [*protocol*]

Syntax Description

type	Specifies the 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: • 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.
protocol	Specifies the protocol type. • arp—Displays ARP bad actors. • icmp—Displays ICMP bad actors. • dhcp—Displays DHCP bad actors. • pppoe—Displays PPPoE bad actors. • ppp—Displays PPP bad actors. • igmp—Displays IGMP bad actors. • ipv4—Displays IPv4 bad actors. • l2tp—Displays L2TP bad actors. • all—Displays bad actors for all protocols.

Command Default None

Command Modes EXEC

Command History

Release	Modification
Release 4.3.0	This command was introduced.

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

Task ID

Task ID	Operation
lpts	read
basic-services	read, write

Examples The sample output for the **show lpts punt excessive-flow-trap ip** command is:

```
RP/0/RSP0/CPU0:router# show lpts punt excessive-flow-trap ip
Interface: Bundle-Ether1.100
         Intf Handle: 0x08000320                          Location: 0/6/CPU0
            Protocol: IPv4/v6                         Punt Reason: Raw-default
        Penalty Rate: 10 pps                       Penalty Timeout: 15 mins

      Time Remaining: 14 mins 31 secs
```

This table describes the significant fields shown in the display.

Table 14: show lpts punt excessive-flow-trap interface Field Descriptions

Field	Description
Intf Handle	The interface handler for the Bundle Ether interface.
location	The location of the interface.
protocol	Specifies if it uses the IPv4 or IPv6 protocol.
punt reason	The reason to punt the excessive flow trap.
penalty-rate	The penalty policing rate for a protocol in pps.

Field	Description
penalty-timeout	The penalty timeout value for a protocol in minutes.

Related Commands

Command	Description
lpts punt excessive-flow-trap, on page 236	Enables the Excessive Punt Flow Trap feature.

show lpts punt excessive-flow-trap protocol

To display a list of interfaces that are in the penalty box for one or all protocols, use the **show lpts punt excessive-flow-trap** *protocol* command in the EXEC mode.

show lpts punt excessive-flow-trap *protocol*

Syntax Description

protocol	Enter the protocol type. • arp—Displays ARP bad actors. • icmp—Displays ICMP bad actors. • dhcp—Displays DHCP bad actors. • pppoe—Displays PPPoE bad actors. • ppp—Displays PPP bad actors. • igmp—Displays IGMP bad actors. • ipv4—Displays IPv4 bad actors. • l2tp—Displays L2TP bad actors. • all—Displays bad actors for all protocols.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

The *protocol* option in the **show lpts punt excessive-flow-trap** *protocol* command points to the protocol type. The show output for each of the protocol differs depending on the protocol type you select on the router.

Task ID

Task ID	Operation
lpts	read
basic-services	read, write

Examples

The sample output for the **show lpts punt excessive-flow-trap ip** command is:

```
RP/0/RSP0/CPU0:router# show lpts punt excessive-flow-trap ip
Interface: Bundle-Ether1.100
         Intf Handle: 0x08000320                          Location: 0/6/CPU0
            Protocol: IPv4/v6                          Punt Reason: Raw-default
        Penalty Rate: 10 pps                       Penalty Timeout: 15 mins

      Time Remaining: 14 mins 31 secs
```

This table describes the significant fields shown in the display.

Table 15: show lpts punt excessive-flow-trap interface Field Descriptions

Field	Description
Intf Handle	The interface handler for the Bundle Ether interface.
location	The location of the interface.
protocol	Specifies if it uses the IPv4 or IPv6 protocol.
punt reason	The reason to punt the excessive flow trap.
penalty-rate	The penalty policing rate for a protocol in pps.
penalty-timeout	The penalty timeout value for a protocol in minutes.

Related Commands

Command	Description
lpts punt excessive-flow-trap, on page 236	Enables the Excessive Punt Flow Trap feature.

IPoE Commands

This module describes the Cisco IOS XR software commands used to configure the IPoE commands for Broadband Network Gateway (BNG) on the Cisco ASR 9000 Series Router. For details regarding the related configurations, refer to the *Cisco ASR 9000 Series Aggregation Services Router Broadband Network Gateway Configuration Guide*.

- initiator dhcp, page 256
- initiator unclassified-source, page 258
- ipsubscriber interface, page 260
- ipsubscriber l2-connected, page 262
- ipsubscriber routed, page 264
- ipsubscriber session-limit, page 266
- show ipsubscriber access-interface, page 268
- show ipsubscriber interface, page 271
- show ipsubscriber summary, page 275

initiator dhcp

To enable DHCP as first-sign-of-life protocol for IPv4 or IPv6 subscriber, use the **initiator dhcp** command in the appropriate configuration submode. To disable this feature, use the **no** form of this command.

initiator dhcp

no initiator dhcp

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

IP subscriber IPv4 L2-connected configuration

IP subscriber IPv6 L2-connected configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.
Release 4.3.0	Supported was added for IPv6.

Usage Guidelines

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

Task ID

Task ID	Operation
network	read, write

Examples

This is an example of configuring the **initiator dhcp** command in the Interface configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether 56
RP/0/RSP0/CPU0:router(config-if)# ipsubscriber ipv4 l2-connected
RP/0/RSP0/CPU0:router(config-if-ipsub-ipv4-l2conn)# initiator dhcp
```

This is an example of configuring the **initiator dhcp** command in the Interface configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether 56
RP/0/RSP0/CPU0:router(config-if)# ipsubscriber ipv6 l2-connected
RP/0/RSP0/CPU0:router(config-if-ipsub-ipv6-l2conn)# initiator dhcp
```

Related Commands

Command	Description
show ipsubscriber summary, on page 275	Displays the ipsubscriber information.

initiator unclassified-source

To enable unclassified packets as first-sign-of-life for IPv4 or IPv6 subscriber, use the **initiator unclassified-source** command in the appropriate configuration submode. To disable this feature, use the **no** form of this command.

initiator unclassified-source

no initiator unclassified-source

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

IP subscriber IPv4 L2-connected configuration

IP subscriber IPv6 L2-connected configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.
Release 4.3.0	Supported was added for IPv6.

Usage Guidelines

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

Task ID

Task ID	Operation
network	read, write

Examples

This is an example of configuring the **initiator unclassified-source** command in the IP subscriber IPv4 L2-connected configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether 56
RP/0/RSP0/CPU0:router(config-if)# ipsubscriber ipv4 l2-connected
RP/0/RSP0/CPU0:router(config-if-ipsub-ipv4-l2conn)# initiator unclassified-source
```

This is an example of configuring the **initiator unclassified-source** command in the IP subscriber IPv6 L2-connected configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether 56
RP/0/RSP0/CPU0:router(config-if)# ipsubscriber ipv6 l2-connected
RP/0/RSP0/CPU0:router(config-if-ipsub-ipv6-l2conn)# initiator unclassified-source
```

Related Commands

Command	Description
show ipsubscriber summary, on page 275	Displays the ipsubscriber information.

ipsubscriber interface

To enable interface based static session in BNG, use the **ipsubscriber interface** command in the interface configuration mode. To remove the static session, use the **no** form of this command.

ipsubscriber interface

no ipsubscriber interface

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.1.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
network	read, write

Examples

This example shows how to enable interface based static session in BNG:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface bundle-ether 1.1
RP/0/RSP0/CPU0:router(config-subif)# ipsubscriber interface
```

Related Commands

Command	Description
show subscriber manager sadb, on page 493	Displays the subscriber management feature attribute database information.
show ipsubscriber access-interface, on page 268	Shows the access interface information for IP subscriber.

Command	Description
show ipsubscriber interface, on page 271	Shows the interface information for IP subscriber interfaces.

ipsubscriber l2-connected

To enable l2-connected IP subscriber for IPv4 or IPv6, use the **ipsubscriber l2-connected** command in the interface configuration mode. To disable this feature, use the **no** form of this command.

ipsubscriber {**ipv4**| **ipv6**} **l2-connected initiator**{**dhcp**| **unclassified-source**}

no ipsubscriber {**ipv4**| **ipv6**} **l2-connected initiator**{**dhcp**| **unclassified-source**}

Syntax Description

ipv4	Specifies IPv4 address prefixes.
ipv6	Specifies IPv6 address prefixes.
initiator	Configures the IP subscriber initiator.
dhcp	Configures DHCP as first-sign-of-life protocol for IPv4 subscriber.
unclassified-source	Configures unclassified packets as first-sign-of-life for IPv4 subscriber.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.
Release 4.3.0	Supported was added for IPv6 prefixes.

Usage Guidelines

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

Task ID

Task ID	Operation
network	read, write

Examples

This is an example of configuring the **ipsubscriber l2-connected** command in the interface configuration mode for IPv4:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether 56
RP/0/RSP0/CPU0:router(config-if)# ipsubscriber ipv4 l2-connected initiator dhcp
```

This is an example of configuring the **ipsubscriber l2-connected** command in the interface configuration mode for IPv6:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether 56
RP/0/RSP0/CPU0:router(config-if)# ipsubscriber ipv6 l2-connected initiator dhcp
```

Related Commands

Command	Description
show ipsubscriber summary, on page 275	Displays the ipsubscriber information.

ipsubscriber routed

To host IPv4 routed subscriber sessions in an access-interface, use the **ipsubscriber routed** command in the interface configuration mode. To disable this feature, use the **no** form of this command.

ipsubscriber ipv4 routed [**initiator dhcp**]

no ipsubscriber ipv4 routed [**initiator dhcp**]

Syntax Description

ipv4	Specifies IPv4 subscriber.
initiator	Specifies session initiator for routed subscriber.
dhcp	Configures DHCP as the session initiator for routed subscriber.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.1.1	This command was introduced.

Usage Guidelines

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

The routed subscriber sessions come up only if a summary route is added on BNG router. The DHCP pool IP address range in BNG must be in compliance with the summary route address range. This DHCP pool IP address range must also match the IP address subnet of the first hop router, which acts as the DHCP relay or proxy. Also, the summary route VRF must be same as the access-interface VRF in BNG router.

Task ID

Task ID	Operation
network	read, write

Examples

This example shows how to host **ipsubscriber routed** IPv4 sessions in an access-interface:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether101.201
RP/0/RSP0/CPU0:router(config-if)# ipsubscriber ipv4 routed initiator dhcp
```

Related Commands

Command	Description
ipsubscriber interface, on page 260	Enables interface based static session in BNG.
show ipsubscriber access-interface, on page 268	Shows the access interface information for IP subscriber.
show subscriber session, on page 500	Displays the subscriber management session information.

ipsubscriber session-limit

To limit the number of IP subscriber sessions on a subscriber interface, use the **ipsubscriber session-limit** command in the interface configuration mode. To disable this feature, use the **no** form of this command.

ipsubscriber session-limit{**total**| **unclassified-source**}**per-vlan** *session_limit*

no ipsubscriber session-limit

Syntax Description

total	Limits IP subscribers for all sources.
unclassified-source	Limits IP subscribers for unclassified sources.
per-vlan	Limits the per VLAN subscribers.
session-limit	Specifies the maximum number to which of the IP subscriber session can be limited.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
network	read, write

Examples

This is an example of configuring the **ipsubscriber session-limit** command in the interface configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether 56
```

```
RP/0/RSP0/CPU0:router(config-if)# ipsubscriber session-limit
RP/0/RSP0/CPU0:router(config-ipsub-sess-limit)# total per-vlan 25
RP/0/RSP0/CPU0:router(config-ipsub-sess-limit)# unclassified-source per-vlan 452
```

show ipsubscriber access-interface

To display the access interface information for IP subscriber, use the **show ipsubscriber access-interface** command in the EXEC mode.

show ipsubscriber access-interface {*type*| *interface-path-id*| **brief**| **location**| *location*}

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.
brief	Displays the brief summary of IP Subscriber access interface status and configuration.
location	Specifies the IP subscriber location.
location	Specifies the fully qualified location specification.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

For interface-based static sessions in the BNG, the value of *Interface Type* field in the **show ipsubscriber access-interface** command output is displayed as **static**.

Task ID

Task ID	Operation
network	read

Examples

This is the sample output of the **show ipsubscriber access-interface** command:

```
RP/0/RSP0/CPU0:router# show ipsubscriber access-interface

Interface: GigabitEthernet0/0/0/0 (ifhandle 0x20000040)
  State: UP
  Type: Plain
  Created Jan 18 00:01:32 (age 00:58:28)
  Initiator DHCP enabled
    Session count 0
    FSOL packets 0, bytes 0
    FSOL dropped packets 0, bytes 0
  Initiator Packet-Trigger enabled
    Session count 0
    FSOL packets 0, bytes 0
    FSOL dropped packets 0, bytes 0
  Initiator DHCPv6 disabled
    Session count 0
    FSOL packets 0, bytes 0
    FSOL dropped packets 0, bytes 0
  Initiator Packet-Trigger-IPv6 enabled
    Session count 0
    FSOL packets 0, bytes 0
    FSOL dropped packets 0, bytes 0

RP/0/RSP0/CPU0:router# show ipsubscriber access-interface brief

Codes: UP - Up, DOWN - Down, DELETED - Deleted State, UNKNOWN - Unknown State,
       PKT - Packet Trigger Initiation, DHCP - DHCP Initiation
       PKTv6 - Packet Trigger Initiation for IPv6, DHCPv6 - DHCPv6 Initiation

Interface              Proto                DHCP        Pkt Trigger DHCPv6      PktTrigIPv6
 State
---------------------- -------------------- ----------- ----------- ----------- -----------
 ---------
Gi0/0/0/0               DHCP,PKT,DHCPv6,PKTv6           0           2           0
 0        UP
BE1.1                   DHCP,PKT                        0           0           0
 0        UP
```

This is the sample output of the **show ipsubscriber access-interface** command for interface-based static sessions:

```
RP/0/RSP0/CPU0:router# show ipsubscriber access-interface
Interface: Bundle-Ether1.10
  State: UP
  Type: Plain
  Interface Type: Static
  Created Apr  8 09:56:57 (age 00:08:08)
  Initiator DHCP disabled
    Session count 0
    FSOL packets 0
    FSOL dropped packets 0
    FSOL flow rate dropped packets 0
    FSOL session limit dropped packets 0
  Initiator Packet-Trigger enabled
```

```
Session count 1
```

This table describes the significant fields shown in the display.

Table 16: show ipsubscriber access-interface Field Descriptions

Field	Description
Interface	Specifies the access interface type.
Proto	Specifies the prototype, for instance, DHCP, DHCPv6, PKTv6.
DHCP	Specifies the DHCP initiation.
Pkt Trigger	Specifies the packet trigger Initiation.
DHCPv6	Specifies the packet trigger Initiation for IPv6.
PktTrigIPv6	Specifies the DHCPv6 initiation.
State	Specifies the various states of the access interface, for example, up, down, deleted, and unknown state.

Related Commands

Command	Description
ipsubscriber l2-connected, on page 262	Displays the subscriber management session information.

show ipsubscriber interface

To display the interface information for the IP subscriber interfaces, use the **show ipsubscriber interface** command in the EXEC mode.

show ipsubscriber interface {*type interface-path-id*| **access-interface**| **address-family**| **brief**| **dynamic-routes** [**location** *node-id*]| **location** *node-id*| **outer-vlan-id** *id* [**inner-vlan-id** *id*]| **subscriber-ip**| **subscriber-label** | **subscriber-mac**| **vrf**}

Syntax Description

type	Interface type. For more information on interface types available for this command, 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.
access-interface	Specifies the access or parent interface.
address-family	Specifies the address-family in which the IP subscriber interface operates.
brief	Displays the brief summary of IP Subscriber access interface status and configuration.
dynamic-routes	Specifies the dynamic routes.
location	Specifies the IP subscriber location.
node-id	Specifies the fully qualified location specification.
outer-vlan-id	Specifies the subscriber outer VLAN ID.
id	Outer VLAN ID. The range is from 1 to 4094.
inner-vlan-id	Specifies the subscriber inner VLAN ID.
id	Inner VLAN ID. The range is from 1 to 4094.
subscriber-ip	Specifies the subscriber IPv4 address.
subscriber-label	Specifies the subscriber label.
subscriber-mac	Specifies the subscriber MAC address.

vrf	Specifies the VRF in which the IP subscriber interface operates.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	This command was introduced.
Release 4.3.1	The **outer-vlan-id** keyword along with an optional **inner-vlan-id** keyword was added.
Release 5.1	The **dynamic-routes** keyword was added.

Usage Guidelines

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

For interface-based static sessions in the BNG, the value of *Type* field in the **show ipsubscriber interface** command output is displayed as **Static**.

Task ID

Task ID	Operation
network	read

Examples

This is the sample output of the **show ipsubscriber interface** command:

```
RP/0/RSP0/CPU0:router# show ipsubscriber interface

Interface: GigabitEthernet0/1/0/0.11.ip1
      Type: L2-connected
      Ifhandle: 0x201000c0
      Access Interface: GigabitEthernet0/1/0/0.11 (0x20100080)
      Subscriber MAC: 0100.0000.0000
      Subscriber IP: 11.10.10.9         <------- this line will not be shown if empty
      Subscriber IPv6 Prefix: FE80::10  <------- this line will not be shown if empty
      Subscriber Label: 0x8000000
      IPv4: Initiator: Packet-Trigger   <-- this line will not be shown if not enabled
      IPv6: Initiator: DHCPv6           <-- this line will not be shown if not enabled
      Created: May 11 16:33:08 (age 00:03:08)
      VRF: vpn1 (0x60000002), IPv4 Table: default (0xe0000002), IPv6 Table: default
(0xe0000002)
      IPv4: State: Up(9) (old: Adjacency added(8))
            Last state change: May 11 16:33:08 (00:03:08 in current state)
```

```
      IPv6: State: Up(9) (old: Adjacency added(8))
            Last state change: May 11 16:33:08 (00:03:08 in current state)

RP/0/RSP0/CPU0:router# show ipsubscriber interface brief

Codes: INV - Invalid, INIT - Initialized, STRTD - Session Creation Started,
       CPEXCTG - Control-Policy Executing, CPEXCTD - Control-Policy Executed,
       FTAPPLD - Session Features Applied, VRFCFGD - VRF Configured,
       ADJADDG - Adding Adjacency, ADJADDD - Adjacency Added, UP - Up,
       DOWN - Down, DISCG - Disconnecting, DISCD - Disconnected, ERR - Error,
       UNKWN - Unknown State, PKT - Packet Trigger Initiation,
       PKTv6 - Packet Trigger Initiation for IPv6,
       DHCP - DHCP Initiation, DHCPv6 - DHCPv6 Initiation

Interface              Proto Subscriber IP      MAC Address        Sublabel   VRF
State
---------------------- ------ ----------------- ------------------ ---------- ----------
----------
Gi0/0/0/0.ip1          DHCP   1.10.10.9          0100.0000.0000     0x40       default
UP
                       DHCPv6                    0100.0000.0000     0x40       default
UP
Gi0/0/0/0.ip2          PKT    2.20.20.9          0200.0000.0000     0x20       default
UP
                       PKTv6                     0200.0000.0000     0x20       default
UP
Gi0/0/0/0.ip3          DHCPv6 5.40.20.9          0200.2200.0000     0x21       default
UP
Gi0/0/0/0.ip4          PKTv6  7.91.20.9          0200.2210.0000     0x31       default
UP
```

This is the sample output of the **show ipsubscriber interface outer-vlan-id** command:

```
RP/0/RSP0/CPU0:router# show ipsubscriber interface outer-vlan-id 200 inner-vlan-id 100

Interface: Bundle-Ether1.200.ip1
  Type: L2-connected
  Access Interface: Bundle-Ether1.200
  Subscriber MAC: 0000.0000.0014
  Subscriber IPv4: 1.10.9.246
  Subscriber Label: 0x4f
  IPv4 Initiator: Packet-Trigger
  VLAN ID: outer 200 inner 100
  Created: Dec 22 00:32:28 (age 00:00:43)
  VRF: default, IPv4 Table: default
  IPv4 State: Up (old: Adjacency added)
       Last state change: Apr 9 00:32:28 (00:00:43 in current state)
```

This is the sample output of the **show ipsubscriber interface dynamic-routes** command:

```
RP/0/RSP0/CPU0:router# show ipsubscriber interface dynamic-routes
Interface              Dynamic-Routes
---------------------- ------------------------------------------------------------
BE1.1.ip3              45.1.32.0/24 (vrf vpn1) nhop 12.1.0.32 (vrf vpn1) distance 3 tag 34
 (added)
BE1.1.ip4              45.1.33.0/24 (vrf vpn1) nhop 12.1.0.33 (vrf vpn1) distance 14 tag
340 (added)
```

This table describes the significant fields shown in the display.

Table 17: show ipsubscriber interface Field Descriptions

Field	Description
Interface	Specifies the access interface type.
Proto	Specifies the prototype, for instance, DHCP, DHCPv6, PKTv6.

Field	Description
Subscriber IP	Specifies the IP address of the subscriber interface.
MAC Address	Specifies the MAC address for each interface type.
Sublabel	Specifies the sub label type for each interface.
VRF	Specifies the default VRF type.
State	Specifies the various states of the access interface, for example, up, down, deleted, and unknown state.

Related Commands

Command	Description
ipsubscriber l2-connected, on page 262	Displays the subscriber management session information.

show ipsubscriber summary

To display the summary information for the IP subscriber interfaces, use the **show ipsubscriber summary** command in the EXEC mode.

show ipsubscriber summary location *location*

Syntax Description

location	Specifies the IP subscriber location.
location	Specifies the fully qualified location specification.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
network	read

Examples

This is the sample output of the **show ipsubscriber summary** command:

```
RP/0/RSP0/CPU0:router# show ipsubscriber summary
IPSUB Summary for all nodes

Interface Counts:
                                    DHCP  Pkt Trigger
                                ---------- ------------
                     Invalid:          0            0
                 Initialized:          0            0
    Session creation started:          0            0
    Control-policy executing:          0            0
     Control-policy executed:          0            0
    Session features applied:          0            0
              VRF configured:          0            0
```

```
            Adding adjacency:          0             0
             Adjacency added:          0             0
                          Up:          0             0
                        Down:          0             0
               Disconnecting:          0             0
                Disconnected:          0             0
               Unknown state:          0             0
                       Error:          0             0
                             ---------- ------------
                       Total:          0             0

                                  DHCPv6 PktTrig-IPv6
                             ---------- ------------
                     Invalid:          0             0
                 Initialized:          0             0
    Session creation started:          0             0
    Control-policy executing:          0             0
     Control-policy executed:          0             0
    Session features applied:          0             0
              VRF configured:          0             0
            Adding adjacency:          0             0
             Adjacency added:          0             0
                          Up:          0             0
                        Down:          0             0
               Disconnecting:          0             0
                Disconnected:          0             0
               Unknown state:          0             0
                       Error:          0             0
                             ---------- ------------
                       Total:          0             0

Routes Per VRF (0 VRFs):
                                   Count
                             ----------

Access Interface Counts (1 interfaces):

                                    DHCP  Pkt Trigger
                             ---------- ------------
                 FSOL Packets:          0             0
                   FSOL Bytes:          0             0

                                  DHCPv6 PktTrig-IPv6
                             ---------- ------------
                 FSOL Packets:          0             0
                   FSOL Bytes:          0             0
```

This table describes the significant fields shown in the display.

Table 18: show ipsubscriber summary Field Descriptions

Field	Description
Invalid	Specifies the number of invalid packets for DHCP and Packet Trigger.
Initialized	Specifies the number of packets that were initialized for DHCP and Packet Trigger.
Session creation started	Specifies the total number of session initiation that was created.
Control-policy executing	Specifies the control policies that are executing for DHCP and Packet Trigger.

Field	Description
Control-policy executed	Specifies the control policies that were executed for DHCP and Packet Trigger.
Session features applied	Specifies the number of session features that were applied for DHCP and Packet Trigger.
VRF configured	Specifies the VRFs configured.
Up	Specifies the number of packets that are in the UP state.
Down	Specifies the number of packets that are in the DOWN state.
Disconnecting	Specifies the number of packets that are disconnecting.
Disconnected	Specifies the number of packets that are disconnected.
Unknown State	Specifies the packets that are in the unknown state.
Error	Specifies the number of packets that are errored out.

Related Commands

Command	Description
ipsubscriber l2-connected, on page 262	Displays the subscriber management session information.

IPv4 and IPv6 Commands

This module describes the Cisco IOS XR software commands used to configure the IPv4 and IPv6 commands for Broadband Network Gateway (BNG) on the Cisco ASR 9000 Series Router. For details regarding the related configurations, refer to the *Cisco ASR 9000 Series Aggregation Services Router Broadband Network Gateway Configuration Guide*.

- ipv4 mtu (BNG), page 280
- ipv4 unnumbered (point-to-point -BNG), page 282
- ipv4 unreachables disable (BNG), page 284
- ipv4 verify unicast source reachable-via (BNG), page 286
- ipv6 enable (BNG), page 288
- ipv6 mtu (BNG), page 290
- ipv6 unreachables disable (BNG), page 292
- show ipv4 interface (BNG), page 294
- show ipv4 traffic (BNG), page 298
- show ipv6 interface (BNG), page 301
- show ipv6 neighbors (BNG), page 305
- show ipv6 neighbors summary (BNG), page 311
- show ipv6 traffic (BNG), page 313

ipv4 mtu (BNG)

To set the maximum transmission unit (MTU) size of IPv4 packets sent on an interface, use the **ipv4 mtu** command in an appropriate 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

Dynamic template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.2.0	This command was supported in the dynamic template configuration mode for BNG.

Usage Guidelines

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

The router will fragment any IPv4 packet that exceeds the MTU set for the interface.

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.

To enter the dynamic template configuration mode, run **dynamic-template** command in the global configuration mode.

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 to 300 bytes in dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv4 mtu 300
```

Related Commands

Command	Description
show ipv4 interface (BNG), on page 294	Displays the MTU status of interfaces configured for IPv4.

ipv4 unnumbered (point-to-point -BNG)

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 appropriate 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

Dynamic template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.2.0	This command was supported in the dynamic template configuration mode for BNG.

Usage Guidelines

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

To enter the dynamic template configuration mode, run **dynamic-template** command in the global configuration 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

In this example the Bundle-Ether interface is assigned address 100.10 in the dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv4 unnumbered Bundle-Ether100.10
```

ipv4 unreachables disable (BNG)

To disable the generation of IPv4 Internet Control Message Protocol (ICMP) unreachable messages, use the **ipv4 unreachables disable** command in an appropriate configuration mode. To re-enable the generation of ICMP unreachable messages, use the **no** form of this command.

ipv4 unreachables disable

no ipv4 unreachables disable

Syntax Description

This command has no keywords or arguments.

Command Default

IPv4 ICMP unreachables messages are generated.

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.2.0	This command was supported in the dynamic template configuration mode for BNG.

Usage Guidelines

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

If the software receives a nonbroadcast packet destined for itself that uses a protocol it does not recognize, it sends an ICMP protocol unreachable message to the source.

If the software receives a datagram that it cannot deliver to its ultimate destination because it knows of no route to the destination address, it replies to the originator of that datagram with an ICMP host unreachable message.

This command affects a number of ICMP unreachable messages.

To enter the dynamic template configuration mode, run **dynamic-template** command in the global configuration mode.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write

Task ID	Operations
config-services	read, write

Examples

This example shows how to disable the generation of ICMP unreachable messages on dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp foo
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv4 unreachables disable
```

ipv4 verify unicast source reachable-via (BNG)

To enable IPv4 unicast Reverse Path Forwarding (RPF) checking, use the **ipv4 verify unicast source reachable-via** command in an appropriate configuration mode. To disable unicast RPF, use the **no** form of this command.

ipv4 verify unicast source reachable-via {**any**| **rx**} **[allow-default] [allow-self-ping]**

no ipv4 verify unicast source reachable-via {**any**| **rx**} **[allow-default] [allow-self-ping]**

Syntax Description

any	Enables loose unicast RPF checking. If loose unicast RPF is enabled, a packet is not forwarded unless its source prefix exists in the routing table.
rx	Enables strict unicast RPF checking. If strict unicast RPF is enabled, a packet is not forwarded unless its source prefix exists in the routing table and the output interface matches the interface on which the packet was received.
allow-default	(Optional) Enables the matching of default routes. This option applies to both loose and strict RPF.
allow-self-ping	(Optional) Enables the router to ping out an interface.This option applies to both loose and strict RPF.

Command Default

IPv4 unicast RPF is disabled.

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.2.0	This command was supported in the dynamic template configuration mode for BNG.

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 enter the dynamic template configuration mode, run **dynamic-template** command in the global configuration mode.

Use the **ipv4 verify unicast source reachable-via** interface command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through a router. Malformed or forged source addresses can indicate denial-of-service (DoS) attacks based on source IP address spoofing.

When strict unicast RPF is enabled on an interface, the router examines all packets received on that interface. The router checks to make sure that the source address appears in the routing table and matches the interface on which the packet was received.

When loose unicast RPF is enabled on an interface, the router examines all packets received on that interface. The router checks to make sure that the source address can be reached through any of the router interfaces.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write
config-services	read, write

Examples

This example shows how to configure strict RPF on dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv4 verify unicast source reachable-via
 rx
```

ipv6 enable (BNG)

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

This command has no keywords or arguments.

Command Default

IPv6 is disabled.

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.3.0	This command was supported in the dynamic template configuration mode for BNG.

Usage Guidelines

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

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.

To enter the dynamic template configuration mode, run **dynamic-template** command in the global configuration mode.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

This example show how to enable IPv6 processing on dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp foo
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv6 enable
```

Related Commands

Command	Description
show ipv6 interface (BNG), on page 301	Displays the usability status of interfaces configured for IPv6.

ipv6 mtu (BNG)

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

Dynamic template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.3.0	This command was supported in the dynamic template configuration mode for BNG.

Usage Guidelines

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

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.

To enter the dynamic template configuration mode, run **dynamic-template** command in the global configuration 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
network	read, write
config-services	read, write

Examples

This example shows how to set the maximum IPv6 packet size to 1350 bytes in the dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp foo
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv6 mtu 1350
```

Related Commands

Command	Description
show ipv6 interface (BNG), on page 301	Displays the usability status of interfaces configured for IPv6.

ipv6 unreachables disable (BNG)

To disable the generation of IPv6 Internet Control Message Protocol (ICMP) unreachable messages, use the **ipv6 unreachables disable** command in an appropriate configuration mode. To re-enable the generation of ICMP unreachable messages, use the **no** form of this command.

ipv6 unreachables disable

no ipv6 unreachables disable

Syntax Description

This command has no keywords or arguments.

Command Default

IPv6 ICMP unreachables messages are generated.

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.3.0	This command was supported in the dynamic template configuration mode for BNG.

Usage Guidelines

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

If the software receives a nonbroadcast packet destined for itself that uses a protocol it does not recognize, it sends an ICMP protocol unreachable message to the source.

If the software receives a datagram that it cannot deliver to its ultimate destination because it knows of no route to the destination address, it replies to the originator of that datagram with an ICMP host unreachable message.

This command affects a number of ICMP unreachable messages.

To enter the dynamic template configuration mode, run **dynamic-template** command in the global configuration mode.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Task ID	Operations
config-services	read, write

Examples

This example shows how to disable the generation of ICMP unreachable messages on dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp foo
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv6 unreachables disable
```

show ipv4 interface (BNG)

To display the usability status of interfaces configured for IPv4, use the **show ipv4 interface** command in the EXEC mode.

show ipv4 [**vrf** *vrf-name*] **interface** [*type interface-path-id*| **brief**| **summary**]

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
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

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.2.0	This command was supported for BNG.

Usage Guidelines

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

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/RSP0/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
gigabitethernet0
/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
```

```
gigabitethernet0
/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 19: 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.
Secondary address	Displays a secondary address, if one has been set.
MTU	Displays the IPv4 MTU[1] 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[2] is enabled or disabled on an interface.
ICMP redirects	Specifies whether ICMPv4[3] 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.

1 MTU = maximum transmission unit

2 ARP = Address Resolution Protocoladdress resolution protocol
3 ICMPv4 = Internet Control Message Protocol internet control message protocol version 4

Related Commands

Command	Description
show ipv6 interface (BNG), on page 301	Displays the usability status of interfaces configured for IPv6.

show ipv4 traffic (BNG)

To display the IPv4 traffic statistics, use the **show ipv4 traffic** command in the 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

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced .
Release 4.2.0	This command was supported for BNG.

Usage Guidelines

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

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/RSP0/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 20: show ipv4 traffic Command Field Descriptions

Field	Description
bad hop count	Occurs when a packet is discarded because its TTL[4] 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.

4 TTL = time-to-live

Related Commands

Command	Description
show ipv6 traffic (BNG), on page 313	Displays statistics about IPv6 traffic.

show ipv6 interface (BNG)

To display the usability status of interfaces configured for IPv6, use the **show ipv6 interface** command in the EXEC mode.

show ipv6 [**vrf** *vrf-name*] **interface** [*type interface-path-id*| **brief**| **summary**]

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
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.
summary	(Optional) Displays the number of interfaces on the router that are assigned, unassigned, or unnumbered.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.3.0	This command was supported for BNG.

Usage Guidelines

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

The **show ipv6 interface** command provides output similar to the **show ipv4 interface** command, except that it is IPv6-specific.

Task ID

Task ID	Operations
ipv6	read

Examples

This is the sample output of the **show ipv6 interface** command:

```
RP/0/RSP0/CPU0:router# show ipv6 interface

GigabitEthernet0/2/0/0 is Up, line protocol is Up, Vrfid is default (0x60000000)
  IPv6 is enabled, link-local address is fe80::212:daff:fe62:c150
  Global unicast address(es):
    202::1, subnet is 202::/64
  Joined group address(es): ff02::1:ff00:1 ff02::1:ff62:c150 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 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.
  Outgoing access list is not set
  Inbound  access list is not set
```

This table describes the significant fields shown in the display.

Table 21: show ipv6 interface Command Field Descriptions

Field	Description
GigabitEthernet0 /3/0/0 is Shutdown, line protocol is Down	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.
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).

Field	Description
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.

Related Commands

Command	Description
show ipv4 interface (BNG), on page 294	Displays the usability status of interfaces configured for IPv4.

show ipv6 neighbors (BNG)

To display the IPv6 neighbor discovery cache information, use the **show ipv6 neighbors** command in the 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 Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.3.0	This command was supported for BNG.

Usage Guidelines

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

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 interface type and number:

```
RP/0/RSP0/CPU0:router# show ipv6 neighbors
gigabitethernet

0/0/0/0

IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH gigabitethernet2

FE80::203:A0FF:FED6:141E                    0 0003.a0d6.141e  REACH gigabitethernet2

3001:1::45a                                 - 0002.7d1a.9472  REACH gigabitethernet2
```

This is the sample output of the **show ipv6 neighbors** command when entered with an IPv6 address:

```
RP/0/RSP0/CPU0:router# show ipv6 neighbors 2000:0:0:4::2

IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH gigabitethernet2
```

This is the sample output of the **show ipv6 neighbors** command:

```
RP/0/RSP0/CPU0:router# show ipv6 neighbors

IPv6 Address     Age Link-layer Addr State Interface    Location
2001:1::3        130  0011.9400.0003 REACH BE1          0/0/CPU0
2001:1::4        335  0011.9400.0004 REACH BE1          0/0/CPU0
2001:1::5        314  0011.9400.0005 REACH BE1          0/0/CPU0
2001:1::6        291  0011.9400.0006 REACH BE1          0/0/CPU0
2001:1::7        235  0011.9400.0007 REACH BE1          0/0/CPU0
2001:1::8        340  0011.9400.0008 REACH BE1          0/0/CPU0
2001:1::9        230  0011.9400.0009 REACH BE1          0/0/CPU0
2001:1::a        99   0011.9400.000a REACH BE1          0/0/CPU0
2001:1::b        291  0011.9400.000b REACH BE1          0/0/CPU0
2001:1::c        226  0011.9400.000c REACH BE1          0/0/CPU0
2001:1::d        272  0011.9400.000d REACH BE1          0/0/CPU0
2001:1::e        14   0011.9400.000e REACH BE1          0/0/CPU0
2001:1::f        299  0011.9400.000f REACH BE1          0/0/CPU0
2001:1::10       131  0011.9400.0010 REACH BE1          0/0/CPU0
2001:1::11       70   0011.9400.0011 REACH BE1          0/0/CPU0
2001:1::12       131  0011.9400.0012 REACH BE1          0/0/CPU0
2001:1::13       137  0011.9400.0013 REACH BE1          0/0/CPU0
2001:1::14       290  0011.9400.0014 REACH BE1          0/0/CPU0
2001:1::15       19   0011.9400.0015 REACH BE1          0/0/CPU0
2001:1::16       158  0011.9400.0016 REACH BE1          0/0/CPU0
2001:1::17       35   0011.9400.0017 REACH BE1          0/0/CPU0
2001:1::18       222  0011.9400.0018 REACH BE1          0/0/CPU0
```

This is the sample output of the **show ipv6 neighbors** command when entered with a location:

```
RP/0/RSP0/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 22: 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	

Field	Description
	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;

Field	Description
	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.

Related Commands

Command	Description
show ipv6 neighbors summary (BNG), on page 311	Displays summary information for the neighbor entries.

show ipv6 neighbors summary (BNG)

To display summary information for the neighbor entries, use the **show ipv6 neighbors summary** command in the EXEC mode.

show ipv6 neighbors summary

Syntax Description

This command has no keywords or arguments.

Command Default

The default value is disabled.

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.3.0	This command was supported for BNG.

Usage Guidelines

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

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:

```
RP/0/RSP0/CPU0:router# show ipv6 neighbors summary

Mcast nbr entries:
    Subtotal: 0
Static nbr entries:
    Subtotal: 0
Dynamic nbr entries:
    Subtotal: 0

Total nbr entries: 0
```

Related Commands

Command	Description
show ipv6 neighbors (BNG), on page 305	Displays IPv6 neighbor discovery cache information.

show ipv6 traffic (BNG)

To display the IPv6 traffic statistics, use the **show traffic** command in the 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

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.3.0	This command was supported for BNG.

Usage Guidelines

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

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/RSP0/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 23: 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.

Field	Description
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.
ICMP statistics:	Internet Control Message Protocol statistics.

Related Commands

Command	Description
show ipv4 traffic (BNG), on page 298	Displays statistics about IPv4 traffic.

Multicast Commands

This module describes the Cisco IOS XR software commands used to configure the Multicast commands for Broadband Network Gateway (BNG) on the Cisco ASR 9000 Series Router. For details regarding the related configurations, refer to the *Cisco ASR 9000 Series Aggregation Services Router Broadband Network Gateway Configuration Guide*.

- router igmp vrf, page 318
- igmp accounting, page 319
- igmp explicit-tracking, page 320
- igmp query-interval, page 322
- igmp query-max-response-time, page 324
- multicast (BNG), page 326
- unicast-qos-adjust, page 328
- show igmp unicast-qos-adjust statistics, page 330
- show igmp vrf (BNG), page 333
- clear igmp unicast-qos-adjust, page 335

router igmp vrf

To configure route-policy to be used to map the bandwidth profile, use the **router igmp vrf** command in the global configuration mode. To disable this feature, use the **no** form of this command.

router igmp vrf *vrf_name* {**traffic| profile**| *profile_name*}

no router igmp vrf *vrf_name* {**traffic| profile**| *profile_name*}

Syntax Description

vrf_name	Specifies the VRF name.
traffic	Configures IGMP traffic variables.
profile	Configures route-policy to be used to map the bandwidth profile.
profile_name	Specifies the profile name.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
multicast	read, write

Examples

This is an example of configuring the **router igmp vrf** command in the global configuration mode:

```
RP/0/RSP0/CPU0:router # configure
RP/0/RSP0/CPU0:router(config)# router igmp vrf vrf1
RP/0/RSP0/CPU0:router(config)# router igmp vrf vrf1 traffic profile prof-name
```

igmp accounting

To enable accounting feature under igmp, use the **igmp accounting** command in the global configuration mode. To disable this feature, use the **no** form of this command.

igmp accounting{ **max-history**| *number_of_days*}

no igmp accounting{ **max-history**| *number_of_days*}

Syntax Description

max-history	Sets the maximum history for the accounting in days.
number_of_days	Specifies the number of days the history has to be retained. This value ranged from 1 to 365.

Command Default

If max-history is not specified, then the default is 0 days, which indicates that there was no history saved.

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
multicast	read, write

Examples

This is an example of configuring the **igmp accounting** command in the global configuration mode:

```
RP/0/RSP0/CPU0:router # configure
RP/0/RSP0/CPU0:router(config)# router igmp accounting max-history 67
```

igmp explicit-tracking

To configure explicit host tracking under Internet Group Management Protocol (IGMP) Version 3, use the **igmp explicit-tracking** command in the dynamic-template configuration mode. To disable explicit host tracking, use the **no** form of this command.

igmp explicit-tracking *access_list_name*

no igmp explicit-tracking

Syntax Description

access_list_name	Specifies the access list tracking group range.

Command Default

None

Command Modes

Dynamic template configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Use the **dynamic-template type ppp** command to enter dynamic template type ppp configuration mode.

Task ID

Task ID	Operation
multicast	read, write

Examples

This is an example of configuring the **igmp explicit-tracking** command in the dynamic-template configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template
RP/0/RSP0/CPU0:router(config-dynamic-template)# type ppp foo
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# igmp explicit-tracking igmp1
```

Related Commands

Command	Description
igmp query-interval, on page 322	Configures the frequency at which the Cisco IOS XR Software sends Internet Group Management Protocol (IGMP) host-query messages.
unicast-qos-adjust, on page 328	Configures the IGMP QOS Shaper for subscriber unicast traffic.
show igmp unicast-qos-adjust statistics, on page 330	Displays the internal statistics of the unicast-qos-adjusted feature.
igmp query-max-response-time, on page 324	Configures the maximum response time advertised in Internet Group Management Protocol (IGMP) queries
multicast (BNG), on page 326	Configures the mode in which the multicast components will work for subscriber sessions associated with a dynamic template.

igmp query-interval

To configure the frequency at which the Cisco IOS XR Software sends Internet Group Management Protocol (IGMP) host-query messages, use the **igmp query-interval** command in the dynamic-template configuration mode. To disable this feature, use the **no** form of this command.

igmp query-interval *seconds*

no igmp query-interval

Syntax Description

seconds	Specifies the frequency used to send IGMP host-query messages and ranges between 1 to 3600.

Command Default

The default query-interval value is 60s.

Command Modes

Dynamic template configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Use the **dynamic-template type ppp** command to enter dynamic template type ppp configuration mode.

Task ID

Task ID	Operation
multicast	read, write

Examples

This is the example of configuring the **igmp query-interval** command in the dynamic-template configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template
RP/0/RSP0/CPU0:router(config-dynamic-template)# type ppp foo
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# igmp query-interval 60
```

Related Commands

Command	Description
unicast-qos-adjust, on page 328	Configures the IGMP QOS Shaper for subscriber unicast traffic.
igmp explicit-tracking, on page 320	Configures explicit host tracking under Internet Group Management Protocol (IGMP) Version 3
igmp query-max-response-time, on page 324	Configures the maximum response time advertised in Internet Group Management Protocol (IGMP) queries
multicast (BNG), on page 326	Configures the mode in which the multicast components will work for subscriber sessions associated with a dynamic template.
show igmp unicast-qos-adjust statistics, on page 330	Displays the internal statistics of the unicast-qos-adjusted feature.

igmp query-max-response-time

To configure the maximum response time advertised in Internet Group Management Protocol (IGMP) queries, use the **igmp query-max-response-time** command in the dynamic-template configuration mode. To disable this feature, use the **no** form of this command.

igmp query-max-response-time *seconds*

no igmp query-max-response-time

Syntax Description

seconds	Specifies the maximum response time, in seconds, advertised in IGMP queries, and ranges between 1 to 12.

Command Default

The default query-max-response-time is 10 seconds.

Command Modes

Dynamic template configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Use the **dynamic-template type ppp** command to enter dynamic template type ppp configuration mode.

Task ID

Task ID	Operation
multicast	read, write

Examples

This is the example of configuring the **igmp query-max-response-time** command in the dynamic-template configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template
RP/0/RSP0/CPU0:router(config-dynamic-template)# type ppp foo
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# igmp query-max-response-time 12
```

Related Commands

Command	Description
igmp query-interval, on page 322	Configures the frequency at which the Cisco IOS XR Software sends Internet Group Management Protocol (IGMP) host-query messages.
igmp explicit-tracking, on page 320	Configures explicit host tracking under Internet Group Management Protocol (IGMP) Version 3
show igmp unicast-qos-adjust statistics, on page 330	Displays the internal statistics of the unicast-qos-adjusted feature.
unicast-qos-adjust, on page 328	Configures the IGMP QOS Shaper for subscriber unicast traffic.
multicast (BNG), on page 326	Configures the mode in which the multicast components will work for subscriber sessions associated with a dynamic template.

multicast (BNG)

To configure the mode in which the multicast components will work for subscriber sessions associated with a dynamic template, use the **multicast** command in the dynamic-template configuration mode. To disable this feature, use the **no** form of this command.

multicast[**ipv4**]{**qos-correlation**| **passive**}

no multicast[**ipv4**]{**qos-correlation**| **passive**}

qos-correlation	Configures multicast in a IGMP-HQOS correlation mode.
passive	Configures multicast is an passive mode.
ipv4	Optional. Specifies configuration for IPv4 address family.

Command Default

None

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Use the **dynamic-template type ppp** command to enter dynamic template type ppp configuration mode.

Task ID

Task ID	Operation
multicast	read, write

Examples

This is an example of configuring the **multicast** command in the dynamic-template configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template
```

```
RP/0/RSP0/CPU0:router(config-dynamic-template)# type ppp foo
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# multicast ipv4 qos-correlation
```

Related Commands

Command	Description
igmp query-interval, on page 322	Configures the frequency at which the Cisco IOS XR Software sends Internet Group Management Protocol (IGMP) host-query messages.
unicast-qos-adjust, on page 328	Configures the IGMP QOS Shaper for subscriber unicast traffic.
igmp explicit-tracking, on page 320	Configures explicit host tracking under Internet Group Management Protocol (IGMP) Version 3
igmp query-max-response-time, on page 324	Configures the maximum response time advertised in Internet Group Management Protocol (IGMP) queries
show igmp unicast-qos-adjust statistics, on page 330	Displays the internal statistics of the unicast-qos-adjusted feature.

unicast-qos-adjust

To configure the IGMP QOS Shaper for subscriber unicast traffic, use the **unicast-qos-adjust** command in the IGMP configuration mode. To disable this feature, use the **no** form of this command.

unicast-qos-adjust {**adjustment-delay**| **download-interval**| **holdoff**}

no unicast-qos-adjust

Syntax Description

adjustment-delay	Configures the time to wait before programming rate in QOS.
download-interval	Configures the time before downloading a batch of interfaces to QOS.
holdoff	Configures the hold-off time before QOS clears the stale entries.

Command Default

None

Command Modes

IGMP configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Use the **dynamic-template type ppp** command to enter dynamic template type ppp configuration mode.

Task ID

Task ID	Operation
multicast	read, write

Examples

This is an example of configuring the **unicast-qos-adjust** command in the IGMP configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router igmp
RP/0/RSP0/CPU0:router(config-igmp)# unicast-qos-adjust
```

Related Commands

Command	Description
igmp query-interval, on page 322	Configures the frequency at which the Cisco IOS XR Software sends Internet Group Management Protocol (IGMP) host-query messages.
igmp explicit-tracking, on page 320	Configures explicit host tracking under Internet Group Management Protocol (IGMP) Version 3.
show igmp unicast-qos-adjust statistics, on page 330	Displays the internal statistics of the unicast-qos-adjusted feature.
igmp query-max-response-time, on page 324	Configures the maximum response time advertised in Internet Group Management Protocol (IGMP) queries.
multicast (BNG), on page 326	Configures the mode in which the multicast components will work for subscriber sessions associated with a dynamic template.

show igmp unicast-qos-adjust statistics

To show the statistics of the unicast-qos-adjusted feature, use the **show igmp unicast-qos-adjust statistics** command in the EXEC mode.

show igmp unicast-qos-adjust statistics[**interface** *type interface-path-id*]

Syntax Description

interface	(Optional). Displays the interface specific information such as name of the interface, number of flows adjusted, total rate adjusted, and uptime after first adjustment, in a tabular format. If the interface is specified, then the interface specific statistics are displayed with table of 5 latest updates.
|	Specifies the output modifiers.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
multicast	read

Examples

This is the sample output of the **show igmp unicast-qos-adjust statistics** command:

```
RP/0/RSP0/CPU0:router# show igmp unicast-qos-adjust statistics
```

The show igmp unicast-qos-adjust statistics output is as follows:

```
Mon Feb  4 08:47:01.640 GMT

IGMP to QoS Batch stats
Current Queue count                          : 0
```

```
Last IGMP-to-QOS Batch count                  : 0
Last IGMP-to-QOS Batch errors                 : 0
Interfaces added to queue(all batches)        : 0
Interfaces removed from queue(all batches)    : 0

IGMP to QoS message send stats
Number of Send Success                        : 1
Number of Send Error COMMS                    : 0
Number of Send Error Partial                  : 0
Time elapsed since last download              : 3w0d

Resync stats
Is RESYNC required                            : No
Is RESYNC REQUEST received                    : No
Is RESYNC START message sent                  : No
Has Mark&Sweep happened anytime               : Yes
Time elapsed since last mark and sweep        : 3w0d
```

This table describes the significant fields shown in the display.

Table 24: show igmp unicast-qos-adjust statistics Field Descriptions

Field	Description
IGMP to QoS Batch stats	Specifies the batch statistics details for IGMP to QoS, such as current queue count, batch counter, batch errors, number of interfaces added to the queue, and the number of interfaces removed from the queue.
IGMP to QoS message send stats	Specifies the send statistics details for IGMP to QoS, such as number of send messages that was successful, number of send messages that had errored, number of send messages that had partially errored, and time elapsed since the last download.
Resync stats	Specifies the detailed information on the resynchronization statistics, such as whether resync is required, if the resync request was received, if the resync start message was sent, if mark and sweep for the resync has taken place, and time elapsed since the last mark and sweep.

Related Commands

Command	Description
igmp query-interval, on page 322	Configures the frequency at which the Cisco IOS XR Software sends Internet Group Management Protocol (IGMP) host-query messages.
unicast-qos-adjust, on page 328	Configures the IGMP QOS Shaper for subscriber unicast traffic.
igmp explicit-tracking, on page 320	Configures explicit host tracking under Internet Group Management Protocol (IGMP) Version 3

Command	Description
igmp query-max-response-time, on page 324	Configures the maximum response time advertised in Internet Group Management Protocol (IGMP) queries
multicast (BNG), on page 326	Configures the mode in which the multicast components will work for subscriber sessions associated with a dynamic template.

show igmp vrf (BNG)

To show the igmp vrf specific information, use the **show igmp vrf** command in the EXEC mode.

show igmp vrf *vrf_name*{**groups| interface| nsf| ranges| ssm| summary| traffic| unicast-qos-adjusted**}

Syntax Description

vrf	Shows the vrf information for igmp unicast qos shaper.
vrf_name	Specifies the vrf name.
groups	Shows the igmp group membership information.
interface	Shows igmp interface information.
nsf	Shows igmp nsf status.
ranges	Shows igmp group-map ranges.
ssm	Shows ssm related information.
summary	Shows igmp summary information.
traffic	Show igmp traffic counters.
unicast-qos-adjusted	Shows igmp unicast qos shaper.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
multicast	read

Examples

This is the sample output of the **show igmp vrf** command:

```
RP/0/RSP0/CPU0:router#show igmp vrf vrf1 summary
```

The show igmp vrf vrf1 summary output is as follows:

```
Thu Feb  7 10:02:24.457 GMT
Robustness Value 2
No. of Group x Interfaces 10
Maximum number of Group x Interfaces 50000

Supported Interfaces   : 2
Unsupported Interfaces : 0
Enabled Interfaces     : 2
Disabled Interfaces    : 0

MTE tuple count        : 0

Interface                      Number  Max #
                                         Groups  Groups
BVI1                                      7       10
Loopback1001                   3       25000

RP/0/RSP0/CPU0:router#show igmp vrf vrf1 interface bvi1

Thu Feb  7 10:02:48.231 GMT

BVI1 is up, line protocol is up
  Internet address is 172.16.251.1/30
  IGMP is enabled on interface
  Current IGMP version is 3
  IGMP query interval is 60 seconds
  IGMP querier timeout is 125 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 1 seconds
  IGMP activity: 26 joins, 19 leaves
  IGMP querying router is 172.16.251.1 (this system)
  Time elapsed since last query sent 00:00:41
  Time elapsed since IGMP router enabled 3w3d
  Time elapsed since last report received 00:00:32
```

This table describes the significant fields shown in the display.

Table 25: show igmp vrf Field Descriptions

Field	Description
Supported Interfaces	Specifies the number of supported interfaces.
Unsupported Interfaces	Specifies the number of unsupported interfaces.
Enabled Interfaces	Specifies the number of interfaces that are enabled.
Disabled Interfaces	Specifies the number of interfaces that are disabled.

clear igmp unicast-qos-adjust

To clear IGMP unicast rate adjustment database, use the **clear igmp unicast-qos-adjust** command in the EXEC mode.

clear igmp unicast-qos-adjust {**rate** | **statistics** } **interface** {*type* | *interface_path_id* }

Syntax Description

rate	Specifies the rate programmed in QoS.
statistics	Specifies the unicast rate adjustment statistics.
interface	Specifies the interface specific rate.
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 (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/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

Clears all unicast qos adjust parameters.

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	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.

Task ID

Task ID	Operation
multicast	exec

Examples

This is an example of using the **clear igmp unicast-qos-adjust** command:

```
RP/0/RSP0/CPU0:router# clear igmp unicast-qos-adjust rate interface Loopback 1
```

Neighbor Discovery Commands

This module describes the Cisco IOS XR software commands used to configure the Neighbor Discovery Commands for Broadband Network Gateway (BNG) on the Cisco ASR 9000 Series Router. For details regarding the related configurations, refer to the *Cisco ASR 9000 Series Aggregation Services Router Broadband Network Gateway Configuration Guide*.

- ipv6 nd dad attempts (BNG), page 338
- ipv6 nd framed-prefix-pool, page 341
- ipv6 nd managed-config-flag (BNG), page 342
- ipv6 nd ns-interval (BNG), page 344
- ipv6 nd nud-enable, page 346
- ipv6 nd other-config-flag (BNG), page 347
- ipv6 nd ra-initial, page 349
- ipv6 nd ra-interval (BNG), page 351
- ipv6 nd ra-lifetime (BNG), page 353
- ipv6 nd ra-unicast, page 355
- ipv6 nd reachable-time (BNG), page 356
- ipv6 nd suppress-cache-learning, page 358
- ipv6 nd suppress-ra (BNG), page 359

ipv6 nd dad attempts (BNG)

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

Dynamic template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.3.0	This command was supported in the dynamic template configuration mode for BNG.

Usage Guidelines

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

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 global configuration mode.

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 gigabitethernet0
```

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 shows how to display the state (tentative or duplicate) of the unicast IPv6 address on the dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv6 nd dad attempts 1
```

Related Commands

Command	Description
ipv6 nd ns-interval (BNG), on page 344	Configures the interval between IPv6 neighbor solicitation transmissions on an interface.

ipv6 nd framed-prefix-pool

To set the IPv6 Neighbor Discovery (ND) framed prefix pool, use the **ipv6 nd framed-prefix-pool** command in the dynamic template configuration mode. To disable the framed prefix pool configuration, use the **no** form of this command.

ipv6 nd framed-prefix-pool *pool_name*

no ipv6 nd framed-prefix-pool

Syntax Description

pool_name	Specifies the framed address pool name.

Command Default

None

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

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

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.

To enter the dynamic template configuration mode, run **dynamic-template** command in the global configuration mode.

Task ID

Task ID	Operations
config-services	read, write

Examples

This example creates an IPv6 framed prefix pool in the dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv6 nd framed-prefix-pool pool1
```

ipv6 nd managed-config-flag (BNG)

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

Dynamic template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.3.0	This command was supported in the dynamic template configuration mode for BNG.

Usage Guidelines

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

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 global configuration mode.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

This example shows how to configure the managed address configuration flag in IPv6 router advertisements on dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv6 nd managed-config-flag
```

Related Commands

Command	Description
show ipv6 interface (BNG), on page 301	Displays the usability status of interfaces configured for IPv6.

ipv6 nd ns-interval (BNG)

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

Dynamic template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.3.0	This command was supported in the dynamic template configuration mode for BNG.

Usage Guidelines

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

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 global configuration mode.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Task ID	Operations
config-services	read, write

Examples

This example configures an IPv6 neighbor solicit transmission interval of 9000 milliseconds in the dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv6 nd ns-interval 9000
```

Related Commands

Command	Description
show ipv6 interface (BNG), on page 301	Displays the usability status of interfaces configured for IPv6.

ipv6 nd nud-enable

To enable the IPv6 neighbor un-reachability detection (NUD), use the **ipv6 nd nud-enable** command in the dynamic template configuration mode. To disable IPv6 NUD, use the **no** form of this command.

ipv6 nd nud-enable

no ipv6 nd nud-enable

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
config-services	read, write

Examples

This example shows how to enable IPv6 neighbor un-reachability detection in dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv6 nd nud-enable
```

ipv6 nd other-config-flag (BNG)

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

Dynamic template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.3.0	This command was supported in the dynamic template configuration mode for BNG.

Usage Guidelines

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

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 global configuration mode.

Task ID

Task ID	Operations
ipv6	read, write

Task ID	Operations
network	read, write
config-services	read, write

Examples

This example configures the “other stateful configuration” flag for IPv6 router advertisements in the dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv6 nd other-config-flag
```

Related Commands

Command	Description
ipv6 nd managed-config-flag (BNG), on page 342	Sets the managed address configuration flag in IPv6 router advertisements.
show ipv6 interface (BNG), on page 301	Displays the usability status of interfaces configured for IPv6.

ipv6 nd ra-initial

To set the IPv6 initial router advertisement count and interval, use the **ipv6 nd ra-initial** command in the dynamic template configuration mode. To restore the default interval, use the **no** form of this command.

ipv6 nd ra-initial *count interval*

no ipv6 nd ra-initial

Syntax Description

value	The initial count or the initial number of the IPv6 router advertisements. The value ranges from 0-32.
interval	The interval (in seconds) between IPv6 router advertisement counts. The value ranges from 4-1800.

Command Default

None

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 4.3.0	This command was supported in the dynamic template configuration mode for BNG.

Usage Guidelines

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

To enter the dynamic template configuration mode, run **dynamic-template** command in the global configuration mode.

Task ID

Task ID	Operations
config-services	read, write

Examples

This example configures an IPv6 router advertisement count of 5 and an interval of 201 seconds in the dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv6 nd ra-initial 5 201
```

Related Commands

Command	Description
ipv6 nd ra-interval (BNG), on page 351	Configures the interval between IPv6 router advertisement transmissions on an interface.

ipv6 nd ra-interval (BNG)

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

Syntax Description

seconds	The interval (in seconds) between IPv6 router advertisement transmissions.

Command Default

seconds : 200 seconds

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.3.0	This command was supported in the dynamic template configuration mode for BNG.

Usage Guidelines

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

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 global configuration mode.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

This example configures an IPv6 router advertisement interval of 201 seconds in the dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv6 nd ra-interval 201
```

Related Commands

Command	Description
ipv6 nd ra-lifetime (BNG), on page 353	Configures the lifetime of an IPv6 router advertisement.
show ipv6 interface (BNG), on page 301	Displays the usability status of interfaces configured for IPv6.

ipv6 nd ra-lifetime (BNG)

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

Dynamic template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.3.0	This command was supported in the dynamic template configuration mode for BNG.

Usage Guidelines

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

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 global configuration mode.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Task ID	Operations
config-services	read, write

Examples

This example configures an IPv6 router advertisement lifetime of 1801 seconds in the dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv6 nd ra-lifetime 1801
```

Related Commands

Command	Description
ipv6 nd ra-interval (BNG), on page 351	Configures the interval between IPv6 router advertisement transmissions on an interface.
show ipv6 interface (BNG), on page 301	Displays the usability status of interfaces configured for IPv6.

ipv6 nd ra-unicast

To enable the IPv6 unicast router advertisement (RA), use the **ipv6 nd ra-unicast** command in the dynamic template configuration mode. To disable IPv6 unicast RA, use the **no** form of this command.

ipv6 nd ra-unicast

no ipv6 nd ra-unicast

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
config-services	read, write

Examples

This example shows how to enable the IPv6 unicast router advertisement in dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv6 nd ra-unicast
```

Related Commands

Command	Description
dynamic-template, on page 216	Groups a set of configuration items that can be applied to a group of subscribers.

ipv6 nd reachable-time (BNG)

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

Dynamic template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.3.0	This command was supported in the dynamic template configuration mode for BNG.

Usage Guidelines

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

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 global configuration mode.

Task ID

Task ID	Operations
ipv6	read, write

Task ID	Operations
network	read, write
config-services	read, write

Examples

This example shows how to configure an IPv6 reachable time of 1,700,000 milliseconds in the dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv6 nd reachable-time 1700000
```

Related Commands

Command	Description
show ipv6 interface (BNG), on page 301	Displays the usability status of interfaces configured for IPv6.

ipv6 nd suppress-cache-learning

To suppress cache learning for IPv6 neighbor discovery, use the **ipv6 nd suppress-cache-learning** command in the dynamic template configuration mode. To disable cache learning suppress, use the **no** form of this command.

ipv6 nd suppress-cache-learning

no ipv6 nd suppress-cache-learning

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 4.3.0	This command was introduced.

Usage Guidelines

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
config-services	read, write

Examples

This example shows how to suppress cache learning for IPv6 neighbor discovery in dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv6 nd suppress-cache-learning
```

ipv6 nd suppress-ra (BNG)

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

Dynamic template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.3.0	This command was supported in the dynamic template configuration mode for BNG.

Usage Guidelines

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

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 global configuration mode.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

This example shows how to suppress IPv6 router advertisements in the dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv6 nd suppress-ra
```

Related Commands

Command	Description
show ipv6 interface (BNG), on page 301	Displays the usability status of interfaces configured for IPv6.

BNG PPP Commands

This module describes the Cisco IOS XR software commands used to configure the PPP commands for Broadband Network Gateway (BNG) on the Cisco ASR 9000 Series Router. For details regarding the related configurations, refer to the *Cisco ASR 9000 Series Aggregation Services Router Broadband Network Gateway Configuration Guide*.

- ppp authentication (BNG), page 362
- ppp chap, page 365
- ppp ipcp, page 367
- ppp lcp, page 369
- ppp max-bad-auth (BNG), page 371
- ppp max-configure (BNG), page 373
- ppp max-failure (BNG), page 375
- ppp ms-chap, page 377
- ppp timeout, page 379
- show ppp interfaces (BNG), page 381
- show ppp statistics, page 389
- show ppp summary, page 392

ppp authentication (BNG)

To enable Challenge Handshake Authentication Protocol (CHAP), MS-CHAP, or Password Authentication Protocol (PAP), and to specify the order in which CHAP, MS-CHAP, and PAP authentication is selected on the interface, use the **ppp authentication** command an appropriate configuration mode. To disable PPP authentication, use the **no** form of this command.

ppp authentication *protocol* [*protocol* [*protocol*]] {*list-name*| **default**}

no ppp authentication

Syntax Description

protocol	Name of the authentication protocol used for PPP authentication. See Table 26: PPP Authentication Protocols for Negotiation, on page 363 for the appropriate keyword. You may select one, two, or all three protocols, in any order.
list-name	(Optional) Used with authentication, authorization, and accounting (AAA). Name of a list of methods of authentication to use. If no list name is specified, the system uses the default. The list is created with the **aaa authentication ppp** command.
default	(Optional) Specifies the name of the list of methods created with the **aaa authentication ppp** command.

Command Default

PPP authentication is not enabled.

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.
Release 4.2.0	This command was supported in the dynamic template configuration mode for BNG.

Usage Guidelines

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

When you enable CHAP or PAP authentication (or both), the local router requires the remote device to prove its identity before allowing data traffic to flow. PAP authentication requires the remote device to send a name and a password, which is checked against a matching entry in the local username database or in the remote security server database. CHAP authentication sends a challenge message to the remote device. The remote device encrypts the challenge value with a shared secret and returns the encrypted value and its name to the

local router in a response message. The local router attempts to match the remote device's name with an associated secret stored in the local username or remote security server database; it uses the stored secret to encrypt the original challenge and verify that the encrypted values match.

You can enable CHAP, MS-CHAP, or PAP in any order. If you enable all three methods, the first method specified is requested during link negotiation. If the peer suggests using the second method, or refuses the first method, the second method is tried. Some remote devices support only one method. Base the order in which you specify methods on the remote device's ability to correctly negotiate the appropriate method, and on the level of data line security you require. PAP usernames and passwords are sent as clear text strings, which can be intercepted and reused.

To enter the dynamic template configuration mode, run **dynamic-template** command in the global configuration mode.

Note If you use a *list-name* value that was not configured with the **aaa authentication ppp** command, then authentication does not complete successfully and the line does not come up.

Table 26: PPP Authentication Protocols for Negotiation, on page 363 lists the protocols used to negotiate PPP authentication.

Table 26: PPP Authentication Protocols for Negotiation

Protocol	Description
chap	Enables CHAP on an interface.
ms-chap	Enables Microsoft's version of CHAP (MS-CHAP) on an interface.
pap	Enables PAP on an interface.

Enabling or disabling PPP authentication does not affect the ability of the local router to authenticate itself to the remote device.

MS-CHAP is the Microsoft version of CHAP. Like the standard version of CHAP, MS-CHAP is used for PPP authentication. In this case, authentication occurs between a personal computer using Microsoft Windows NT or Microsoft Windows 95 and a Cisco router or access server acting as a network access server.

Enabling or disabling PPP authentication does not affect the local router authenticating itself to the remote device.

Task ID

Task ID	Operations
ppp	read, write
aaa	read, write

Examples

This is an example of configuring the **ppp authentication** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ppp authentication chap ms-chap pap
```

Related Commands

Command	Description
ppp chap, on page 365	Configures the PPP chap hostname.
ppp ipcp, on page 367	Sets IPCP negotiation options.
ppp lcp, on page 369	Configures the lcp global configure for PPP protocol.

ppp chap

To enable a router calling a collection of routers to configure a common Challenge Handshake Authentication Protocol (CHAP) for PPP interfaces, use the **ppp chap** command in the dynamic template configuration mode. To disable this feature, use the **no** form of this command.

ppp chap hostname *chap_hostname*

no ppp chap

Syntax Description

hostname	Sets the CHAP hostname.
chap_hostname	Specifies the CHAP hostname.

Command Default

None

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Use the **dynamic-template type ppp** command to enter the ppp dynamic template type configuration mode.

Task ID

Task ID	Operation
ppp	read, write

Examples

This is an example of configuring the **ppp chap** command in the dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ppp chap hostname host1
```

Related Commands

Command	Description
ppp authentication (BNG), on page 362	Sets PPP link authentication method.

ppp ipcp

To set Internet Protocol Control Protocol (IPCP) negotiation options, use the **ppp ipcp** command in the dynamic template configuration mode. To disable this feature, use the **no** form of this command.

ppp ipcp [**dns** { *primary_ip_address*| *secondary_ip_address* } | **mask** *peer_netmask_address* | **peer-address** { **default**| *peer_ipaddress*| **pool**| *pool_name* } | **renegotiation ignore** | **wins** |*primary_ipaddress* |*secondary_ipaddress*]

no ppp ipcp

Syntax Description

dns	Configures the dns options.
primary_ip_address	Specifies the primary DNS IP addresses.
secondary_ip_address	Specifies the secondary DNS IP addresses.
mask	Specifies the IPv4 netmask to use for the peer.
peer_netmask_address	Specifies the peer netmask address.
peer-address	Specifies the change in peer-address configuration.
default	Specifies the default peer IP address.
peer_ipaddress	Specifies the peer IP address.
pool	Configures the pool options.
pool_name	Specifies the pool name.
renegotiation	Specifies the peer negotiation options.
wins	Specifies the WINS options.

Command Default

None

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

Use the **dynamic-template type ppp** command to enter the ppp dynamic template type configuration mode.

Task ID

Task ID	Operation
ppp	read, write
aaa	read, write

Examples

This is an example of configuring the **ppp ipcp** command in the dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ppp ipcp
```

Related Commands

Command	Description
ppp authentication (BNG), on page 362	Sets PPP link authentication method.

ppp lcp

To enable the link control protocol (LCP) on PPP interfaces, use the **ppp lcp** command in the dynamic template configuration mode. To disable this feature, use the **no** form of this command.

ppp lcp [**delay** *delay_seconds delay_milliseconds* | **renegotiation ignore**]

no ppp lcp

Syntax Description

delay	Sets the time to delay before starting active LCP negotiations.
delay_seconds	Specifies the delay time in seconds. The value ranges from 0-255.
delay_milliseconds	Specifies the delay time in milliseconds. The value ranges from 0-999.
renegotiation	Specifies the peer renegotiation options.
ignore	Specifies the number of attempts that can be ignored by the peer to renegotiate LCP.

Command Default

None

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

Use the **dynamic-template type ppp** command to enter the ppp dynamic template type configuration mode.

Task ID

Task ID	Operation
ppp	read, write
aaa	read, write

Examples

This is an example of configuring the **ppp lcp** command in the dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router# configure
```

```
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ppp lcp delay 45 890
```

Related Commands

Command	Description
ppp authentication (BNG), on page 362	Sets PPP link authentication method.

ppp max-bad-auth (BNG)

To configure a PPP interface not to reset itself immediately after an authentication failure but instead to allow a specified number of authentication retries, use the **ppp max-bad-auth** command in the appropriate configuration mode. To reset to the default of immediate reset, use the **no** form of this command.

ppp max-bad-auth *retries*

no ppp max-bad-auth

Syntax Description

retries	Number of retries after which the interface is to reset itself. Range is from 0 to 10. Default is 0 retries.

Command Default

retries: 0

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.
Release 4.2.0	This command was supported in the dynamic template configuration mode for BNG.

Usage Guidelines

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

The **ppp max-bad-auth** command applies to any interface on which PPP encapsulation is enabled.

To enter the dynamic template configuration mode, run **dynamic-template** command in the global configuration mode.

Task ID

Task ID	Operations
ppp	read, write
aaa	read, write

Examples

This example shows how to allow two additional retries after an initial authentication failure in the dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ppp max-configure 5
```

ppp max-configure (BNG)

To specify the maximum number of configure requests to attempt (without response) before stopping the requests, use the **ppp max-configure** command in an appropriate configuration mode. To disable the maximum number of configure requests and return to the default, use the **no** form of this command.

ppp max-configure *retries*

no ppp max-configure

Syntax Description

retries	Maximum number of retries. Range is 4 through 20. Default is 10.

Command Default

retries: 10

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.
Release 4.2.0	This command was supported in the dynamic template configuration mode for BNG.

Usage Guidelines

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

Use the **ppp max-configure** command to specify how many times an attempt is made to establish a Link Control Protocol (LCP) session between two peers for a particular interface. If a configure request message receives a reply before the maximum number of configure requests are sent, further configure requests are abandoned.

To enter the dynamic template configuration mode, run **dynamic-template** command in the global configuration mode.

Task ID

Task ID	Operations
ppp	read, write
aaa	read, write

Examples

This example shows how a limit of four configure requests is specified in the dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ppp ipcp
```

Related Commands

Command	Description
ppp max-failure (BNG), on page 375	Configures the maximum number of consecutive CONFNAKs to permit before terminating a negotiation.

ppp max-failure (BNG)

To configure the maximum number of consecutive Configure Negative Acknowledgments (CONFNAKs) to permit before terminating a negotiation, use the **ppp max-failure** command in an appropriate configuration mode. To disable the maximum number of CONFNAKs and return to the default, use the **no** form of this command.

ppp max-failure *retries*

no ppp max-failure

Syntax Description

retries	Maximum number of CONFNAKs to permit before terminating a negotiation. Range is from 2 to 10. Default is 5.

Command Default

retries: 5

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.
Release 4.2.0	This command was supported in the dynamic template configuration mode for BNG.

Usage Guidelines

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

To enter the dynamic template configuration mode, run **dynamic-template** command in the global configuration mode.

Task ID

Task ID	Operations
ppp	read, write
aaa	read, write

Examples

This example shows how no more than three CONFNAKs are permitted before terminating the negotiation in the dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ppp max-failure 4
```

Related Commands

Command	Description
ppp max-configure (BNG), on page 373	Specifies the maximum number of configure requests to attempt (without response) before stopping the requests.

ppp ms-chap

To configure CHAP using the point-to-point protocol, use the **ppp ms-chap** command in the dynamic template configuration mode. To disable this feature, use the **no** form of this command.

ppp ms-chap hostname *chap_hostname*

no ppp ms-chap

Syntax Description

hostname	Sets the MS-CHAP hostname.
chap_hostname	Specifies the name of the MS-CHAP hostname.

Command Default

None

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Use the **dynamic-template** command to enter the dynamic template configuration mode.

Task ID

Task ID	Operation
ppp	read, write
aaa	read, write

Examples

This is an example of configuring the **ppp ms-chap** command in the dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ppp ms-chap hostname host1
```

Related Commands

Command	Description
ppp authentication (BNG), on page 362	Sets PPP link authentication method.

ppp timeout

To configure timeouts for PPP protocol, use the **ppp timeout** command in the dynamic template configuration mode. To disable this feature, use the **no** form of this command.

ppp timeout [**absolute** *absolute_minutes* | **authentication** *auth_seconds* | **retry** *retry_seconds*]

no ppp timeout

Syntax Description

absolute	Specifies the absolute timeout for a PPP session.
authentication	Specifies the maximum wait time to receive an authentication response.
retry	Specifies the maximum time to wait for a response during PPP negotiation.
absolute_minutes	Specifies the absolute timeout in minutes. This value ranges from 0-70000000.
auth_seconds	Specifies the authentication wait time in seconds. This value ranges from 3-30.
retry_seconds	Specifies the retry timeout in seconds. This value ranges from 1-10.

Command Default

None

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Use the **dynamic-template** command to enter the dynamic template configuration mode.

Task ID

Task ID	Operation
ppp	read, write
aaa	read, write

Examples

This is an example of configuring the **ppp timeout** command in the dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ppp timeout absolute 56
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ppp timeout authentication 4
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ppp timeout retry 5
```

Related Commands

Command	Description
ppp authentication (BNG), on page 362	Sets PPP link authentication method.

show ppp interfaces (BNG)

To display PPP state information for an interface, use the **show ppp interfaces** command in EXEC mode.

show ppp interfaces [**brief**| **detail**] {**all**| *type interface-path-id*| **location** *node-id*}

Syntax Description

brief	(Optional) Displays brief output for all interfaces on the router, for a specific POS interface instance, or for all interfaces on a specific node.
detail	(Optional) Displays detailed output for all interfaces on the router, for a specific interface instance, or for all interfaces on a specific node.
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.
all	(Optional) Displays detailed PPP information for all nodes.
location *node-id*	(Optional) Displays detailed PPP 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

EXEC

Command History

Release	Modification
Release 3.9.0	This command was introduced.
Release 4.2.0	This command was supported in the dynamic template configuration mode for BNG.

Usage Guidelines

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

There are seven possible PPP states applicable for either the Link Control Protocol (LCP) or the Network Control Protocol (NCP).

The command output displays a summary of the interface as it is in the PPP Interface Descriptor Block (IDB). The output includes the following information (where applicable):

- Interface state
- Line protocol state
- Link Control Protocol (LCP) state
- Network Control Protocol (NCP) state
- Multilink PPP state
- Multilink PPP configuration
- Keepalive configuration
- Authentication configuration
- Negotiated MRUs
- Negotiated IP addresses

This command can display information for a single interface, all interfaces on a specified node, or all interfaces on the router.

Task ID

Task ID	Operations
ppp	read

Examples

This example shows how to display PPP state information for a POS interface:

```
RP/0/RSP0/CPU0:router# show ppp interface POS 0/2/0/3

    POS0/2/0/3 is up, line protocol is up
      LCP: Open
         Keepalives enabled (10 sec)
         Local MRU: 4470 bytes
         Peer  MRU: 4470 bytes
      Authentication
         Of Us:    CHAP (Completed as 'test-user')
         Of Peer:  PAP (Completed as 'peer-user')
      CDPCP: Listen
      IPCP: Open
         Local IPv4 address: 55.0.0.1
         Peer IPv4 address:  55.0.0.2
         Peer DNS Primary:   55.0.0.254
         Peer DNS Secondary: 155.0.0.254
      IPV6CP: Open
         Local IPv6 address: fe80::3531:35ff:fe55:5747/128
```

```
      Peer IPv6 address:  fe80::3531:35ff:fe55:4213/128
    MPLSCP: Stopped
```

This example shows how to display PPP state information for a POS interface that is running as a Layer 2 attachment circuit:

```
RP/0/0/CPU0:# show ppp interface POS0/2/0/2

  POS0/2/0/2 is up, line protocol is up
    LCP: Open
      Running as L2 AC
```

This example shows how to display PPP state information for a multilink interface:

```
RP/0/RSP0/CPU0:router:# show ppp interface Multilink 0/3/0/0/100

  Multilink0/3/0/0/100 is up, line protocol is down
    LCP: Open
      SSO-State: Standby-Up
      Keepalives disabled
    IPCP: Open
      SSO-State: Standby-Up
      Local IPv4 address: 100.0.0.1
      Peer IPv4 address:  100.0.0.2
    IPV6CP: Open
      Local IPv6 address: fe80::3531:35ff:fe55:4600/128
      Peer IPv6 address:  fe80::3531:35ff:fe55:3215/128
    Multilink
      Local MRRU: 1500 bytes
      Peer MRRU:  1500 bytes
      Local Endpoint Discriminator: 1234567812345678
      Peer Endpoint Discriminator:  1111222233334444
      MCMP classes: Local 4, Remote 2
      Member links: 2 active, 6 inactive (min-active 2)
        - Serial0/3/1/3/1  ACTIVE
        - Serial0/3/1/3/2  ACTIVE
        - Serial0/3/1/3/3  INACTIVE : LCP not negotiated
        - Serial0/3/1/3/4  INACTIVE : Mismatching peer endpoint
        - Serial0/3/1/3/5  INACTIVE : Mismatching peer auth name
        - Serial0/3/1/3/6  INACTIVE : MRRU option rejected by Peer
        - Serial0/3/1/3/7  INACTIVE : Mismatching local MCMP classes
        - Serial0/3/1/3/8  INACTIVE : MCMP option rejected by peer
```

This example shows how to display PPP state information for a serial interface:

```
RP/0/RSP0/CPU0:router# show ppp interface Serial 0/3/1/3/1

  Serial0/3/1/3/1 is down, line protocol is down
    LCP: Open
      SSO-State: Standby-Up
      Keepalives enabled (10 sec)
      Local MRU: 1500 bytes
      Peer MRU:  1500 bytes
      Local Bundle MRRU: 1500 bytes
      Peer Bundle MRRU:  1500 bytes
      Local Endpoint Discriminator: 1234567812345678
      Peer Endpoint Discriminator:  1111222233334444
      Local MCMP Classes:  Not negotiated
      Remote MCMP Classes: Not negotiated
    Authentication
      Of Us:    CHAP (Completed as 'test-user')
      Of Peer:  PAP (Completed as 'peer-user')
    Multilink
      Multilink group id: 100
      Member status: ACTIVE
```

Table 27: show ppp interfaces Field Descriptions

Field	Description
Ack-Rcvd	Configuration acknowledgemt was received; waiting for peer to send configuration request.
Ack-Sent	Configuration acknowledgemt was sent; waiting for peer to respond to configuration request.
Authentication	Type of user authentication configured on the local equipment and on the peer equipment. Possible PPP authentication protocols are Challenge Handshake Authentication Protocol (CHAP), MS-CHAP, and Password Authentication Protocol (PAP).
Closed	Lower layer is up, but this layer is not required.
Closing	Shutting down due to local change.
Initial	Connection is idle.

Field	Description
IPCP	IP Control Protocol (IPCP) state. The seven possible states that may be displayed are as follows: • Initial—Lower layer is unavailable (Down), and no Open has occurred. The Restart timer is not running in the Initial state. • Starting—An administrative Open has been initiated, but the lower layer is still unavailable (Down). The Restart timer is not running in the Starting state. When the lower layer becomes available (Up), a Configure-Request is sent. • Closed— IPCP is not currently trying to negotiate. • Stopped—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received. • Closing—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received. Upon reception of a Terminate-Ack, the Closed state is entered. Upon the expiration of the Restart timer, a new Terminate-Request is transmitted, and the Restart timer is restarted. After the Restart timer has expired Max-Terminate times, the Closed state is entered. • Stopping—A Terminate-Request has been sent and the Restart timer is running, but a IPCP-Ack has not yet been received. Req-Sent. • ACKsent—IPCP has received a request and has replied to it. • ACKrcvd—IPCP has received a reply to a request it sent. • Open—IPCP is functioning properly.
Keepalive	Keepalive setting and interval in seconds for echo request packets.

Field	Description
LCP	Indicates the current state of LCP. The state of the LCP will report the following states: • Initial—Lower layer is unavailable (Down), and no Open has occurred. The Restart timer is not running in the Initial state. • Starting—An administrative Open has been initiated, but the lower layer is still unavailable (Down). The Restart timer is not running in the Starting state. When the lower layer becomes available (Up), a Configure-Request is sent. • Closed— LCP is not currently trying to negotiate. • Stopped—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received. • Closing—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received. Upon reception of a Terminate-Ack, the Closed state is entered. Upon the expiration of the Restart timer, a new Terminate-Request is transmitted, and the Restart timer is restarted. After the Restart timer has expired Max-Terminate times, the Closed state is entered. • Stopping—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received. Req-Sent. • ACKsent—LCP has received a request and has replied to it. • ACKrcvd—LCP has received a reply to a request it sent. • Open—LCP is functioning properly
Local IPv4 address	IPv4 address for the local interface.
Local MRU	Maximum receive unit. The maximum size of the information transported, in bytes, in the PPP packet received by the local equipment.
Open	Connection open.

Field	Description
OSICP	Open System Interconnection Control Protocol (OSICP) state. The possible states that may be displayed are as follows: • Initial—Lower layer is unavailable (Down), and no Open has occurred. The Restart timer is not running in the Initial state. • Starting—An administrative Open has been initiated, but the lower layer is still unavailable (Down). The Restart timer is not running in the Starting state. When the lower layer becomes available (Up), a Configure-Request is sent. • Closed— OSICP is not currently trying to negotiate. • Stopped—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received. • Closing—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received. Upon reception of a Terminate-Ack, the Closed state is entered. Upon the expiration of the Restart timer, a new Terminate-Request is transmitted, and the Restart timer is restarted. After the Restart timer has expired Max-Terminate times, the Closed state is entered. • Stopping—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received. Req-Sent. • ACKsent—OSICP has received a request and has replied to it. • ACKrcvd—OSICP has received a reply to a request it sent. • Open—OSICP is functioning properly.
Peer IPv4 address	IPv4 address for the peer equipment.
Peer MRU	Maximum receive unit. The maximum size of the information transported, in bytes, in the PPP packet received by the peer equipment.
Req-Sent	Configuration request was sent; waiting for peer to respond.

Field	Description
Starting	This layer is required, but lower layer is down.
Stopped	Listening for a configuration request.
Stopping	Shutting down as a result of interactions with peer.

show ppp statistics

To display the statistics information for PPP interfaces, use the **show ppp statistics** command in EXEC mode.

show ppp statistics {**extended**| {**location**| *location*}| **interface**| {*interface-type*| *interface-path-id*}| **summary**| {**location**| *location*}}

Syntax Description

extended	Displays the extended PPP statistics across all interfaces.
interface	Displays the PPP statistics for a single interface.
summary	Displays aggregated PPP statistics across all interfaces.
location	Displays the PPP statistics for interfaces at a location.
location	Specifies the location details.
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

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	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.

Task ID

Task ID	Operation
ppp	read

Examples

This example shows the output of the **show ppp statistics** command:

```
RP/0/RSP0/CPU0:router# show ppp statistics summary location 0/RSP0/CPU0

Thu Sep  6 06:38:17.668 DST
LCP
Packets                          Sent             Received
Conf-Req                            0                    0
Conf-Ack                            0                    0
Conf-Nak                            0                    0
Conf-Rej                            0                    0
Term-Req                            0                    0
Term-Ack                            0                    0
Code-Rej                            0                    0
Proto-Rej                           0                    0
Echo-Req                            0                    0
Echo-Rep                            0                    0
Disc-Req                            0                    0
Line state brought up: 0
Keepalive Link Failures: 0
Authentication
Packets                          Sent             Received
PAP
Request                          0                    0
Ack                              0                    0
Nak                              0                    0
(MS-)CHAP
Challenge                        0                    0
Response                         0                    0
Rep Success                      0                    0
Rep Fail                         0                    0
AAA authentication timeouts: 0
CDPCP
Packets                          Sent             Received
Conf-Req                            0                    0
Conf-Ack                            0                    0
Conf-Nak                            0                    0
Conf-Rej                            0                    0
Term-Req                            0                    0
Term-Ack                            0                    0
Proto-Rej                           0                    0
IPCP
Packets                          Sent             Received
Conf-Req                            0                    0
Conf-Ack                            0                    0
Conf-Nak                            0                    0
Conf-Rej                            0                    0
Term-Req                            0                    0
Term-Ack                            0                    0
Proto-Rej                           0                    0
IPCPIW
Packets                          Sent             Received
Conf-Req                            0                    0
Conf-Ack                            0                    0
Conf-Nak                            0                    0
Conf-Rej                            0                    0
Term-Req                            0                    0
Term-Ack                            0                    0
Proto-Rej                           0                    0
IPv6CP
```

```
Packets                          Sent             Received
Conf-Req                            0                    0
Conf-Ack                            0                    0
Conf-Nak                            0                    0
Conf-Rej                            0                    0
Term-Req                            0                    0
Term-Ack                            0                    0
Proto-Rej                           0                    0
MPLSCP
Packets                          Sent             Received
Conf-Req                            0                    0
Conf-Ack                            0                    0
Conf-Nak                            0                    0
Conf-Rej                            0                    0
Term-Req                            0                    0
Term-Ack                            0                    0
Proto-Rej                           0                    0
OSICP
Packets                          Sent             Received
Conf-Req                            0                    0
Conf-Ack                            0                    0
Conf-Nak                            0                    0
Conf-Rej                            0                    0
Term-Req                            0                    0
Term-Ack                            0                    0
Proto-Rej                           0                    0
```

Related Commands

Command	Description
show ppp interfaces (BNG), on page 381	Displays the PPP interfaces.
show ppp summary, on page 392	Displays the PPP summary.

show ppp summary

To display the summary information for the PPP interfaces, use the **show ppp summary** command in EXEC mode.

show ppp summary location *location*

Syntax Description

location	Displays the PPP summary for interfaces at a location.
location	Specifies the location details.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	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.

Task ID

Task ID	Operation
ppp	read

Examples

This example shows the output of the **show ppp summary** command for interfaces running PPP:

```
RP/0/RSP0/CPU0:router# show ppp summary location 0/5/CPU0

====================================
 Interfaces running PPP
====================================
 POS                    0
 Serial                 200
 PPPoE                  10000
 Multilink Bundles      100
 ---------------------------
 Total                  10300

====================================
```

```
 CP FSM States
=====================================
                     ACK   ACK   REQ   Stop- Clos- Stop- Clos- Start-
 Name    Total Open  sent  rcvd  sent  ping  ing   ped   ed    ing  Initial
 ------ ----- ----- ----- ----- ----- ----- ----- ----- ----- ----- -----
 LCP    10300 10300     0     0     0     0     0     0     0     0     0
 CDPCP    100     0     0     0   100     0     0     0     0     0     0
 IPCP   10000 10000     0     0     0     0     0     0     0     0     0
 IPv6CP     0     0     0     0     0     0     0     0     0     0     0
 MPLSCP     0     0     0     0     0     0     0     0     0     0     0
 OSICP      0     0     0     0     0     0     0     0     0     0     0

=====================================
 LCP/Authentication Phases
=====================================
 LCP Not Negotiated             100
 Authenticating                   0
 Line held down                   0
 Line Up (Local Termination)  10200
 Line Up (L2 Forwarded)           0
 Line UP (VPDN Tunneled)        100
```

Related Commands

Command	Description
show ppp statistics, on page 389	Displays the PPP statistics.
show ppp interfaces (BNG), on page 381	Displays the PPP interfaces.

PPPoE LAC-Specific Commands

This module describes the Cisco IOS XR software commands used to configure the PPPoE LAC-specific commands for Broadband Network Gateway (BNG) on the Cisco ASR 9000 Series Router. For details regarding the related configurations, refer to the *Cisco ASR 9000 Series Aggregation Services Router Broadband Network Gateway Configuration Guide*.

- l2tp-class, page 396
- l2tp reassembly, page 398
- process-failures switchover, page 399
- redundancy (BNG), page 401
- session-limit (BNG), page 402
- template (BNG), page 404
- tunnel, page 406
- vpdn, page 408
- vpn, page 410
- show l2tpv2, page 412
- show l2tpv2 redundancy, page 414
- show l2tpv2 redundancy mirroring, page 416
- show vpdn, page 418
- show vpdn redundancy, page 420
- show vpdn redundancy mirroring, page 422

l2tp-class

To create the l2tp class that needs to be used for L2TP parameters for the vpdn-group and to enter the l2tp class configuration submode, use the **l2tp-class** command in global configuration mode. To disable this feature, use the **no** form of this command.

l2tp-class {**c1** | **l1** | *l2tp_class_name* } [**authentication** | **congestion-control** | **digest** | **hello-interval** | **hidden** | **hostname** | **ip** | **password** | **receive-window** | **retransmit** | **security** | **timeout** | **tunnel**]

no l2tp-class

c1	Specifies the l2tp class name.
l1	Specifies the l2tp class name.
l2tp_class_name	Specifies the l2tp class name.
authentication	Authenticates the L2TP control connection.
congestion-control	Enables L2Tp congestion control.
digest	Specifies message digest configuration for L2TPv3 control connection.
hello-interval	Hides AVPs in outgoing control messages.
hidden	Sets HELLO message interval.
hostname	Specifies the local hostname for control connection authentication.
ip	Specifies the settings for tunnel.
password	Specifies the password for control connection authentication.
receive-window	Receives the window size for control connection.
retransmit	Specifies the control message retransmission parameters.
security	Specifies the L2TP security command.
timeout	Specifies the control connection timeout parameters.
tunnel	Specifies the tunnel settings.

Command Default No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

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

Task ID

Task ID	Operation
tunnel	read, write

Examples

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2tp-class c1
RP/0/RSP0/CPU0:router(config)# l2tp-class c1 congestion-control
```

Related Commands

Command	Description
tunnel, on page 406	Configures l2tp tunnel.

l2tp reassembly

To configure the L2TP reassembly feature on L2TP Access Concentrator (LAC), use the **l2tp reassembly** command in VPDN configuration mode. To disable this feature, use the **no** form of this command.

l2tp reassembly

no l2tp reassembly

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

VPDN configuration

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

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

Use the **vpdn** command in global configuration mode to enter the VPDN configuration mode.

When the L2TP reassembly is enabled, the line card supports 2000 concurrent flows in a steady state condition and the traffic rate supported for each line card is 10,000 packets per second (pps), which is 10,000 packet fragments IN per second and 5000 reassembled packets OUT per second.

Task ID

Task ID	Operation
tunnel	read, write

Examples

This example shows how to enable the L2TP reassembly feature on LAC:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# vpdn
RP/0/RSP0/CPU0:router(config-vpdn)# l2tp reassembly
```

process-failures switchover

To force a switchover in case of a process failure, use the **process-failures switchover** command in VPDN redundancy configuration mode.

process-failures switchover

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

VPDN redundancy configuration mode

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
tunnel	read, write

Examples

This is an example of enabling process-failures switchover.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# vpdn
RP/0/RSP0/CPU0:router(config-vpdn)# redundancy
RP/0/RSP0/CPU0:router(config-vpdn-redundancy)# process-failures switchover
RP/0/RSP0/CPU0:router(config-vpdn-redundancy)#
```

Related Commands

Command	Description
vpdn, on page 408	Configures VPDN and enters the VPDN sub-configuration mode.
redundancy (BNG), on page 401	Enables VPDN redundancy and enters the VPDN redundancy configuration mode.

redundancy (BNG)

To enable VPDN redundancy and to enter the VPDN redundancy configuration mode, use the **redundancy** command in VPDN configuration mode. To disable VPDN redundancy, use the **no** form of this command.

redundancy

no redundancy

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

VPDN configuration mode

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
tunnel	read, write

Examples

This is an example of enabling the vpdn **redundancy** and entering the vpdn redundancy configuration submode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# vpdn
RP/0/RSP0/CPU0:router(config-vpdn)# redundancy
RP/0/RSP0/CPU0:router(config-vpdn-redundancy)#
```

Related Commands

Command	Description
vpdn, on page 408	Configures VPDN and enters the VPDN sub-configuration mode.

session-limit (BNG)

To configure maximum simultaneous VPDN sessions, use the **session-limit** command in vpdn configuration mode. To disable this feature, use the **no** form of this command.

session-limit *number*

no session-limit

Syntax Description

number	Specifies the number of sessions and the value can range between 1-131072.

Command Default

The default and max value for global session-limit is 65536(64k sessions).

Command Modes

VPDN configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Use the **vpdn** command to enter vpdn configuration submode.

Note Per vpdn group session limiting is not supported on LAC.

If limit is configured after a number of sessions are up, then those sessions remain up irrespective of the limit and new sessions will not come up based on the limit. The **no** form of the command results in removing limits on number of sessions and new sessions are accepted by vpdn.

Task ID

Task ID	Operation
tunnel	read, write

Examples

This is an example of configuring the **session-limit** command in vpdn configuration mode:

```
RP/0/RSP0/CPU0:router# configure
```

```
RP/0/RSP0/CPU0:router(config)# vpdn
RP/0/RSP0/CPU0:router(config-vpdn)# session-limit 567
```

template (BNG)

To configure the VPDN template and enter the vpdn template configuration mode, use the **template** command in vpdn configuration mode. To disable vpdn template, use the **no** form of this command.

template *vpdn-template_name*{**description| caller-id| ip| dsl-line-forwarding| ipv4| l2tp-class| tunnel| vpn**}

no template

Syntax Description

vpdn-template_name	Specifies the vpdn template name.
description	Specifies the description of the vpdn template.
caller-id	Specifies the options to apply on calling station id.
ip	Specifies the tos ip value.
dsl-line-forwarding	Enables dsl line information forwarding.
ipv4	Specifies the ipv4 settings for tunnel.
l2tp-class	Specifies the l2tp class name.
tunnel	Specifies the l2tp tunnel commands.
vpn	Specifies the vpn id/vrf name.

Command Default

None

Command Modes

VPDN configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Use the **vpdn** command, to enter vpdn configuration submode.

Task ID

Task ID	Operation
tunnel	read, write

Examples

This is an example of configuring the **template** command in vpdn configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# vpdn
RP/0/RSP0/CPU0:router(config-vpdn)# template temp1
RP/0/RSP0/CPU0:router(config-vpdn-temp)#
```

tunnel

To configure the amount of time that the peer will be put in a dead cache, use the **tunnel** command in vpdn template configuration mode. To disable this feature, use the **no** form of this command.

tunnel busy list timeout *timeout_value*

no tunnel

Syntax Description

timeout_value	Specifies the amount of time in seconds that the peer will remain in dead cache. This value ranges from 60 to 65535.

Command Default

None

Command Modes

VPDN template configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Use the **vpdn template** command to enter vpdn template configuration submode.

Task ID

Task ID	Operation
tunnel	read, write

Examples

This is an example of configuring the **tunnel** command in vpdn template configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# vpdn template
RP/0/RSP0/CPU0:router(config-vpdn-template)# tunnel busy list timeout 56
```

Related Commands

Command	Description
vpdn, on page 408	Configures VPDN and to enter the VPDN sub-configuration mode.

vpdn

To configure VPDN and to enter the VPDN configuration submode, use the **vpdn** command in global configuration mode. To disable vpdn, use the **no** form of this command.

vpdn {**caller-id**| **history**| **l2tp**| **logging**| **session-limit**| **softshut**| **template**}

no vpdn

Syntax Description

caller-id	Specifies the options to apply on calling station id.
history	Enables VPDN history logging.
l2tp	Specifies the l2tpv2 protocol commands.
logging	Enables logging for VPDN.
session-limit	Allows to configure maximum simultaneous VPDN sessions.
softshut	Specifies that a new session is no longer allowed.
template	Specifies the VPDN template configuration.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Use the **vpdn** command to enter vpdn sub-configuration mode.

Task ID

Task ID	Operation
tunnel	read, write

Examples

This is an example of configuring the **vpdn** command in global configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# vpdn
RP/0/RSP0/CPU0:router(config-vpdn)# history failure
RP/0/RSP0/CPU0:router(config-vpdn)# softshut
```

vpn

To configure the VPN ID or VRF name, use the **vpn** command in vpdn template configuration mode. To disable this feature, use the **no** form of this command.

vpn { **id** *vpn_index*|**vrf** *vrf_name* }

no vpn

Syntax Description

id	Specifies the VPN ID.
vrf	Specifies the VRF.
vpn_index	Specifies a value between 0-ffffff.
vrf_name	Specifies the name of the vrf.

Command Default

None

Command Modes

VPDN template configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Use the **vpdn template** command to enter vpdn template configuration submode.

Task ID

Task ID	Operation
tunnel	read, write

Examples

This is an example of configuring the **vpn** command in vpdn template configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# vpdn template
```

```
RP/0/RSP0/CPU0:router(config-vpdn-template)# vpn vrf vrf1
```

show l2tpv2

To display the tunnel-related information, use the **show l2tpv2** command in the EXEC mode.

show l2tpv2{**class**| **counters**| **session**| **statistics**| **tunnel**}

Syntax Description

class	Displays the L2TP class details.
counters	Displays the L2TP counter information.
session	Displays the L2TP session information.
statistics	Displays the L2TP protocol statistics.
tunnel	Displays the L2TP tunnel information.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
ipv4	read
network	read

Examples

This is the sample output of the **show l2tpv2** command in the EXEC mode:

```
RP/0/RSP0/CPU0:router# show l2tpv2 class name c1
RP/0/RSP0/CPU0:router# show l2tpv2 counters forwarding tunnel id 67
RP/0/RSP0/CPU0:router# show l2tpv2 session brief if 89 789
```

```
RP/0/RSP0/CPU0:router# show l2tpv2 statistics | file tftp: vrf vrf1 |
RP/0/RSP0/CPU0:router# show l2tpv2 tunnel accounting statistics | file tftp: vrf vrf1 |
```

Show output for l2tpv2 session:

```
Sun Dec  4 22:37:48.554 PST

Session id 46362 is up, tunnel id 58775, logical session id 131086
  Remote session id is 16, remote tunnel id 54970
  Locally initiated session
Call serial number is 2062300015
Remote tunnel name is ios_lns
  Internet address is 3.3.3.4
Local tunnel name is blah_client_auth_id
  Internet address is 1.1.1.1
IP protocol 17
  Session is L2TP signaled
  Session state is established, time since change 00:06:56
  UDP checksums are enabled
  Sequencing is off
  Conditional debugging is disabled
  Unique ID is 0
  Session username is user3_vpdn@domain.com
    Interface GigabitEthernet0_0_0_1.pppoe14
```

Show output for l2tpv2 tunnel detail:

```
  Mon Dec  5 20:37:55.891 PST
Tunnel id 133 is up, remote id is 15705, 1 active sessions
  Locally initiated tunnel
  Tunnel state is established, time since change 6d09h
Tunnel transport is UDP (17)
  Remote tunnel name is IOS_LNS
    Internet Address 3.3.3.3, port 1701
  Local tunnel name is XR_LAC
    Internet Address 1.1.1.1, port 1701
  VRF name: default
  Tunnel group id
  L2TP class for tunnel is VPDN_3.3.3.3
  Control Ns 9205, Nr 342
  Local RWS 512 (default), Remote RWS 1024
  Control channel Congestion Control is disabled
  Tunnel PMTU checking disabled
  Retransmission time 1, max 1 seconds
  Unsent queuesize 0, max 0
  Resend queuesize 0, max 2
  Total resends 0, ZLB ACKs sent 340
  Total out-of-order dropped pkts 0
  Total out-of-order reorder pkts 0
  Total peer authentication failures 0
  Current no session pak queue check 0 of 5
  Retransmit time distribution: 0 0 0 0 0 0 0 0 0
  Control message authentication is disabled
```

Related Commands

Command	Description
l2tp-class, on page 396	Configures the l2tp class.

show l2tpv2 redundancy

To display the L2TP redundancy related information, use the **show l2tpv2 redundancy** command in the EXEC mode.

show l2tpv2 redundancy

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
tunnel	read

Examples

This is the sample output of the **show l2tpv2 redundancy** command in the EXEC mode:

```
RP/0/RSP0/CPU0:router# show l2tpv2 redundancy

  L2TP Tunnels:     0/0/0/0 (total/enabled/syncing/synced)
  L2TP Sessions:    0/0/0 (total/enabled/synced)

L2TP HA Timestamps:
  APP VPDN:
    Configured:                 TRUE
    Enabled:                    TRUE
    Time Configured:            Oct 12 14:00:25
    Time Unconfigured:          Oct 12 14:00:25
    Time Enabled:               Oct 12 14:00:35
    Time Disabled:
    Time Ready:                 Oct 12 14:00:35
    Time Not-Ready:

L2TP Switchover Resync Statistics:
  Poisoned sessions:                        0
```

```
Unestablished sessions:                    0
No app sessions:                           0
Sessions cleared by peer:                  0
Attempted during resync sessions:          0
Tunnel poisoned sessions:                  0
Tunnel cleared by peer sessions:           0
Excess restrans tunnel sessions:           0
Unestablished tunnel sessions:             0
Tunnel cleared other sessions:             0
Other cleared sessions:                    0
Poisoned sessions:                         0
Peer cleared tunnels:                      0
Excess retrans tunnel:                     0
Unestablished tunnels:                     0
Other cleared tunnels:                     0
```

Related Commands

Command	Description
l2tp-class, on page 396	Configures the L2TP class.

show l2tpv2 redundancy mirroring

To display the L2TP related mirroring statistics, use the **show l2tpv2 redundancy mirroring** command in the EXEC mode.

show l2tpv2 redundancy mirroring

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

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

This command displays mirrored data on the backup RP. If the data in the show command is not applicable on the backup RP, then trivial output such as '0' or empty is displayed.

Task ID

Task ID	Operation
tunnel	read

Examples

This is the sample output of the **show l2tpv2 redundancy mirroring** command in the EXEC mode:

```
RP/0/RSP0/CPU0:router# show l2tpv2 redundancy mirroring

L2TPv2 Mirroring Statistics
                                                  Since Last CLear
                          Send/Receive/Drop       Send/Receive/Drop
CCSync                          0/       0/       0       0/       0/       0
CCProtoSync                     0/       0/       0       0/       0/       0
CCUnsync                        0/       0/       0       0/       0/       0
CCSyncAck                       0/       0/       0       0/       0/       0
CCIAck                          0/       0/       0       0/       0/       0
CCSessionSyncDone               0/       0/       0       0/       0/       0
SessionSync                     0/       0/       0       0/       0/       0
AppStatus                       0/       1/       0       0/       1/       0
AddCCSteadyState                0/       1/       0       0/       1/       0
DelCCSteadyState                0/       0/       0       0/       0/       0
```

```
ADDSessionSteadyState           0/       5/       3          0/       5/       3
DelSessionSteadyState           0/       0/       0          0/       0/       0
CCOtherPackets                  0/       0/       0          0/       0/       0
ZLB ACK                         0/       0/       0          0/       0/       0
SCCRQ                           0/       0/       0          0/       0/       0
SCCRP                           0/       0/       0          0/       0/       0
SCCCN                           0/       1/       0          0/       1/       0
StopCCN                         0/       0/       0          0/       0/       0
Hello                           0/       0/       0          0/       0/       0
OCRQ                            0/       0/       0          0/       0/       0
OCRP                            0/       0/       0          0/       0/       0
OCCN                            0/       0/       0          0/       0/       0
ICRQ                            0/       1/       0          0/       1/       0
ICRP                            0/       0/       0          0/       0/       0
ICCN                            0/       4/       0          0/       4/       0
CDN                             0/       0/       0          0/       0/       0
WEN                             0/       0/       0          0/       0/       0
SLI                             0/       0/       0          0/       0/       0
L2TP QAD Send Statistics
                                     Total    Since Last Clear
  Messages Sent:                         0                   0
  Acks Sent:                             1                   1
  No Partner:                            0                   0
  Messages Failed:                       0                   0
  Acks Failed:                           0                   0
  Pending Acks:                          0                   0
  Suspends:                              0                   0
  Resumes:                               0                   0
  Sends Fragmented:                      0                   0
L2TP QAD Receive Statistics
                                     Total    Since Last Clear
  Messages Recevied:                     6                   6
  Acks Received:                         0                   0
  Acks Failed:                           0                   0
  Timeouts:                              0                   0
  Messages Processed:                    6                   6
  Message Drops:                         0                   0
  Stale Messages:                        0                   0
  Unknown Acks received:                 0                   0
```

Related Commands

Command	Description
l2tp-class, on page 396	Configures the L2TP class.

show vpdn

To display all vpdn-related information, use the **show vpdn** command in the EXEC mode.

show vpdn{**client**| **config**| **history**| **tunnel destination**| **session**}

Syntax Description

client	Displays VPDN client information.
config	Dislays VPDN configuration information.
history	Displays the vpdn session history information.
tunnel destination	Displays the vpdn tunnel destination information.
session	Displays the vpdn session information.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
ipv4	read
network	read

Examples

This is the sample output of the **show vpdn** command in the EXEC mode:

```
RP/0/RSP0/CPU0:router# show vpdn history failure | file tftp: vrf vrf1 |
RP/0/RSP0/CPU0:router# show vpdn client location 0/0/CPU0
RP/0/RSP0/CPU0:router# show vpdn tunnel destination detail |
```

```
RP/0/RSP0/CPU0:router# show vpdn session destination 4.5.4.5
```

Show output for vpdn session:

```
Sun Dec  4 22:34:19.328 PST

Subscriber label: 0x45, interface name: GigabitEthernet0/0/0/1.pppoe14
user name: user3_vpdn@domain.com
parent interface: GigabitEthernet0/0/0/1
state: est last change: 00:03:26
time to setup session:   0:164(s:msec)
conditional debug flags: 0
L2TP data
  local end point: 1.1.1.1 remote end point: 3.3.3.4
  call serial number: 2062300015
  local tunnel id: 58775 remote tunnel id: 54970
  local session id: 46362 remote session id: 16 remote port: 1701
  tunnel client authentication id: blah_client_auth_id
  tunnel server authentication id: ios_lns
  tunnel authentication: disabled
  class attribute mask:
      local hostname from AAA
      tunnel password from AAA
Subscriber data
  NAS port id: lac_circuit_id.lac_remote_id
  NAS port type: PPPoE over Ethernet
  physical channel id: 0
  Rx speed: 1000000000, Tx speed: 1000000000
Configuration data
  table id: 0xe0000000, VRF id: 0x60000000, VPN id: 0:0
  VRF name: default
  dsl line info forwarding: disabled, l2tp busy timeout: 60
  TOS mode: set, value: 13
```

Show output for tunnel destination:

```
Sun Dec  4 22:36:15.296 PST
Destination     VRF-name      Status  Load
3.3.3.4         default       active  1
```

Related Commands

Command	Description
vpdn, on page 408	Configures VPDN and enters the VPDN sub-configuration mode.

show vpdn redundancy

To display all vpdn redundancy related information, use the **show vpdn redundancy** command in the EXEC mode.

show vpdn redundancy

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
network	read

Examples

This is the sample output of the **show vpdn redundancy** command in the EXEC mode:

```
RP/0/RSP0/CPU0:router# show vpdn redundancy

VPDN HA STATUS      :       STEADY_STATE

VPDN HA SUMMARY
Total Sessions      :        2000
Sessions Synced     :        2000

VPDN HA TIME STAMPS
Init sync started   :        Dec 15 04:37:56
Init sync finished  :        Dec 15 04:37:56
Init sync aborted   :
```

Related Commands

Command	Description
vpdn, on page 408	Configures VPDN and enters the VPDN sub-configuration mode.
redundancy (BNG), on page 401	Enables VPDN redundancy and enters the VPDN redundancy configuration mode.

show vpdn redundancy mirroring

To display vpdn related mirroring statistics, use the **show vpdn redundancy mirroring** command in the EXEC mode.

show vpdn redundancy mirroring

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

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

This command displays mirrored data on the backup RP. If the data in the show command is not applicable on the backup RP, then trivial output such as '0' or empty is displayed.

Task ID

Task ID	Operation
network	read

Examples

This is the sample output of the **show vpdn redundancy mirroring** command in the EXEC mode:

```
RP/0/RSP0/CPU0:router# show vpdn redundancy mirroring

HA SSO Msg Stats

Sync not conn count                       0
SSO error count                           0
SSO batch error count                     0
ALLOC error count                         0
ALLOC count                               0

VPDN QAD Send Statistics
                                    Total    Since Last Clear
Messages :                              0                   0
Acks :                                  2                   2
Messages Failed:                        0                   0
```

```
Acks Failed:                            0               0
Pending Acks:                           0               0
Suspends:                               0               0
Resumes:                                0               0
Sends Fragmented:                       0               0

VPDN QAD Receive Statistics
                                      Total     Since Last Clear
Messages Recevied:                        2               2
Acks Received:                            0               0
Acks Failed:                              0               0
Timeouts:                                 0               0
Messages Processed:                       2               2
Message Drops:                            0               0
Stale Messages:                           0               0
Unknown Acks received:                    0               0
```

Related Commands

Command	Description
vpdn, on page 408	Configures VPDN and enters the VPDN sub-configuration mode.
redundancy (BNG), on page 401	Enables VPDN redundancy and enters the VPDN redundancy configuration mode.

PPPoE Commands

This module describes the Cisco IOS XR software commands used to configure the PPPoE commands for Broadband Network Gateway (BNG) on the Cisco ASR 9000 Series Router. For details regarding the related configurations, refer to the *Cisco ASR 9000 Series Aggregation Services Router Broadband Network Gateway Configuration Guide*.

- pado delay, page 426
- pado delay circuit-id, page 428
- pado delay remote-id, page 430
- pado delay service-name, page 432
- pppoe bba-group, page 434
- pppoe enable bba-group, page 437
- pppoe sessions limit, page 439
- pppoe sessions throttle, page 442
- clear pppoe statistics, page 444
- show pppoe interfaces, page 446
- show pppoe limits, page 448
- show pppoe statistics, page 452
- show pppoe summary, page 455
- show pppoe throttles, page 457

pado delay

To set a delay for a PPPoE Active Discovery Offer (PADO) message for a particular PPPoE BBA-Group, use the **pado delay** command in PPPoE BBA-Group configuration mode. To disable the PADO delay configuration, use the **no** form of this command.

pado delay *delay*

no pado delay

Syntax Description

delay	Delay value for PADO message, in milliseconds. The range is from 0 to 10000.

Command Default

None

Command Modes

PPPoE BBA-Group configuration

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

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

Setting a value of 0 for *delay* means that no transmission delay is set for PADO message. Setting a value of 10000 means that an infinite delay is set for PADO message or in other words, PADO message is never sent.

Task ID

Task ID	Operation
ppp	read, write

Examples

This example shows how to configure a delay of 1000 milliseconds for the PADO message:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pppoe bba-group bba1
RP/0/RSP0/CPU0:router(config-bbagroup)# pado delay 1000
```

Related Commands

Command	Description
pado delay circuit-id, on page 428	Configures a delay for PPPoE PADO message for a PPPoE BBA-Group in BNG, based on the Circuit-ID received in PADI message.
pado delay remote-id, on page 430	Configures a delay for PPPoE PADO message for a PPPoE BBA-Group in BNG, based on the Remote-ID received in PADI message.
pado delay service-name, on page 432	Configures a delay for PPPoE PADO message for a PPPoE BBA-Group in BNG, based on the Service-Name received in PADI message.

pado delay circuit-id

To set a delay for a PPPoE Active Discovery Offer (PADO) message for a particular PPPoE BBA-Group, based on the Circuit-ID received in PPPoE Active Discovery Initiator (PADI) message, use the **pado delay circuit-id** command in PPPoE BBA-Group configuration mode. To disable the PADO delay configuration based on the Circuit-ID, use the **no** form of this command.

pado delay circuit-id {*delay* | {**string | contains**} *string delay*}

no pado delay circuit-id {*delay* | {**string | contains**} *string delay*}

Syntax Description

delay	Delay value for PADO message, in milliseconds, based on the Circuit-ID. The range is from 0 to 10000.
string	Delays the PADO message, when the Circuit-ID string received in PADI message matches the configured *string*.
contains	Delays the PADO message, when the Circuit-ID received in PADI message contains the configured *string*.
string	String received in PADI message, that needs to be exactly matching the Circuit-ID (when used along with **string** keyword) or the string received in PADI message, that needs to be contained within the Circuit-ID (when used along with the **contains** keyword).

Command Default

None

Command Modes

PPPoE BBA-Group configuration

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

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

Setting a value of 0 for *delay* means that no transmission delay is set for the PADO message. Setting a value of 10000 means that an infinite delay is set for PADO message; or, in other words, the PADO message is never sent.

Within the category of Circuit-ID matches, full string matches are preferred to sub-string matches. If more than one sub-string match occur, the selection is based on a random order.

If there is neither a string match nor a sub-string match, the configured Circuit-ID delay is used (if a Circuit-ID is present in the PADI message), followed by the configured Remote-ID delay (if a Remote-ID is present in the PADI message).

If there are no matches, the configured pado delay is used for PADO message.

Task ID

Task ID	Operation
ppp	read, write

Examples

This example shows how to configure a delay of 1000 milliseconds for the PADO message:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pppoe bba-group bba1
RP/0/RSP0/CPU0:router(config-bbagroup)# pado delay circuit-id 1000
```

This example shows how to configure a delay of 8000 milliseconds for the PADO message, if the Circuit-ID received in the PADI message exactly matches the configured string (**circuit1** in this example):

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pppoe bba-group bba1
RP/0/RSP0/CPU0:router(config-bbagroup)# pado delay circuit-id string circuit1 8000
```

This example shows how to configure a delay of 5000 milliseconds for the PADO message, if the Circuit-ID received in the PADI message contains the configured string (**circuit2** in this example):

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pppoe bba-group bba1
RP/0/RSP0/CPU0:router(config-bbagroup)# pado delay circuit-id contains circuit2 5000
```

Related Commands

Command	Description
pado delay, on page 426	Configures a specific delay for PPPoE PADO message for a PPPoE BBA-Group in BNG.
pado delay remote-id, on page 430	Configures a delay for PPPoE PADO message for a PPPoE BBA-Group in BNG, based on the Remote-ID received in PADI message.
pado delay service-name, on page 432	Configures a delay for PPPoE PADO message for a PPPoE BBA-Group in BNG, based on the Service-Name received in PADI message.

pado delay remote-id

To set a delay for a PPPoE Active Discovery Offer (PADO) message for a particular PPPoE BBA-Group, based on the Remote-ID received in PPPoE Active Discovery Initiator (PADI) message, use the **pado delay remote-id** command in PPPoE BBA-Group configuration mode. To disable the PADO delay configuration based on the Remote-ID, use the **no** form of this command.

pado delay remote-id {*delay* | {**string | contains**} *string delay*}

no pado delay remote-id {*delay* | {**string | contains**} *string delay*}

Syntax Description

delay	Delay value for PADO message, in milliseconds, based on the Remote-ID. The range is from 0 to 10000.
string	Delays the PADO message, when the Remote-ID received in PADI message matches the configured *string*.
contains	Delays the PADO message, when the Remote-ID received in PADI message contains the configured *string*.
string	String received in PADI message, that needs to be matching the Remote-ID (when used along with **string** keyword) or the string received in PADI message, that needs to be contained within the Remote-ID (when used along with the **contains** keyword).

Command Default

None

Command Modes

PPPoE BBA-Group configuration

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

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

Setting a value of 0 for *delay* means that no transmission delay is set for the PADO message. Setting a value of 10000 means that an infinite delay is set for PADO message; or, in other words, the PADO message is never sent.

Within the category of Remote-ID matches, full string matches are preferred to sub-string matches. If more than one sub-string match occurs, the selection is based on a random order.

If there is neither a string match nor a sub-string match, the configured Circuit-ID delay is used (if a Circuit-ID is present in PADI message), followed by the configured Remote-ID delay (if a Remote-ID is present in PADI message).

If there are no matches, the configured pado delay is used for PADO message.

Task ID

Task ID	Operation
ppp	read, write

Examples

This example shows how to configure a delay of 1000 milliseconds for the PADO message:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pppoe bba-group bba1
RP/0/RSP0/CPU0:router(config-bbagroup)# pado delay remote-id 1000
```

This example shows how to configure a delay of 8000 milliseconds for the PADO message, if the Remote-ID received in the PADI message exactly matches the configured string (**remote1** in this example):

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pppoe bba-group bba1
RP/0/RSP0/CPU0:router(config-bbagroup)# pado delay remote-id string remote1 8000
```

This example shows how to configure a delay of 5000 milliseconds for the PADO message, if the remote-id received in the PADI message contains the configured string (**remote2** in this example):

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pppoe bba-group bba1
RP/0/RSP0/CPU0:router(config-bbagroup)# pado delay remote-id contains remote2 5000
```

Related Commands

Command	Description
pado delay, on page 426	Configures a specific delay for PPPoE PADO message for a PPPoE BBA-Group in BNG.
pado delay circuit-id, on page 428	Configures a delay for PPPoE PADO message for a PPPoE BBA-Group in BNG, based on the Circuit-ID received in PADI message.
pado delay service-name, on page 432	Configures a delay for PPPoE PADO message for a PPPoE BBA-Group in BNG, based on the Service-Name received in PADI message.

pado delay service-name

To set a delay for a PPPoE Active Discovery Offer (PADO) message for a particular PPPoE BBA-Group, based on the Service-Name received in PPPoE Active Discovery Initiator (PADI) message, use the **pado delay service-name** command in PPPoE BBA-Group configuration mode. To disable the PADO delay configuration based on the Service-Name, use the **no** form of this command.

pado delay service-name {**string | contains**} *string delay*

no pado delay service-name {**string | contains**} *string delay*

Syntax Description

string	Delays the PADO message, when the Service-Name string received in PADI message matches the configured *string*.
contains	Delays the PADO message, when the Service-Name received in PADI message contains the configured *string*.
string	String received in PADI message, that needs to be matching the Service-Name (when used along with **string** keyword) or the string received in PADI message, that needs to be contained within the Service-Name (when used along with the **contains** keyword).
delay	Delay value for PADO message, in milliseconds, based on the Service-Name. The range is from 0 to 10000.

Command Default

None

Command Modes

PPPoE BBA-Group configuration

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

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

Setting a value of 0 for *delay* means that no transmission delay is set for the PADO message. Setting a value of 10000 means that an infinite delay is set for PADO message; or, in other words, the PADO message is never sent.

Within the category of service-name matches, full string matches are preferred to sub-string matches. If more than one sub-string match occurs, the selection is based on a random order.

If there is neither a string match nor a sub-string match, the configured Circuit-ID delay is used (if a Circuit-ID is present in PADI message), followed by the configured Remote-ID delay (if a Remote-ID is present in PADI message).

If there are no matches, the configured pado delay is used for the PADO message.

Task ID

Task ID	Operation
ppp	read, write

Examples

This example shows how to configure a delay of 8000 milliseconds for the PADO message, if the Service-Name received in the PADI message exactly matches the configured string (**service1** in this example):

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pppoe bba-group bba1
RP/0/RSP0/CPU0:router(config-bbagroup)# pado delay service-name string service1 8000
```

This example shows how to configure a delay of 5000 milliseconds for the PADO message, if the Service-Name received in the PADI message contains the configured string (**service** in this example):

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pppoe bba-group bba1
RP/0/RSP0/CPU0:router(config-bbagroup)# pado delay service-name contains service 5000
```

Related Commands

Command	Description
pado delay, on page 426	Configures a specific delay for PPPoE PADO message for a PPPoE BBA-Group in BNG.
pado delay circuit-id, on page 428	Configures a delay for PPPoE PADO message for a PPPoE BBA-Group in BNG, based on the Circuit-ID received in PADI message.
pado delay remote-id, on page 430	Configures a delay for PPPoE PADO message for a PPPoE BBA-Group in BNG, based on the Remote-ID received in PADI message.

pppoe bba-group

To add configuration for a particular BBA-Group and to enter the BBA-Group submode, use the **pppoe bba-group** command in global configuration mode. To disable this feature, use the **no** form of this command.

pppoe bba-group *bba-group name*{**ac**| **name**| *new_name*| **control-packets**| **priority**| *priority_bits*| **service**| {**name**| *new_name*| **selection**| **disable**}| **sessions**| {**access-interface**| **circuit-id**| **mac**| **mac-iwf**| {**access-interface**| **pair**| **limit**}| **max**| {**access-interface**| **limit**| **throttle**}}| **limit**| *session_limit*| **tag**| {**ppp-max-payload**| {**deny**| **minimum**| *minimum_payload*}}}

no pppoe bba-group

Syntax Description

bba-group-name	Specifies the bba group name.
ac	Enables modification of the access concentrator configuration.
name	Indicates the name change to include in the AC tag.
new_name	Specifies the new name.
control-packets	Enables change of control-packets configuration.
priority	Sets the priority to use in PPPoE and PPP control packets.
priority_bits	Specifies the priority bits for outgoing PPPoE and PPP control packets. This ranges between 0 and 7, where 0 indicates highest priority and 7 indicates the lowest.
service	Enables modification of service configuration.
name	Configures the service name.
new_name	Specifies the new service name.
selection	Specifies the selection of unrequested service names.
disable	Disables the advertising of unrequested service names.
sessions	Enables modification of sessions configuration.
access-interface	Limits PPPoE sessions on any one access interface.
circuit-id	Limits PPPoE sessions with any one circuit-id.
mac	Limits or throttles PPPoE sessions from any one mac-address.

mac-iwf	Limits or throttles IWF PPPoE sessions from any one mac-address.
max	Sets a per-card session limit.
limit	Specifies the action of limiting the PPPoE sessions for various attributes.
session_limit	Specifies the access-interface session limit. The value ranges from 1 to 65535.
tag	Enables modification of tag configuration.
ppp-max-payload	Modifies the ppp-max-payload configuration and allows to configure minimum and maximum payloads.
deny	Ignores the ppp-max-payload tag.
minimum	Configures the minimum payload.
minimum_payload	Specifies the value of the minimum payload. The value ranges from 500 to 2000.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

BBA-Groups are configured globally (these are essentially configuration templates), containing the PPPoE configuration settings.

When this configuration changes to use a different BBAGroup, then all existing PPPoE sessions running under the interface are terminated.

Task ID

Task ID	Operation
ppp	read, write

Examples

This is an example of configuring the **pppoe bba-group** command in global configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pppoe bba-group bba1
RP/0/RSP0/CPU0:router(config-bbagroup)# ac name red
RP/0/RSP0/CPU0:router(config-bbagroup)# service name blue
RP/0/RSP0/CPU0:router(config-bbagroup)# service selection disable
RP/0/RSP0/CPU0:router(config-bbagroup)# sessions max limit 45
RP/0/RSP0/CPU0:router(config-bbagroup)# tag ppp-max-payload minimum 689 maximum 788
```

Related Commands

Command	Description
pppoe enable bba-group, on page 437	Enables PPPoE on an interface.

pppoe enable bba-group

To enable pppoe on an interface, use the **pppoe enable bba-group** command in interface configuration mode. To disable the pppoe on the interface, use the **no** form of this command.

pppoe enable bba-group *bba-group name*

no pppoe enable bba-group

Syntax Description

bba-group name	Specifies the name of the bba-group.

Command Default

If no BBA-Group is specified, then the default configuration options are used, else the BBA-Group's configuration is used on this interface.

Command Modes

Interface configuration

Command History

Release	Modification
Release 4.2.0	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 configuration changes to use a different BBAGroup, then all existing PPPoE sessions running under the interface are terminated.

Task ID

Task ID	Operation
ppp	read, write

Examples

This is an example of configuring the **pppoe enable bba-group** command in interface configuration mode:

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)#interface Bundle-Ether100.10
RP/0/RSP0/CPU0:router(config-if)# pppoe enable bba-group bba1
```

Related Commands

Command	Description
pppoe bba-group, on page 434	Enables you to add configuration for a particular bba-group.

pppoe sessions limit

To set a limit for PPPoE sessions in a particular PPPoE BBA-Group, use the **sessions limit** command in PPPoE BBA-Group configuration mode. To remove the specified limit for PPPoE sessions, use the **no** form of this command.

sessions {**access-interface**| **circuit-id**| **circuit-id-and-remote-id**| **inner-vlan**| {**mac**| **mac-iwf**} **[access-interface]**| **max**| **outer-vlan**| **remote-id**| **vlan**} **limit** *limit-value* [**threshold** *threshold-value*]

no sessions {**access-interface**| **circuit-id**| **circuit-id-and-remote-id**| **inner-vlan**| {**mac**| **mac-iwf**} **[access-interface]**| **max**| **outer-vlan**| **remote-id**| **vlan**} **limit** *limit-value* [**threshold** *threshold-value*]

Syntax Description

access-interface	Limits PPPoE sessions on any one access interface.
circuit-id	Limits PPPoE sessions with any one circuit-ID.
circuit-id-and-remote-id	Limits PPPoE sessions by circuit-id and remote-id.
inner-vlan	Limits PPPoE sessions with any one inner-vlan id.
mac	Limits PPPoE sessions from any one mac address.
mac-iwf	Limits IWF PPPoE sessions from any one mac address.
max	Sets a per-card session limit.
outer-vlan	Limits PPPoE sessions with any one outer-vlan id.
remote-id	Limits PPPoE sessions with any one remote-id.
vlan	Limits PPPoE sessions with matching vlan ids.
limit	Specifies the action of limiting the PPPoE sessions for various attributes.
limit-value	Specifies the session limit value. The range is from 1 to 65535. The default is 65535.
threshold	Specifies the action of generating a log message when the threshold has reached.
threshold-value	Specifies the threshold value. The range is from 1 to 65535.

Command Default

None

Command Modes

PPPoE BBA-Group configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.
Release 4.3.1	The PPPoE sessions limit support was extended for **mac access-interface**, **mac-iwf access-interface**, **inner-vlan**, **outer-vlan**, **vlan**, and **circuit-id-and-remote-id** Support for the optional argument, **threshold** was added.

Usage Guidelines

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

If a session limit is configured after the limit has already been exceeded, the existing sessions are torn down until the number of sessions matches the configured limit.

If both mac limit and mac-iwf limit are configured, only IWF limit is used for IWF sessions, so that a higher IWF limit than the limit for non-IWF sessions can be used. The same is the case if both mac access-interface limit and mac-iwf access-interface limit are configured.

Task ID

Task ID	Operation
ppp	read, write

Examples

This example shows how to configure a pppoe session limit of 1000, for each access-interface in a PPPoE BBA-Group:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pppoe bba-group bba1
RP/0/RSP0/CPU0:router(config-bbagroup)# sessions access-interface limit 1000
```

This example shows how to configure a pppoe session limit of 5000 and a threshold value of 4900, for each peer mac-address under individual access-interface in a PPPoE BBA-Group:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pppoe bba-group bba1
RP/0/RSP0/CPU0:router(config-bbagroup)# sessions mac access-interface limit 5000 threshold
 4900
```

This example shows how to configure a pppoe session limit of 8000 and a threshold value of 7500, for each circuit-id in a PPPoE BBA-Group:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pppoe bba-group bba1
```

```
RP/0/RSP0/CPU0:router(config-bbagroup)# sessions circuit-id limit 8000 threshold 7500
```

Related Commands

Command	Description
pppoe sessions throttle, on page 442	Configures a throttle value for PPPoE sessions for a PPPoE BBA-Group in BNG.
show pppoe limits, on page 448	Shows the PPPoE session limit information.

pppoe sessions throttle

To set a throttle value for the PPPoE sessions for a particular PPPoE BBA-Group, use the **sessions throttle** command in PPPoE BBA-Group configuration mode. To remove the specified throttle value for PPPoE sessions, use the **no** form of this command.

sessions {**circuit-id**| **circuit-id-and-remote-id**| **inner-vlan**| **mac [access-interface]**| **mac-iwf access-interface**| **outer-vlan**| **remote-id**| **vlan**} **throttle** *request-count request-period blocking-period*

no sessions {**circuit-id**| **circuit-id-and-remote-id**| **inner-vlan**| **mac [access-interface]**| **mac-iwf access-interface**| **outer-vlan**| **remote-id**| **vlan**} **throttle** *request-count request-period blocking-period*

Syntax Description

access-interface	Throttles PPPoE sessions based on any one access interface
circuit-id	Throttles PPPoE sessions with any one circuit-id.
circuit-id-and-remote-id	Throttles PPPoE sessions by circuit-id and remote-id.
inner-vlan	Throttles PPPoE sessions with any one inner-vlan id.
mac	Throttles PPPoE sessions from any one mac address.
mac-iwf	Throttles Inter-Working Function (IWF) sessions from any one mac address.
outer-vlan	Throttles PPPoE sessions with any one outer-vlan id.
remote-id	Throttles PPPoE sessions with any one remote-id.
vlan	Throttles PPPoE sessions with matching vlan ids.
throttle	Specifies the action of throttling the PPPoE sessions for various attributes.
request-count	Specifies the number of session requests allowed before throttling.
request-period	Specifies the time interval during which the session requests are counted.
blocking-period	Specifies the time interval during which no more requests from the subscriber are accepted, when the subscriber has already been throttled.

Command Default

Sessions throttle is disabled by default.

Command Modes

PPPoE BBA-Group configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.
Release 4.3.1	The pppoe sessions throttle support was extended for **circuit-id**, **remote-id**, **inner-vlan**, **outer-vlan**, **vlan** and **circuit-id-and-remote-id** Support for the variables, *request-count*, *request-period* and *blocking-period* was added.

Usage Guidelines

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

If both mac access-interface throttle and mac-iwf access-interface throttle are configured, only IWF throttle is used for IWF sessions, so that different throttling can be applied to IWF and non-IWF sessions.

Task ID

Task ID	Operation
ppp	read, write

Examples

This example shows how to configure a throttle for pppoe sessions for each circuit-id in a PPPoE BBA-Group:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pppoe bba-group bba1
RP/0/RSP0/CPU0:router(config-bbagroup)# sessions circuit-id throttle 1000 50 25
```

This example shows how to configure a throttle for IWF session requests for each peer mac-address under individual access-interface in a PPPoE BBA-Group:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pppoe bba-group bba1
RP/0/RSP0/CPU0:router(config-bbagroup)# sessions mac-iwf access-interface throttle 5000 100
 50
```

Related Commands

Command	Description
pppoe sessions limit, on page 439	Configures a limit for PPPoE sessions for a PPPoE BBA-Group in BNG.
show pppoe throttles, on page 457	Shows the throttle information for the PPPoE sessions.

clear pppoe statistics

To clear the statistics of packets received and sent by the PPPoE sessions in BNG, use the **clear pppoe statistics** command in EXEC mode.

clear pppoe statistics [internal] location *node-id*

Syntax Description

internal	Clears internal PPPoE statistics.
location	Clears PPPoE statistics for a given node.
node-id	Specifies the node ID. The node-id argument is entered in the rack/slot/module notation.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
ppp	read, write

Examples

This example shows the sample output before and after clearing the PPPoE statistics:

```
RP/0/RSP0/CPU0:router# show pppoe statistics
Tue Feb  5 21:17:36.137 UTC

0/RSP1/CPU0
-----------
Packets                    Sent        Received         Dropped
-------------------------------------------------------------------
```

```
PADI                            0           16163              60
PADO                        16103               0               0
PADR                            0           16103               0
PADS (success)              16102               0               0
PADS (error)                    1               0               0
PADT                        28173              19               0
Session-stage                   0            8200               0
Other                           0               0               0
                            -----           -----           -----
TOTAL                       60379           40485              60

Packet Error                                            Count
-------------------------------------------------------------
Session-stage packet for unknown session                 4097
Session-stage packet with no error                          6
                                                        -----
TOTAL                                                    4103

RP/0/RSP0/CPU0:router# clear pppoe statistics location 0/RSP1/CPU0

RP/0/RSP0/CPU0:router# show pppoe statistics
Tue Feb  5 21:18:10.509 UTC

0/RSP1/CPU0
-----------
Packets                       Sent        Received         Dropped
-------------------------------------------------------------------
PADI                             0               0               0
PADO                             0               0               0
PADR                             0               0               0
PADS (success)                   0               0               0
PADS (error)                     0               0               0
PADT                             0               0               0
Session-stage                    0               0               0
Other                            0               0               0
                             -----           -----           -----
TOTAL                            0               0               0

Packet Error                                            Count
-------------------------------------------------------------
                                                        -----
TOTAL                                                       0

RP/0/RSP0/CPU0:router#
```

Related Commands

Command	Description
show pppoe statistics, on page 452	Shows the counters for packets received and sent by the PPPoE sessions.

show pppoe interfaces

To display a summary of the protocol state for the specified PPPoE interface filtered by circuit-id, remote-id, interface or location, use the **show pppoe interfaces** command in the EXEC mode.

show pppoe interfaces {**circuit-id**| *circuit_id*| **remote-id**| *remote_id*| **access-interface**| *type*| *interface-path-id*| **location**| *node*| **all**}

Syntax Description

circuit-id	Shows information for a given circuit-id.
circuit_id	Specifies the circuit-id to show data for.
remote-id	Show information for a given remote-id.
remote_id	Specifies the remote-id to show data for.
access-interface	Shows PPPoE status for all sessions on a single access 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.
location	Shows PPPoE status for all sessions at a location.
node	Specifies the fully qualified location specification.
all	Shows PPPoE status for all sessions.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	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.

Task ID

Task ID	Operation
ppp	read

Examples

This is a sample output of the **show pppoe interfaces** command:

```
RP/0/RSP0/CPU0:router# show pppoe interfaces Loopback1
Loopback1 is Complete
Session id: 1
Access interface: Loopback1
BBA-Group: blue
Local MAC address: aabb.cc00.8301
Remote MAC address: aabb.cc00.8201
Tags:
Service-Name: service1
Max-Payload: 1500
IWF
Circuit-ID: circuit1
Remote-ID: remote1
```

show pppoe limits

To show the PPPoE session limit information, use the **show pppoe limits** command in the EXEC mode.

show pppoe limits [active] [**access-interface** *type interface-path-id* | **bba-group** *bba-group-name* | **location** *node*]

Syntax Description

active	Shows only those throttles that are currently blocking packets.
access-interface	Shows PPPoE status for all sessions on a single access 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.
bba-group	Shows throttles for all interfaces with a given bba-group.
bba_group_name	Specifies the bba-group to show throttle for.
location	Shows PPPoE status for all sessions at a location.
node	Specifies the fully qualified location specification.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	This command was introduced.
Release 4.3.1	The command output was extended for the session limits of **mac access-interface**, **mac-iwf access-interface**, **inner-vlan**, **outer-vlan**, **vlan** and **circuit-id-and-remote-id**

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.

Task ID

Task ID	Operation
ppp	read

Examples

This is a sample output of the **show pppoe limits** command:

```
RP/0/RSP0/CPU0:router# show pppoe limits active access-interfaces loopback 45
BBA-Group TEST
--------------
Card session limit information:
Maximum session limit: 50 sessions
Warning threshold: 40 sessions
State #Sessions
----- ---------
Block 50
Access-interface session limits not configured.
MAC session limits not configured.
MAC-IWF session limits not configured.
Circuit-ID session limit information:
Maximum session limit: 50 sessions
Warning threshold: 40 sessions
Circuit-ID State #Sessions
---------- ----- ---------
circuit_id1 Block 50
circuit_id_field_which_can_be_up_to_sixty_four_chars_long Warn 45
circuit_id2 OK 32
circuit_id,/[]* OK 1
BBA-Group TEST2
---------------
Card session limits not configured.
Access-interfaces session limit information:
Maximum session limit: 50 sessions
Warning threshold: 40 sessions
Access-Interface State #Sessions
---------------- ----- ---------
GE0/1/0/0/0 Block 50
GE0/1/0/0/1 Warn 45
GE0/1/0/0/2 OK 32
GE0/1/0/0/0.12 OK 1
MAC session limits not configured.
MAC-IWF session limits not configured.
Circuit-ID session limits not configured.
```

This is another sample output of **show pppoe limits** command:

```
RP/0/RSP0/CPU0:router# show pppoe limits
Tue Feb  5 21:09:40.823 UTC

0/RSP1/CPU0
-----------
BBA-Group BNG_BBA
-----------------
Card session limits not configured.

Access-interface session limits not configured.

MAC session limits not configured.
```

```
MAC-IWF session limits not configured.

Circuit-ID session limit information:
  Maximum session limit: 10 sessions
  Warning threshold:     8 sessions

  Circuit-ID                                                    State   #Sessions
  ----------                                                    -----   ---------
  circuit0                                                      Block          10

Remote-ID session limit information:
  Maximum session limit: 10 sessions
  Warning threshold:     8 sessions

  Remote-ID                                                     State   #Sessions
  ----------                                                    -----   ---------
  remote10                                                      Block          10

MAC-Access-Interface session limits not configured.

MAC-IWF-Access-Interface session limits not configured.

Inner-VLAN-ID session limit information:
  Maximum session limit: 10 sessions
  Warning threshold:     8 sessions

  Access-Int                  Inner VLAN ID                     State   #Sessions
  ----------                  -------------                     -----   ---------
  BE2.10                      10                                Block          10

Outer-VLAN-ID session limit information:
  Maximum session limit: 10 sessions
  Warning threshold:     8 sessions

  Access-Int                  Outer VLAN ID                     State   #Sessions
  ----------                  -------------                     -----   ---------
  BE2.10                      10                                Block          10

VLAN-ID session limit information:
  Maximum session limit: 10 sessions
  Warning threshold:     8 sessions

  Access-Int            Outer, Inner VLAN ID                    State   #Sessions
  ----------            --------------------                    -----   ---------
  BE2.10                   10, 10                               Block          10

Circuit-ID-and-Remote-ID session limit information:
  Maximum session limit: 10 sessions
  Warning threshold:     8 sessions

  Circuit-ID                                                    State   #Sessions
    Remote-ID                                                             (/Max)
  -----------                                                   -----   ---------
  circuit0                                                      Block          10
    remote10
```

This table describes the significant fields displayed in the **show pppoe limits** command output :

Field	Description
Block	Specifies that the number of sessions is at the maximum limit.
OK	Specifies that the number of sessions is below the maximum limit and the warning threshold (if configured).

Field	Description
Warn	Specifies that the number of sessions is at or above the warning threshold (if configured). No warning threshold is used when a limit is overridden.

Related Commands

Command	Description
pppoe sessions limit, on page 439	Configures a limit for PPPoE sessions for a PPPoE BBA-Group in BNG.
show pppoe throttles, on page 457	Shows the throttle information for the PPPoE sessions.
show pppoe interfaces, on page 446	Shows a summary of the protocol state for the specified PPPoE interface filtered by circuit-id, remote-id, interface, or location.
show pppoe statistics, on page 452	Shows the counters for packets received and sent by the PPPoE sessions.
show pppoe summary, on page 455	Shows summary information of the PPPoE sessions.

show pppoe statistics

To show the counters for packets received and sent by the PPPoE sessions, use the **show pppoe statistics** command in the EXEC mode.

show pppoe statistics {**access-interface**| *type*| *interface-path-id*| **internal** | { **location**| *node*}| **location**| *node*}

Syntax Description

access-interface	Shows PPPoE status for all sessions on a single access 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.
internal	Shows internal PPPoE statistics.
location	Shows PPPoE status for all sessions at a location.
node	Specifies the fully qualified location specification.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	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.

Task ID

Task ID	Operation
ppp	read

Examples

This is the sample output of the **show pppoe statistics** command:

```
RP/0/RSP0/CPU0:router# show pppoe statistics access-interfaces Loopback 156

Packets Sent Received Dropped
-----------------------------------------------------------------
PADI 0 3723 18
PADO 3182 0 0
PADR 0 1732 93
PADS (success) 1601 0 0
PADS (error) 38 0 0
PADT 158 552 9
Session-stage 0 18 17
Other 0 2 2
----- ----- -----
TOTAL 3979 6063 139

RP/0/RSP0/CPU0:router# show pppoe statistics location 0/2/cpu0

Packets Sent Received Dropped
-----------------------------------------------------------------
PADI 0 3723 18
PADO 3182 0 0
PADR 0 1732 93
PADS (success) 1601 0 0
PADS (error) 38 0 0
PADT 158 552 9
Session-stage 0 18 17
Other 0 2 2
----- ----- -----
TOTAL 3979 6063 139
Packet Error Count
-----------------------------------------------------------
No interface handle 1
No packet payload 1
No packet mac-address 1
Invalid version-type value 3
Bad packet length 7
Unknown interface 11
PADO receive
ed 1
PADS received 1
Unknown packet type received 1
Unexpected Session-ID in packet 1
No Service-Name Tag 11
PADT for unknown session 13
PADT with wrong peer-mac 7
PADT before PADS sent 1
Session-stage packet for unknown session 13
Session-stage packet with wrong mac 19
Session-stage packet with no error 1
Tag too short 1
Bad tag-length field 1
Multiple Service-Name tags 1
Multiple Max-Payload tags 1
Invalid Max-Payload tag 1
Multiple Vendor-specific tags 1
Unexpected AC-Name tag 1
Unexpected error tags 3
Unknown tag received 1
No IANA code in vendor tag 1
Invalid IANA code in vendor tag 1
Vendor tag too short 1
Bad vendor tag length field 1
Multiple Host-Uniq tags 1
Multiple Circuit-ID tags 1
Multiple Remote-ID tags 1
Invalid DSL tag 1
Multiple of the same DSL tag 1
```

```
Invalid IWF tag 1
Multiple IWF tags 1
Unknown vendor-tag 11
No space left in packet 1
Duplicate Host-Uniq tag received 1
Packet too long 1
-----
TOTAL 140
```

show pppoe summary

To show the summary information for the PPPoE sessions, use the **show pppoe summary** command in the EXEC mode.

show pppoe summary {**per-access-interface**| **total**} { **location**| *node*}

Syntax Description

per-access-interface	Summarizes PPPoE sessions running on each access-interface.
total	Shows the overall summary information of access-interfaces and sessions.
location	Shows PPPoE status for all sessions at a location.
node	Specifies the fully qualified location specification.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	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.

Task ID

Task ID	Operation
ppp	read

Examples

This is the sample output of the **show pppoe summary** command:

```
RP/0/RSP0/CPU0:router# show pppoe summary per-access-interfaces location 0/1/cpu0

COMPLETE: Complete PPPoE Sessions
INCOMPLETE: PPPoE sessions being brought up or torn down
Interface BBA-Group READY TOTAL COMPLETE INCOMPLETE
------------------------------------------------------------------------------
Fa0/1/0/0 blue Y 20 18 2
```

```
Fa0/1/0/1.1 red Y 128000 100010 27990
Fa0/1/0/1.2 green N 0 0 0
---------------------------------
TOTAL 2 128020 100028 27992
RP/0/0/CPU0:demo#show pppoe summary total location 0/5/cpu0
==============================
Configured Access Interfaces
==============================
Ready 300
Not-Ready 15
----------------------------
TOTAL 315
==============================
PPPoE Sessions
==============================
Complete 3812
Incomplete 302
----------------------------
TOTAL 4114
==============================
Flow Control
==============================
Limit 1000
In Flight 12
Dropped 212
Disconnected 6
Successful 1021
```

show pppoe throttles

To show the throttle information for the PPPoE sessions, use the **show pppoe throttles** command in the EXEC mode.

show pppoe throttles [active] [**access-interface** *type interface-path-id* | **bba-group** *bba-group-name* | **location** *node*]

Syntax Description

active	Shows only those throttles that are currently blocking packets.
access-interface	Shows PPPoE status for all sessions on a single access 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.
bba-group	Shows throttles for all interfaces with a given bba-group.
bba_group_name	Specifies the bba-group name.
location	Shows PPPoE status for all sessions at a location.
node	Specifies the fully qualified location specification.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	This command was introduced.
Release 4.3.1	The command output was extended for the throttle for **circuit-id**, **remote-id**, **inner-vlan**, **outer-vlan**, **vlan** and **circuit-id-and-remote-id**.

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.

Task ID

Task ID	Operation
ppp	read

Examples

This is the sample output of the **show pppoe throttles** command:

```
RP/0/RSP0/CPU0:router# show pppoe throttles location 0/2/cpu0

BBA-Group TEST
--------------
MAC throttle information:
Max packets per request period: 5
Request period duration: 20s
Blocking period duration: 5s
Time Since
MAC Address State left reset PADI PADR
----------- ----- ---- ----- ---- ----
aabb.ccdd.1123 Idle 30s 16s 0 0
7582.1352.e29a Monitor 3s 20s 5 5
7582.1352.e29a Block 4s 17s 6 5
MAC Access-interface throttle information:
Max packets per request period: 5
Request period duration: 20s
Blocking period duration: 5s
Time Since
Access-Int MAC Address State left reset PADI PADR
---------- ----------- ----- ---- ----- ---- ----
GE0/1/0/0 aabb.ccdd.1123 Idle 30s 16s 0 0
GE0/1/0/0 7582.1352.e29a Monitor 3s 20s 5 5
GE0/1/0/0 7582.1352.e29a Block 4s 17s 6 5
MAC IWF throttle information:
Max packets per request period: 5
Request period duration: 20s
Blocking period duration: 5s
Time Since
MAC Address State left reset PADI PADR
----------- ----- ---- ----- ---- ----
aabb.ccdd.1123 Idle 30s 16s 0 0
7582.1352.e29a Mon 3s 20s 5 5
7582.1352.e29a Block 4s 17s 6 5
BBA-Group TEST2
--------------
MAC throttling is not configured.
MAC Access-interface throttling is not configured.
MAC IWF throttling is not configured.
```

Another sample output of the **show pppoe throttles** command:

```
RP/0/RSP0/CPU0:router# show pppoe throttles
BBA-Group BNG_BBA1
------------------
MAC throttles not configured.

MAC-Access-interface throttles not configured.

MAC-IWF-Access-interface throttles not configured.
```

```
Circuit-ID throttle information:
  Max packets per request period: 10
  Request period duration:        10s
  Blocking period duration:       100s

                                                    Time  Since
  Circuit-ID                                State   left  reset  PADI  PADR
  ----------                                -----   ----  -----  ----  ----
  circuit0                                  Block    91s     8s    10    10

Remote-ID throttle information:
  Max packets per request period: 10
  Request period duration:        10s
  Blocking period duration:       100s

                                                    Time  Since
  Remote-ID                                 State   left  reset  PADI  PADR
  ----------                                -----   ----  -----  ----  ----
  remote10                                  Block    91s     8s    10    10

Inner-VLAN-ID throttle information:
  Max packets per request period: 10
  Request period duration:        10s
  Blocking period duration:       100s

                                                    Time  Since
  Access-Int                Inner VLAN ID   State   left  reset  PADI  PADR
  ----------                -------------   -----   ----  -----  ----  ----
  BE2.10                    10              Block    91s     8s    10    10

Outer-VLAN-ID throttle information:
  Max packets per request period: 10
  Request period duration:        10s
  Blocking period duration:       100s

                                                    Time  Since
  Access-Int                Outer VLAN ID   State   left  reset  PADI  PADR
  ----------                -------------   -----   ----  -----  ----  ----
  BE2.10                    10              Block    91s     8s    10    10

VLAN-ID throttle information:
  Max packets per request period: 10
  Request period duration:        10s
  Blocking period duration:       100s

                                                    Time  Since
  Access-Int           Outer, Inner VLAN ID   State   left  reset  PADI  PADR
  ----------           --------------------   -----   ----  -----  ----  ----
  BE2.10                  10, 10              Block    91s     8s    10    10

Circuit-ID-and-Remote-ID throttle information:
  Max packets per request period: 0
  Request period duration:        0s
  Blocking period duration:       0s

                                                    Time  Since
  Circuit-ID                                State   left  reset  PADI  PADR
    Remote-ID
  -----------                               -----   ----  -----  ----  ----
  circuit0                                  Block    91s     8s    10    10
    remote10
```

This table describes the significant fields displayed in the **show pppoe throttles** command output :

Field	Description
Block	Specifies that the throttle is active and that packets are dropped.
Idle	Specifies that the packets relevant to the throttle are not yet received.

Field	Description
Monitor	Specifies that the packets are counted, but the throttle is not yet active.
Time left	Specifies the time remaining until the throttle enters idle state, or if the throttle is already in idle state, the time until the throttle entry is removed.
Since reset	Specifies the time since the throttle counters were last reset. Throttle counters are reset upon entering the idle state.
PADI	Specifies the number of PADI messages received which match the entry criteria (say, mac address).
PADR	Specifies the number of PADR messages received which match the entry criteria (say, mac address).

Related Commands

Command	Description
pppoe sessions throttle, on page 442	Configures a throttle value for PPPoE sessions for a PPPoE BBA-Group in BNG.
show pppoe limits, on page 448	Shows the PPPoE session limit information.
show pppoe interfaces, on page 446	Shows a summary of the protocol state for the specified PPPoE interface filtered by circuit-id, remote-id, interface, or location.
show pppoe statistics, on page 452	Shows the counters for packets received and sent by the PPPoE sessions.
show pppoe summary, on page 455	Shows summary information of the PPPoE sessions.

QOS Commands

This module describes the Cisco IOS XR software commands used to configure the QoS commands for Broadband Network Gateway (BNG) on the Cisco ASR 9000 Series Router. For details regarding the related configurations, refer to the *Cisco ASR 9000 Series Aggregation Services Router Broadband Network Gateway Configuration Guide*.

- qos account, page 462
- qos output minimum-bandwidth, page 464
- service-policy (QoS-BNG), page 466
- service-policy (interface-BNG), page 468
- show qos inconsistency (BNG), page 470
- show qos interface (BNG), page 473
- show qos shared-policy-instance (BNG), page 478
- show qos summary (BNG), page 481

qos account

To enable QoS Layer 2 overhead accounting, use the **qos account** command in dynamic template configuration mode. To disable this qos account, use the **no** form of this command.

qos account[**AAL5**|**user-defined** *offset* **atm**] [**mux-1483 routed**|**mux-dot1q-rbe**|**mux-pppoa**|**mux-rbe**|**snap-1483routed**|**snap-dot1q-rbe**|**snap-pppoa**|**snap-rbe**]

no qos account

Syntax Description

AAL5	Specifies AAL5 for qos.
user-defined	Specifies the user-defined keyword.
offset	Specifies the user-defined offset size.
atm	Adds ATM cell tax to the L2 overhead.
mux-1483 routed	Specifies the mux-1483 routed.
mux-dot1q-rbe	Specifies the mux-dot1q-rbe.
mux-pppoa	Specifies the mux-pppoa.
mux-rbe	Specifies the mux-rbe.
snap-1483routed	Specifies the snap-1483routed.
snap-dot1q-rbe	Specifies the snap-dot1q-rbe.
snap-pppoa	Specifies the snap-pppoa
snap-rbe	Specifies the snap-rbe.

Command Default

None

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 4.2.0	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.

This command is available only in the dynamic template type ppp submode.

Task ID

Task ID	Operation
qos	read, write

Examples

This is an example of configuring the **qos account** command in dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# qos account AAL5 snap-rbe
```

Related Commands

Command	Description
qos output minimum-bandwidth, on page 464	Sets the minimum guaranteed output bandwidth for a subscriber.

qos output minimum-bandwidth

To set the minimum guaranteed output bandwidth for a subscriber, use the **qos output minimum-bandwidth** command in dynamic template configuration mode.

qos output minimum-bandwidth *range*

Syntax Description

range	Specifies the minimum bandwidth range (1- 4294967295 kpbs).

Command Default

None

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 4.2.0	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..

This command is available only in the dynamic template type ppp submode. The value specified in this command is used only if IGMP HQoS correlation is configured. This is to ensure that the resultant bandwidth does not go below the specified value.

Task ID

Task ID	Operation
vrrp	read, write

Examples

This is an example of configuring the **qos output minimum-bandwidth** command in dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# qos output minimum-bandwidth 10
```

Related Commands

Command	Description
qos account, on page 462	Enables QoS Layer 2 overhead accounting.

service-policy (QoS-BNG)

To enable the QoS policy on a parent S-VLAN, or to enable ingress and egress VLAN policies on an access-interface, use the **service-policy** command in the interface configuration mode. To disable this feature, use the **no** form of this command.

Egress S-VLAN Policy:

service-policy output *service_policy_name* **subscriber-parent** [**resource-id** *value*]

no service-policy output *service_policy_name* **subscriber-parent** [**resource-id** *value*]

Ingress and Egress VLAN Policies:

service-policy {**input | output**} *service_policy_name*

no service-policy {**input | output**} *service_policy_name*

Syntax Description

input	Attaches the specified service-policy to the ingress direction.
output	Attaches the specified service-policy to the egress direction.
service_policy_name	Name of the input or output service-policy.
subscriber-parent	Configures an S-VLAN policy. **Note** This keyword applies only to the egress direction.
resource-id	Specifies a resource ID that allows to map the desired chunk to be used for this S-VLAN and all the subscribers under it. **Note** This keyword applies only to an S-VLAN policy and not to VLAN policy.
value	The resource ID value that ranges from 0-3.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Release	Modification
Release 4.3.0	Support for the **resource-id** keyword was added.
Release 4.3.1	Support for the ingress and egress VLAN policies on an access interface was added.

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.

If the **resource-id** option is not specified, then the S-VLAN policy and all the subscribers under it are assigned to the default chunk, which its parent interface is associated with.

The VLAN policy needs to be attached to the access interfaces, before bringing up the sessions with the QoS policy. It is recommended that you do not remove VLAN policies when sessions are already active.

You cannot make non-rate modifications when sessions are already active on the access-interface. To make non-rate modifications to the VLAN policy, you must bring down the sessions that are brought up over the access-interface, modify the policy, and then bring up the sessions again over the access-interface.

Task ID

Task ID	Operation
qos	read, write

Examples

This example shows how to configure an egress S-VLAN policy using the **service-policy** command, with **subscriber-parent** keyword, in the interface configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface bundle-ether 18.12
RP/0/RSP0/CPU0:router(config-subif)# service-policy output svlan-policy subscriber-parent
resource-id 1
```

This example shows how to configure an ingress VLAN policy on an access-interface:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface bundle-ether 18.203
RP/0/RSP0/CPU0:router(config-subif)# service-policy input mark
```

This example shows how to configure an egress VLAN policy on an access-interface:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface bundle-ether 18.203
RP/0/RSP0/CPU0:router(config-subif)# service-policy output metering
```

service-policy (interface-BNG)

To attach a policy map to an input interface or output interface to be used as the service policy for that interface, and optionally multiple subinterfaces, use the **service-policy** command in the appropriate configuration mode. To remove a service policy from an input or output interface, use the **no** form of the command.

service-policy {**input**| **output**} *policy-map* [**shared-policy-instance** *instance-name*]

no service-policy {**input**| **output**} *policy-map* [**shared-policy-instance** *instance-name*]

Syntax Description

input	Attaches the specified policy map to the input interface.
output	Attaches the specified policy map to the output interface.
policy-map	Name of a service policy map (created using the **policy-map** command) to be attached.
shared-policy-instance	(Optional) Allows sharing of QoS resources across multiple subinterfaces. **Note** Sharing across multiple physical interfaces is not supported.
instance-name	(Optional) String of up to 32 characters to identify the shared policy instance.

Command Default

No service policy is specified.

Command Modes

Dynamic template configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 3.9.0	This command was updated to support shared policy instance over bundle interfaces.
Release 3.6.0	The command was supported in Layer 2 transport configuration mode.
Release 4.3.0	The command was supported in dynamic template configuration mode in BNG.

Usage Guidelines

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

You can attach a single policy map to one or more interfaces to specify the service policy for those interfaces. The class policies composing the policy map are then applied to packets that satisfy the class map match criteria for the class. To apply a new policy to an interface, you must remove the previous policy. A new policy cannot replace an existing policy.

To enter the dynamic template configuration mode, run **dynamic-template** command in the global configuration mode.

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows policy map policy 1 applied in the dynamic template configuration mode.

```
RP/0/RSP0/CPU0:router(config)#dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)#service-policy policy1
shared-policy-instance subscriber1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)#exit

RP/0/RSP0/CPU0:router(config)# dynamic-template type ipsubscriber ipsub1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# service-policy output policy1
shared-policy-instance subscriber1
```

show qos inconsistency (BNG)

To display inconsistency information for the QoS policy on an interface, use the **show qos inconsistency** command in EXEC mode.

show qos inconsistency {**detail** *warning-type* {**file** *filename*| **location** *node-id*}| **summary** {**file** *filename*| **location** *node-id*}}

Syntax Description

detail	Displays interface and policy name details of the inconsistency.
warning-type	Selects the warning types to display: • 0—All warning types • 1—ANCP - No shaper at top policy map • 2—ANCP - Multiple classes at top policy map • 3—ANCP - Downstream rate less than shaper rate • 4—ANCP - Downstream rate more than port speed • 5—ANCP - Policy resolution failure • 6—ANCP - Traffic manager program failure • 7—Port speed - Policy resolution failure • 8—Port speed - Traffic manager program failure • 9—Bundle member addition failure • 10—Interface state not matching system configuration
file *filename*	Specify a file name, such as disk0:tmp.log or bootflash:.
location *node-id*	Displays detailed QoS information for the designated node. The *node-id* argument is entered in the rack/slot/module notation.
summary	Displays summary counts of QoS inconsistency warnings.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Release	Modification
Release 4.3.0	The command was supported in dynamic template configuration mode in BNG.

Usage Guidelines

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

To enter the dynamic template configuration mode, run **dynamic-template** command in the global configuration mode.

Task ID

Task ID	Operations
qos	read

Examples

This example provides detail about QoS policy inconsistency, for all warning types:

```
RP/0/RSP0/CPU0:router# show qos inconsistency detail 0 location 0/7/CPU0

Interface Lists with QoS Inconsistency Warning:
===============================================================

                     Node 0/7/CPU0
---------------------------------------------------------------

Interfaces with QoS Inconsistency:  ANCP - No Shaper at top policymap
=========================================================================
Interface                  Direction  Policy Name             SPI Name
-------------------------------------------------------------------------
GigabitEthernet0/7/0/1.5     output    parent-none

Interfaces with QoS Inconsistency:  ANCP - Downstream Rate less than Shaper Rate
=========================================================================
Interface                  Direction  Policy Name             SPI Name
-------------------------------------------------------------------------
GigabitEthernet0/7/0/1       output    parent                   SPI1
GigabitEthernet0/7/0/1.2     output    parent
GigabitEthernet0/7/0/1       output    normal-policy-name      normal-spi-name
```

This example displays summary counts of inconsistency warnings:

```
RP/0/RSP0/CPU0:router#
RP/0/RSP0/CPU0:router# show qos inconsistency summary location 0/7/CPU0

Summary Counts of QoS Inconsistency Warnings:
===============================================================


                     Node 0/7/CPU0

   Inconsistency Warning Type                 Count
-------------------------------------------------------
ANCP - No Shaper at top policymap:               1
ANCP - Downstream Rate less than Shaper Rate:    4
```

Related Commands

Command	Description
show qos interface (BNG), on page 473	Displays QoS information for a specific interface.

show qos interface (BNG)

To display QoS information for a specific interface, use the **show qos interface** command in the EXEC mode.

show qos interface *type interface-path-id* {**input| output**} [**host-link** *interface-path-id*| **location** *node-id*]

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 RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/ RSP0 RP1 /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.
input	Attaches the specified policy map to the input interface.
output	Attaches the specified policy map to the output interface.
host-link	Specifies the host-link.

location *node-id*	(Optional) Displays detailed QoS 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

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.3.0	The command was supported in dynamic template configuration mode in BNG.

Usage Guidelines

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

The **show qos interface** command displays configuration for all classes in the service policy that is attached to an interface.

Use this command to check the actual values programmed in the hardware from the action keywords in the **police rate** command.

To enter the dynamic template configuration mode, run **dynamic-template** command in the global configuration mode.

Task ID

Task ID	Operations
qos	read

Examples

This is the sample output shows the QoS information on a GigabitEthernet interface:

```
show qos interface gig0/0/0/11.1 output

Wed Mar 18 18:25:20.140 UTC
Interface: GigabitEthernet0_0_0_11.1 output Bandwidth: 1000000 kbps ANCP: 999936 kbps
Policy: parent-3play-subscriber-line Total number of classes: 5
------------------------------------------------------------------------
Level: 0 Policy: parent-3play-subscriber-line Class: class-default
QueueID: N/A
Shape Profile: 1 CIR: 200000 kbps (200 mbps)
CBS: 100352 bytes PIR: 999936 kbps PBS: 12517376 bytes
WFQ Profile: 1 Committed Weight: 51 Excess Weight: 100
Bandwidth: 200000 kbps, BW sum for Level 0: 1000000 kbps, Excess Ratio: 100
```

```
------------------------------------------------------------------------
Level: 1 Policy: child-3play Class: 3play-voip
Parent Policy: parent-3play-subscriber-line Class: class-default
QueueID: 136 (Priority 1)
Queue Limit: 16 kbytes Profile: 3 Scale Profile: 0
Policer Profile: 0 (Single)
Conform: 65 kbps (65 kbps) Burst: 1598 bytes (0 Default)
Child Policer Conform: TX
Child Policer Exceed: DROP
Child Policer Violate: DROP
------------------------------------------------------------------------
Level: 1 Policy: child-3play Class: 3play-video
Parent Policy: parent-3play-subscriber-line Class: class-default
QueueID: 137 (Priority 2)
Queue Limit: 8 kbytes (11 Unknown) Profile: 4 Scale Profile: 0
Policer Profile: 24 (Single)
Conform: 128 kbps (128 kbps) Burst: 1598 bytes (0 Default)
Child Policer Conform: TX
Child Policer Exceed: DROP
Child Policer Violate: DROP
WRED Type: COS based Table: 0 Profile: 4 Scale Profile: 0 Curves: 3
Default RED Curve Thresholds Min : 8 kbytes Max: 8 kbytes
WRED Curve: 1 Thresholds Min : 8 kbytes Max: 8 kbytes
 Match: 3
WRED Curve: 2 Thresholds Min : 8 kbytes Max: 8 kbytes
 Match: 4
------------------------------------------------------------------------
Level: 1 Policy: child-3play Class: 3play-premium
Parent Policy: parent-3play-subscriber-line Class: class-default
QueueID: 138 (Priority Normal)
Queue Limit: 2097 kbytes Profile: 2 Scale Profile: 0
WFQ Profile: 6 Committed Weight: 1020 Excess Weight: 1020
Bandwidth: 200000 kbps, BW sum for Level 1: 200000 kbps, Excess Ratio: 1
------------------------------------------------------------------------
Level: 1 Policy: child-3play Class: class-default
Parent Policy: parent-3play-subscriber-line Class: class-default
QueueID: 139 (Priority Normal)
Queue Limit: 65 kbytes Profile: 1 Scale Profile: 3
WFQ Profile: 0 Committed Weight: 1 Excess Weight: 1020
Bandwidth: 0 kbps, BW sum for Level 1: 200000 kbps, Excess Ratio: 1
------------------------------------------------------------------------
```

Use the **host-link** option to display the output for the desired Bundle ICL. In cases when the Satellite is hosted on a redundant (Bundle ICL), the qos command to check for the qos programming also needs to include the host-link option.

The host-link is the underlying ICL Bundle member, this output can be executed for all the members belonging to the ICL Bundle via the host-link option.

For eg, Bundle ICL, Bundle-ether 2, hosting the sat-ether interface gig 100/0/0/34 has a member tengige 0/3/0/7. The qos command to check for the qos programming would be:

```
RP/0/RSP0/CPU0:router # sh qos inter gigabitEthernet 100/0/0/34 output host-link tenGigE
0/3/0/7 location 0/3/CPU0

Interface: GigabitEthernet100_0_0_34 output
Bandwidth configured: 500000 kbps Bandwidth programed: 500000 kbps
ANCP user configured: 0 kbps ANCP programed in HW: 0 kbps
Port Shaper programed in HW: 500000 kbps
Policy: grand Total number of classes: 10
------------------------------------------------------------------------
Level: 0 Policy: grand Class: class-default
QueueID: N/A
Shape CIR : ALL
Shape PIR Profile : 2/4(S) Scale: 488 PIR: 499712 kbps  PBS: 6246400 bytes
WFQ Profile: 2/9 Committed Weight: 10 Excess Weight: 10
Bandwidth: 0 kbps, BW sum for Level 0: 0 kbps, Excess Ratio: 1
------------------------------------------------------------------------
Level: 1 Policy: parent Class: class-default
Parent Policy: grand Class: class-default
```

```
QueueID: N/A
Shape CIR : NONE
Shape PIR Profile : 2/4(S) Scale: 244 PIR: 249856 kbps  PBS: 3123200 bytes
WFQ Profile: 2/9 Committed Weight: 10 Excess Weight: 10
Bandwidth: 0 kbps, BW sum for Level 1: 0 kbps, Excess Ratio: 1
------------------------------------------------------------------------
Level: 2 Policy: child Class: prec1
Parent Policy: parent Class: class-default
QueueID: 131264 (Priority 1)
Queue Limit: 2496 kbytes Abs-Index: 89 Template: 0 Curve: 6
Shape CIR Profile: INVALID
Policer Profile: 54 (Single)
Conform: 50000 kbps (20 percent) Burst: 625000 bytes (0 Default)
Child Policer Conform: set dscp 46  set cos 7
Child Policer Exceed: DROP
Child Policer Violate: DROP
------------------------------------------------------------------------
Level: 2 Policy: child Class: prec2
Parent Policy: parent Class: class-default
QueueID: 131265 (Priority 2)
Queue Limit: 624 kbytes (100 ms) Abs-Index: 59 Template: 0 Curve: 6
Shape CIR Profile: INVALID
Shape PIR Profile : 2/0(E) PIR: 50000 kbps PBS: 624992 bytes
Child Mark: set dscp 46  set cos 7
------------------------------------------------------------------------
Level: 2 Policy: child Class: prec3
Parent Policy: parent Class: class-default
QueueID: 131267 (Priority 3)
Queue Limit: 472 kbytes (100 ms) Abs-Index: 53 Template: 0 Curve: 6
Shape CIR Profile: INVALID
Shape PIR Profile : 2/1(E) PIR: 37496 kbps PBS: 468736 bytes
Child Mark: set dscp 46  set cos 7
------------------------------------------------------------------------
Level: 2 Policy: child Class: prec4
Parent Policy: parent Class: class-default
QueueID: 131266 (Priority Normal)
Queue Limit: 60 kbytes Abs-Index: 18 Template: 0 Curve: 0
Shape CIR Profile: INVALID
Child Mark: set dscp 46  set cos 7
WFQ Profile: 2/39 Committed Weight: 40 Excess Weight: 40
Bandwidth: 0 kbps, BW sum for Level 2: 0 kbps, Excess Ratio: 4
------------------------------------------------------------------------
Level: 2 Policy: child Class: prec5
Parent Policy: parent Class: class-default
QueueID: 131268 (Priority Normal)
Queue Limit: 44 kbytes Abs-Index: 15 Template: 0 Curve: 0
Shape CIR Profile: INVALID
WFQ Profile: 2/29 Committed Weight: 30 Excess Weight: 30
Bandwidth: 0 kbps, BW sum for Level 2: 0 kbps, Excess Ratio: 3
------------------------------------------------------------------------
Level: 2 Policy: child Class: prec6
Parent Policy: parent Class: class-default
QueueID: 131269 (Priority Normal)
Queue Limit: 28 kbytes Abs-Index: 11 Template: 0 Curve: 0
Shape CIR Profile: INVALID
WFQ Profile: 2/19 Committed Weight: 20 Excess Weight: 20
Bandwidth: 0 kbps, BW sum for Level 2: 0 kbps, Excess Ratio: 2
------------------------------------------------------------------------
Level: 2 Policy: child Class: prec7
Parent Policy: parent Class: class-default
QueueID: 131270 (Priority Normal)
Queue Limit: 16 kbytes Abs-Index: 8 Template: 0 Curve: 0
Shape CIR Profile: INVALID
Child Mark: set cos 5
WFQ Profile: 2/9 Committed Weight: 10 Excess Weight: 10
Bandwidth: 0 kbps, BW sum for Level 2: 0 kbps, Excess Ratio: 1
------------------------------------------------------------------------
Level: 2 Policy: child Class: class-default
Parent Policy: parent Class: class-default
QueueID: 131271 (Priority Normal)
Queue Limit: 16 kbytes Abs-Index: 8 Template: 0 Curve: 0
Shape CIR Profile: INVALID
```

```
WFQ Profile: 2/9 Committed Weight: 10 Excess Weight: 10
Bandwidth: 0 kbps, BW sum for Level 2: 0 kbps, Excess Ratio: 1
```

show qos shared-policy-instance (BNG)

To list interface details for a specific location of a specific shared policy instance, attached to either an input or output interface, use the **show qos shared-policy-instance** command in EXEC mode.

show qos shared-policy-instance *instance-name* {**input**| **output**} **location** *node-id*

Syntax Description

instance-name	String of up to 32 characters to identify the shared policy instance.
input	Displays details for the shared policy instance attached to the input interface.
output	Displays details for the shared policy instance attached to the output interface
location *node-id*	Location of node. The node-id argument is entered in *rack/slot/module* notation.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 3.9.0	This command was updated to support shared policy instance over bundle interfaces.
Release 4.3.0	The command was supported in BNG.

Usage Guidelines

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

To enter the dynamic template configuration mode, run **dynamic-template** command in the global configuration mode.

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows the results of the command to show details of the shared policy instance attached to the input interface at location 0/RSP0/CPU0:

```
RP/0/RSP0/CPU0:router# show qos shared-policy-instance instancetwo input location 0/RSP0/CPU0

shared-policy-instance: instancetwo input Bandwidth: 10000000 kbps
Policy: shape Total number of classes: 2
------------------------------------------------------------------------
Level: 0 Policy: shape Class: class-default
QueueID: N/A
Shape Profile: 1 CIR: 16 kbps CBS: 1024 bytes PIR: 128000 kbps PBS:1605632
bytes WFQ Profile: 1 Committed Weight: 1 Excess Weight: 1
Bandwidth: 0 kbps, Parent Bandwidth: 10000000 kbps, Excess Ratio: 1
------------------------------------------------------------------------
Level: 1 Policy: child Class: class-default Parent Policy: shape Class: class-default
QueueID: 268435466 (Priority Normal)
Queue Limit: 1572 kbytes Profile: 1 Scale Profile: 14 WFQ Profile: 2
Committed Weight: 10 Excess Weight: 1020
Bandwidth: 0 kbps, Parent Bandwidth: 0kbps, Excess Ratio: 1
------------------------------------------------------------------------

RP/0/RSP0/CPU0:router# show qos shared-policy-instance spi1 input location 0/1/cPU0

Instancespi1  --   Direction: input
Policy                   hier_l2_ingress
Total number of classes:   5
-----------------------------------------------
MPLS vmrid               160
IPV4 vmrid               159
IPV6 vmrid               158
    LEVEL1 class: classid    =  0x1
    class name               =   class-default
    Policer average                 = 600 mbits/sec (600000 kbps)
    Policer conform burst           = dflt (16777215 bytes)
    Policer conform action          = Just TX
    Policer exceed  action          = DROP PKT

      LEVEL2 class: classid    =  0x2
      class name               =   cos3
      Policer average                 = 100 mbits/sec (100032 kbps)
      Policer conform burst           = dflt (3126000 bytes)
      Policer conform action          = SET EXP AND TX
      Policer conform action value    = 1
      Policer exceed  action          = SET EXP AND TX
      Policer exceed  action value    = 2

      LEVEL2 class: classid    =  0x3
      class name               =   cos4
      Policer average                 = 100 mbits/sec (100032 kbps)
      Policer conform burst           = dflt (3126000 bytes)
      Policer conform action          = SET EXP AND TX
      Policer conform action value    = 3
      Policer exceed  action          = SET EXP AND TX
      Policer exceed  action value    = 4

      LEVEL2 class: classid    =  0x4
      class name               =   cos5
      Policer average                 = 100 mbits/sec (100032 kbps)
      Policer conform burst           = dflt (3126000 bytes)
      Policer conform action          = SET EXP AND TX
      Policer conform action value    = 5
      Policer exceed  action          = SET EXP AND TX
      Policer exceed  action value    = 6

      LEVEL2 class: classid    =  0x5
      class name               =   class-default
RP/0/RSP0/CPU0:router# show qos shared-policy-instance spi1 output location 0/1/cPU0

Instancespi1  --   Direction: output
```

```
Policy                   12_egress
Total number of classes:   2
----------------------------------------------
MPLS vmrid               17
IPV4 vmrid               16
IPV6 vmrid               24
    LEVEL1 class: classid    =  0x1
    class name               =   qos_grp1
    queue ID                 =   18
    port ID                  =   2 (Bandwidth = 1000000, MTU = 1522)
    Queue Max. BW.           =   250 mbits/sec (250000 kbps)
    Queue Max. Burst         =   200 ms (4194304 bytes)
    Queue Limit              =   16384 packets (16384 pkts)

    LEVEL1 class: classid    =  0x2
    class name               =   class-default
    queue ID                 =   19
    port ID                  =   2 (Bandwidth = 1000000, MTU = 1522)
    Weight                   =   1 ( BW Remaining % = 0)
    Queue Limit              =   16384 packets (16384 pkts)
```

show qos summary (BNG)

To list the interfaces at a specific location, use the **show qos summary** command in EXEC mode.

show qos summary [**shared-policy-instance** *instance-name* **location** *rack/slot/module/interface.subinterface*| **police** [**interface** *type instance*| **location** [*rack/slot/module/interface.subinterface*| *location-name*]]| **policy** *policy-name* [**interface** *type instance*| **location** *node-location*]| **queue** [**interface** *type instance*| **location** *node-location*]]

Syntax Description

shared-policy-instance *instance-name*	String of up to 32 characters to identify the shared policy instance.
location *rack/slot/module/ interface.subinterface*	Location of node in format rack/slot/module/interface.subinterface.
police	Show policer interface statistics.
interface *type instance*	Interface type and number.
location *location-name*	String to identify the fully qualified location specification.
policy *policy-name*	String to identify the policy.
location *node-location*	Identifies fully qualified location specification.
queue	Show queue statistics.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.3.0	The command was supported in dynamic template configuration mode in BNG.

Usage Guidelines

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

To enter the dynamic template configuration mode, run **dynamic-template** command in the global configuration mode.

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows the results of the command to show interfaces at location 0/RSP0/CPU0 for a shared-policy-instance:

```
RP/0/RSP0/CPU0:router# show qos summary shared-policy-instance instancetwo location
0/RSP0/CPU0

list of interfaces retrieved
  TenGigE0/0/0.1
  TenGigE0/0/0.2
RP/0/RSP0/CPU0:router#
```

Subscriber Commands

This module describes the Cisco IOS XR software commands used to configure the subscriber commands for Broadband Network Gateway (BNG) on the Cisco ASR 9000 Series Router. For details regarding the related configurations, refer to the *Cisco ASR 9000 Series Aggregation Services Router Broadband Network Gateway Configuration Guide*.

- subscriber session limit, page 484
- show subscriber database, page 486
- show subscriber feature accounting, page 491
- show subscriber manager sadb, page 493
- show subscriber manager statistics, page 495
- show subscriber running-config, page 498
- show subscriber session, page 500
- clear subscriber session, page 504

subscriber session limit

To configure a limit for subscriber sessions, use the **subscriber session limit** command in global configuration mode. To remove the session limit for subscribers, use the **no** form of this command.

subscriber session limit *session_limit*

no subscriber session limit *session_limit*

Syntax Description

session_limit	Limit for subscriber sessions. The range is from 1 to 200000.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 5.1.1	This command was introduced.

Usage Guidelines

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

This command does not limit the number of un-authenticated sessions on the router, until the overall session count reaches *session_limit*. If a new session comes up after router reached the *session_limit*, then the long-lived un-authenticated subscriber session is deleted. The new session can be an authenticated or un-authenticated session.

Task ID

Task ID	Operation
config-services	read, write

Examples

This example shows how to configure a limit for subscriber sessions:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# subscriber session limit 100000
```

Related Commands

Command	Description
show subscriber session, on page 500	Displays the subscriber management session information.

show subscriber database

To display the configuration details of subscriber database, use the **show subscriber database** command in the EXEC mode.

show subscriber database {**association** |**configuration** |**connection** |**interface** |**statistics summary** }

Syntax Description

association	Displays the association between subscriber sessions and dynamic templates.
configuration	Displays the configuration database information.
connection	Displays subscriber client connection identifiers.
interface	Displays the mapping between subscriber labels and interface handles.
statistics	Displays the show subscriber database statistics information.
summary	Displays the show subscriber database summary counts.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	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.

Task ID

Task ID	Operation
network	read

Examples

The sample output of the **show subscriber database** command is:

```
RP/0/RSP0/CPU0:router# show subscriber database association

Mon Jun 14 16:24:50.432 EDT
Object Name: TEMPL1
  Object Type: IP-SUBSCRIBER-TEMPLATE
  Feature Name: IPV4
    Attribute Name: ipv4/unnumbered
                    reference count : 1
                    sysDb pathname  :
/cfg/gl/dynamic-templates/ipsubscriber/TEMPL1/ipv4/unnumbered
                    datatype        : string
                    length          : 10
                    value           : Loopback0

Object Name: TEMPL2
  Object Type: IP-SUBSCRIBER-TEMPLATE
  Feature Name: IPV4
    Attribute Name: ipv4/mtu
                    reference count : 1
                    sysDb pathname  : /cfg/gl/dynamic-templates/ipsubscriber/ss/ipv4/mtu
                    datatype        : uint32
                    length          : 4
                    value           : 1500
  Feature Name: QoS
    Attribute Name: qos/service_policy_in/qos_policy
                    reference count : 1
                    sysDb pathname  :
/cfg/gl/dynamic-templates/ipsubscriber/ss/qos/service_policy_in/:qos_policy
                    datatype        : packed
                    length          : 20
                    value           : packed
                                          AB CD 43 21 02 00 04 00
  00 00 00 03 00 00 03 00
                                        00 06 00 00
  Feature Name: 'RSI'
    Attribute Name: rsi/vrf
                    reference count : 1
                    sysDb pathname  : /cfg/gl/dynamic-templates/ipsubscriber/ss/rsi/vrf
                    datatype        : 3
                    length          : 5
                    value           : blue

RP/0/RSP0/CPU0:router# show subscriber database connection

Tue Jun 15 11:00:19.650 EDT

Client Connection Identifier:  0x0
=====================================
    ref_count        = 3
    req_count        = 0
    bpi_reg_count    = 0
    spi_reconciled   = TRUE
    bpi_reconciled   = FALSE
    client_restarted = FALSE
    client_name      = template-mgr
    timer_running    = FALSE

    spi_cb_info:  N/A


    Persistent Information:
        in_use                  = TRUE
        forced_full_resync      = FALSE
        client_flags            = TMPL_PROD
        state                   = SUBDB_CLIENT_FULL
        instance_no             = 0
        num_bpi_regs            = 0
```

```
    num_send_drop_bpi_msg     = 0
    num_send_drop_spi_msg     = 0
    num_recv_drop_bpi_msg     = 0
    num_recv_drop_spi_msg     = 0
    num_sent_bpi_msg          = 0
    num_sent_spi_msg          = 0
    num_recv_bpi_msg          = 0
    num_recv_spi_msg          = 0
    num_sent_pulse            = 0

SPI AIPC Information:
    conn_present              = 0
    tx_attempt_count          = 0
    tx_count                  = 0
    rx_count                  = 0
    notify_connect_count      = 0
    notify_queue_high_count   = 0
    notify_queue_low_count    = 0
    notify_queue_full_count   = 0
    notify_data_waiting_count = 0
    notify_error_count        = 0
    notify_close_count        = 0
    notify_sendstatus_count   = 0
    notify_open_count         = 0
    pulse_data_waiting_count  = 0
    queue_full                = 0
    queue_full_drop           = 0
   outstanding_buffers       = 0
    overflow_queue_size       = 0
    cumulative_overflow_msgs  = 0
    hwm_overflow_msgs         = 0
BPI AIPC Information:
    conn_present              = 1
    tx_attempt_count          = 0
    tx_count                  = 0
    rx_count                  = 1
    notify_connect_count      = 0
    notify_queue_high_count   = 0
    notify_queue_low_count    = 0
    notify_data_waiting_count = 1
    notify_error_count        = 0
    notify_close_count        = 0
    notify_sendstatus_count   = 0
    notify_open_count         = 1
    queue_full                = 0
    queue_full_drop           = 0
    outstanding_buffers       = 0
    overflow_queue_size       = 0
    cumulative_overflow_msgs  = 0
    hwm_overflow_msgs         = 0
Feature Information (number of entries = 3):
-------------------------------------------------
 ***Feature Name***     = RSI
    Connection ID       = 0x1
    Session type        = SUBDB_SESSION_LABEL_TYPE_IP_SUB_INBAND
    Activate Required   = FALSE
    Config Set ID       = 1
    Registration Handle = 0x1
    whichevent[0]       = SUBDB_CB_EVENT_NONE
    whichevent[1]       = SUBDB_CB_EVENT_ALL
    Feature State       = SUBDB_FEATURE_REGISTERED

 ***Feature Name***     = RSI
    Connection ID       = 0x1
    Session type        = SUBDB_SESSION_LABEL_TYPE_PPPOE_SUB
    Activate Required   = FALSE
    Config Set ID       = 1
    Registration Handle = 0x2
    whichevent[0]       = SUBDB_CB_EVENT_NONE
    whichevent[1]       = SUBDB_CB_EVENT_ALL
    Feature State       = SUBDB_FEATURE_REGISTERED

 ***Feature Name***     = RSI
```

```
        Connection ID       = 0x1
        Session type        = SUBDB_SESSION_LABEL_TYPE_IP_SUB_DHCP
        Activate Required   = FALSE
        Config Set ID       = 1
        Registration Handle = 0x3
        whichevent[0]       = SUBDB_CB_EVENT_NONE
        whichevent[1]       = SUBDB_CB_EVENT_ALL
        Feature State       = SUBDB_FEATURE_REGISTERED

Client Connection Identifier:  0x2
====================================
    ref_count        = 2
    req_count        = 0
    bpi_reg_count    = 0
    spi_reconciled   = TRUE
    bpi_reconciled   = TRUE
    client_restarted = FALSE
    client_name      = iedge SVM
    timer_running    = FALSE

    spi_cb_info:
        SUBDB_SPI_CB_PROD_ALL_DONE          = SUBDB_CB_EVENT_NONE
        SUBDB_SPI_CB_SESSION_PROD_DONE      = SUBDB_CB_EVENT_ALL
        SUBDB_SPI_CB_SESSION_ACTIVATED      = SUBDB_CB_EVENT_NONE
        SUBDB_SPI_CB_SESSION_CREATED        = SUBDB_CB_EVENT_NONE
        SUBDB_SPI_CB_SESSION_DESTROYED      = SUBDB_CB_EVENT_NONE
        SUBDB_SPI_CB_SESSION_ASSOCIATED     = SUBDB_CB_EVENT_ALL
        SUBDB_SPI_CB_SESSION_UNASSOCIATED   = SUBDB_CB_EVENT_ALL
        SUBDB_SPI_CB_SESSION_CONFIG_CHANGED = SUBDB_CB_EVENT_ALL
        SUBDB_SPI_CB_TEMPLATE_INSTALLED     = SUBDB_CB_EVENT_ALL
        SUBDB_SPI_CB_TEMPLATE_UNINSTALLED   = SUBDB_CB_EVENT_ALL
        SUBDB_SPI_CB_OBJECT_AGEOUT          = SUBDB_CB_EVENT_ALL


    Persistent Information:
        in_use                    = TRUE
        forced_full_resync        = FALSE
        client_flags              = TMPL_PROD, SESS_PROD
        state                     = SUBDB_CLIENT_FULL
        instance_no               = 1
        num_bpi_regs              = 0
        num_send_drop_bpi_msg     = 0
        num_send_drop_spi_msg     = 0
        num_recv_drop_bpi_msg     = 0
        num_recv_drop_spi_msg     = 0
        num_sent_bpi_msg          = 0
        num_sent_spi_msg          = 0
        num_recv_bpi_msg          = 0
        num_recv_spi_msg          = 1
        num_sent_pulse            = 0

    SPI AIPC Information:
        conn_present              = 1
        tx_attempt_count          = 0
        tx_count                  = 0
        rx_count                  = 2
        notify_connect_count      = 0
        notify_queue_high_count   = 0
        notify_queue_low_count    = 0
        notify_queue_full_count   = 0
        notify_data_waiting_count = 2
        notify_error_count        = 0
        notify_close_count        = 0
        notify_sendstatus_count   = 0
        notify_open_count         = 1
        pulse_data_waiting_count  = 0
        queue_full                = 0
        queue_full_drop           = 0
        outstanding_buffers       = 0
        overflow_queue_size       = 0
        cumulative_overflow_msgs  = 0
        hwm_overflow_msgs         = 0
    BPI AIPC Information:
```

```
        conn_present              = 0
        tx_attempt_count          = 0
        tx_count                  = 0
        rx_count                  = 0
        notify_connect_count      = 0
        notify_queue_high_count   = 0
        notify_queue_low_count    = 0
        notify_data_waiting_count = 0
        notify_error_count        = 0
        notify_close_count        = 0
        notify_sendstatus_count   = 0
        notify_open_count         = 0
        queue_full                = 0
        queue_full_drop           = 0
        outstanding_buffers       = 0
        overflow_queue_size       = 0
        cumulative_overflow_msgs  = 0
        hwm_overflow_msgs         = 0
    Feature Information (number of entries = 0):
    ------------------------------------------------
```

```
RP/0/RSP0/CPU0:router# show subscriber database interface
Tue Jun 15 09:05:53.769 EDT
Interface Ifhandle  Session ID:
Gi0/2/0/0.ip1 0x1000040  0x4000000
Gi0/2/0/0.ip2 0x1000060  0x4000082

RP/0/RSP0/CPU0:router# show subscriber database statistics

Tue Jun 15 09:05:53.769 EDT
3 wrapping entries (2048 possible, 0 filtered, 3 total)
Jun 15 06:49:40.123 subdb/common 0/0/CPU0 t4004322208 Process client ID '2' with connection
 event 'RESTARTED'
Jun 15 06:49:40.125 subdb/common 0/0/CPU0 t4153857728 Process SPI END RECONCILE msg for
client '2 [ring index '0']
Jun 15 06:49:40.125 subdb/common 0/0/CPU0 t4004322208 Process client ID '2' with connection
 event 'RECONCILED'
```

show subscriber feature accounting

To display the feature accounting information of the subscriber, use the **show subscriber feature accounting** command in the EXEC mode.

show subscriber feature accounting ma {**statistics debug** [**location** *location*]| **subscriber-label** *subscriber-id*| **summary** [**location** *location*]| **trace** {**all**| **error**| **event**}}

Syntax Description

ma	Displays the subscriber accounting feature management agent information.
statistics	Displays the accounting feature statistics.
debug	Displays the debug statistics.
location	Specifies the location of the node.
location	Fully qualified location name.
subscriber-label	Specifies the unique subscriber ID.
subscriber-id	ID of the subscriber, in hexadecimal.
summary	Displays the summary data.
trace	Displays the accounting feature ltrace data.
all	Displays trace of all errors and events.
error	Displays trace of errors.
event	Displays trace of events.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	This command was introduced.
Release 5.1	The show command output was extended to display session Idle Timeout feature information.

Usage Guidelines

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

Task ID

Task ID	Operation
network	read

Examples

This is the sample output of the **show subscriber feature accounting** command in the EXEC mode:

```
RP/0/RSP0/CPU0:router# show subscriber feature accounting ma subscriber-label 0x40
Subscriber Label: 0x40          Interface: Gi0/0/0/0.pppoe1

  Feature:  Session Accounting      Method-list: default

  Feature:  Session Idle Timeout
    Timeout value:          200 seconds
    Threshold value:        3 minutes per packet
    Timeout direction:      both
```

This table describes the significant fields displayed in the **show subscriber feature accounting** command output :

Field	Description
Timeout value	Specifies the timeout value configured for that particular subscriber session.
Threshold value	Specifies the threshold value configured for that particular subscriber session, to decide on the duration of the session inactivity.
Timeout direction: both	Specifies that both the ingress and egress traffic is considered for the determination of the idle time for that particular subscriber session.

Related Commands

Command	Description
show subscriber database, on page 486	Displays the configuration details of subscriber database.
show subscriber manager statistics, on page 495	Displays the subscriber management internal manager information.
show subscriber running-config, on page 498	Displays the subscriber running configuration derived from dynamic template.
show subscriber session, on page 500	Displays the subscriber management session information.

show subscriber manager sadb

To display the database information of the subscriber management feature attribute, use the **show subscriber manager sadb** command in the EXEC mode.

show subscriber manager sadb [**location** *location*]

Syntax Description

location	Specifies the location of the node.
location	Fully qualified location name.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
network	read

Examples

This is the sample output of the show subscriber manager sadb command:

```
RP/0/RSP0/CPU0:router#show subscriber manager sadb
Mon Apr  8 10:02:24.274 IST

Sublabel: 0x00000095 Node_ID: 00000000 Signature: 0xabcdef12 Version: 1 Rev: 9
Length: 168

Attribute list: 135469872
1:  outer-vlan-id   len=  4  10(a)
2:  port-type       len=  4  Virtual IP over VLAN
3:  static-session  len=  1  true
4:  parent-if-handle len=  4  1664(680)
5:  string-session-id len=  8  00000049
6:  interface       len=  8  0/0/1/10
```

```
7:  username        len=  6  BNG:10
8:  if-handle       len=  4  1664(680)
9:  vrf-id          len=  4  0(0)
10:  ipv4-session-state len=  1  true
```

Related Commands

Command	Description
show subscriber session, on page 500	Displays the subscriber management session information.
ipsubscriber interface, on page 260	Enables interface based static session in BNG.

show subscriber manager statistics

To display the subscriber management internal manager information, use the **show subscriber manager statistics** command in the EXEC mode.

show subscriber manager statistics {**AAA| HA| PPSM| PRE| SVM| debug| performance| summary**}

Syntax Description

AAA	Displays the Authentication, Authorization, Accounting Coordinator statistics.
HA	Displays the High Availability statistics.
PPSM	Displays the Policy Plane Session Manager statistics.
PRE	Displays the Policy Rule Engine statistics.
SVM	Displays the Service Manager statistics.
debug	Displays the debug statistics.
performance	Displays the performance statistics.
summary	Displays the summary statistics.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	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.

Task ID

Task ID	Operation
network	read

Examples This is the sample output of the **show subscriber manager statistics** command in the EXEC mode:

```
RP/0/RSP0/CPU0:router# show subscriber manager statistics summary total
```

The show subscriber manager statistics output is as follows:

```
Wed Jan 23 09:57:41.855 GMT

[ IEDGE SUMMARY STATISTICS ]

 Location: 0/0/CPU0

IEDGE SUMMARY
=============
Control Policy errors
  Subscriber control policy not applied on interface = 0
  No class match in Start Request                    = 0

Attribute format warnings
  NAS Port                                           = 0
  NAS Port id                                        = 0
  Destination station id                             = 0
  Calling station id                                 = 0
  User Name                                          = 0

User Profile Statistics
  User Profile Install                               = 0
  User Profile Install errors                        = 0
  User Profile Removes                               = 0
  User Profile Errors                                = 0

Session Disconnect Flow Control
  Inflight                                           = 0
  Queued                                             = 0

 Location: 0/1/CPU0

IEDGE SUMMARY
=============
Control Policy errors
  Subscriber control policy not applied on interface = 0
  No class match in Start Request                    = 0

Attribute format warnings
  NAS Port                                           = 72
  NAS Port id                                        = 0
  Destination station id                             = 72
  Calling station id                                 = 72
  User Name                                          = 0

User Profile Statistics
  User Profile Install                               = 0
  User Profile Install errors                        = 0
  User Profile Removes                               = 0
  User Profile Errors                                = 0

Session Disconnect Flow Control
  Inflight                                           = 0
  Queued                                             = 0
```

This table describes the significant fields shown in the display.

Table 28: show subscriber manager statistics Field Descriptions

Field	Description
Control Policy errors	Specifies the errors in the control policy.
Attribute format warnings	Specifies the attribute format warnings.
User Profile Statistics	Specifies the user profile statistics.
Session Disconnect Flow Control	Specifies the session disconnect flow control.

show subscriber running-config

To display the subscriber running configuration derived from dynamic template, use the **show subscriber running-config** command in EXEC.

show subscriber running-config {**location**| **subscriber-label**}

Syntax Description

location	Displays subscriber database running configuration information for all sessions at specified location.
subscriber-label	Allows to enter a hex value subscriber-value that ranges between 0X0-0xffffffff.
|	Specifies the output modifiers.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	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.

Task ID

Task ID	Operation
network	read

Examples

This is a sample output of the **show subscriber running-config** command:

```
RP/0/RSP0/CPU0:router# show subscriber running-config

Tue Jun 15 09:05:53.769 EDT
Session ID: 0x4000000
dynamic-template
 type ipsubscriber TEMPL1
  ipv4 unnumbered Loopback0
```

```
 !
!
dynamic-template
 type ipsubscriber TEMPL2
  service-policy input qos_policy
  vrf blue
  ipv4 mtu 1500
 !
!
Session ID: 0x4000082
dynamic-template
 type ipsubscriber TEMPL1
  ipv4 unnumbered Loopback0
 !
!
dynamic-template
 type ipsubscriber TEMPL2
  service-policy input qos_policy
  vrf blue
  ipv4 mtu 1500
 !
!
```

show subscriber session

To display the subscriber management session information, use the **show subscriber session** command in the EXEC mode.

show subscriber session {**all**| **debug**| **filter**| **subscriber-label**}

Syntax Description

all	Displays all subscriber sessions.
debug	Displays unique subscriber session selected for debugging.
filter	Displays the search results of the subscriber session database based on the filter criteria.
subscriber-label	Displays the unique ID of the subscriber session.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	This command was introduced.
Release 4.3.1	Added example output for **show subscriber session all detail** command to display service accounting feature information.

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.

For interface-based static sessions in the BNG, the value of *Type* field in the **show ipsubscriber session** command output is displayed as **IP: Static**.

Task ID

Task ID	Operation
network	read
config-services	read

Examples

This is the sample output of the **show subscriber session** command in the EXEC mode:

```
RP/0/RSP0/CPU0:router# show subscriber session all
RP/0/RSP0/CPU0:router# show subscriber session all summary location 0/1/CPU0
RP/0/RSP0/CPU0:router# show subscriber session filter vrf vrf1 location 0/1/CPU0
RP/0/RSP0/CPU0:router# show subscriber session subscriber-label 40
```

This is the sample output of the **show subscriber session** command:

```
Wed Jan 23 10:20:58.344 GMT
Codes: IN - Initialize, CN - Connecting, CD - Connected, AC - Activated,
       ID - Idle, DN - Disconnecting, ED - End

Type         Interface                State     Subscriber IP Addr / Prefix
                                               LNS Address (Vrf)
------------------------------------------------------------------------------
PPPoE:PTA    Gi0/1/0/0.pppoe1         AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.pppoe2         AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.pppoe3         AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.1.pppoe1       AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.1.pppoe2       AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.1.pppoe3       AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.2.pppoe1       AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.2.pppoe2       AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.2.pppoe3       AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.3.pppoe1       AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.3.pppoe2       AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.3.pppoe3       AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.pppoe4         AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.pppoe5         AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.pppoe6         AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.1.pppoe4       AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.1.pppoe5       AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.1.pppoe6       AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.2.pppoe4       AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.2.pppoe5       AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.2.pppoe6       AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.3.pppoe4       AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.3.pppoe5       AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.3.pppoe6       AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.pppoe7         AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.pppoe8         AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.pppoe9         AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.1.pppoe7       AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.1.pppoe8       AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.1.pppoe9       AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.2.pppoe7       AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.2.pppoe8       AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.2.pppoe9       AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.3.pppoe7       AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.3.pppoe8       AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.3.pppoe9       AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.pppoe10        AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.pppoe11        AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.pppoe12        AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.1.pppoe10      AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.1.pppoe11      AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.1.pppoe12      AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.2.pppoe10      AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.2.pppoe11      AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.2.pppoe12      AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.3.pppoe10      AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.3.pppoe11      AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.3.pppoe12      AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.pppoe13        AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.pppoe14        AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.pppoe15        AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.1.pppoe13      AC        100.0.0.1 (default)
```

```
PPPoE:PTA    Gi0/1/0/0.1.pppoe14      AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.1.pppoe15      AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.2.pppoe13      AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.2.pppoe14      AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.2.pppoe15      AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.3.pppoe13      AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.3.pppoe14      AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.3.pppoe15      AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.pppoe16        AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.pppoe17        AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.pppoe18        AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.1.pppoe16      AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.1.pppoe17      AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.1.pppoe18      AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.2.pppoe16      AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.2.pppoe17      AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.2.pppoe18      AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.3.pppoe16      AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.3.pppoe17      AC        100.0.0.1 (default)
PPPoE:PTA    Gi0/1/0/0.3.pppoe18      AC        100.0.0.1 (default)
```

This table describes the significant fields shown in the display.

Table 29: show subscriber session Field Descriptions

Field	Description
Type	Specifies the subscriber session type.
Interface	Specifies the interface type.
State	Specifies the states of the subscriber session such as initiate, connecting, connected, activated, disconnected, idle, end.
Subscriber IP Addr / Prefix LNS Address (Vrf)	Specifies the IP address of the subscriber interface.

This example shows the detailed information about all the subscriber sessions including service accounting information.

```
RP/0/RSP0/CPU0:router# show subscriber session all detail

Interface:               Bundle-Ether12.125.ip643
Circuit ID:              Unknown
Remote ID:               00066c9ced63ef20
Type:                    IP: DHCP-trigger
IPv6 State:              Up, Fri Feb  8 16:42:57 2013
IPv6 Address:            2001:2::b246, VRF: default
Delegated IPv6 Prefix:   3000:2:0:8546::/64, VRF: default
IPv6 Interface ID:       0004007d000c (30 30 30 34 30 30 37 64 30 30 30 63)
Mac Address:             0010.6401.0102
Account-Session Id:      00008ad2
Nas-Port:                Unknown
User name:               0010.6401.0102
Outer VLAN ID:           125
Subscriber Label:        0x00000046
Created:                 Fri Feb  8 16:42:57 2013
State:                   Activated
Authentication:          unauthenticated
Access-interface:        Bundle-Ether12.125
Policy Executed:
policy-map type control subscriber BNG-Test
  event Session-Start match-first [at Fri Feb  8 16:42:57 2013]
```

```
    class type control subscriber PPPoE do-until-failure [Failed]
    class type control subscriber IPoE-DS do-until-failure [Succeeded]
      1 activate dynamic-template IPoE [Succeeded]
      10 authorize aaa list default [Succeeded]
      15 activate dynamic-template test-svc1 [Succeeded]
      16 activate dynamic-template test-svc2 [Succeeded]
Session Accounting:
  Acct-Session-Id:          00008ad2
  Method-list:              default
  Accounting started:       Fri Feb  8 16:43:27 2013
  Interim accounting:       Off
Service Accounting:         AcctTurbo1G
  Acct-Session-Id:          00008ad3
  Method-list:              default
  Accounting started:       Fri Feb  8 16:43:27 2013
  Interim accounting:       On, interval 2 mins
    Last successful update: Never
    Next update in:         00:01:48 (dhms)
Service Accounting:         test-svc3
  Acct-Session-Id:          00008ad4
  Method-list:              default
  Accounting started:       Fri Feb  8 16:43:27 2013
  Interim accounting:       On, interval 2 mins
    Last successful update: Never
    Next update in:         00:01:48 (dhms)
Service Accounting:         svcAcct
  Acct-Session-Id:          00008ad5
  Method-list:              default
  Accounting started:       Fri Feb  8 16:43:27 2013
  Interim accounting:       Off
Service Accounting:         test-svc1
  Acct-Session-Id:          00008ad6
  Method-list:              default
  Accounting started:       Fri Feb  8 16:43:27 2013
  Interim accounting:       On, interval 2 mins
    Last successful update: Never
    Next update in:         00:01:48 (dhms)
Service Accounting:         test-svc2
  Acct-Session-Id:          00008ad7
  Method-list:              default
  Accounting started:       Fri Feb  8 16:43:27 2013
  Interim accounting:       On, interval 2 mins
    Last successful update: Never
    Next update in:         00:01:48 (dhms)
Last COA request received: unavailable
```

clear subscriber session

To clear the subscriber sessions in BNG, use the **clear subscriber session** command in EXEC mode.

clear subscriber session {**all** | **debug** { **subscriber-label** } | **identifier** { **access-interface** *interface-type interface-instance* | **interface** *interface-type interface-instance* } } [**location** *node-id*]

Syntax Description

all	Clears all subscriber sessions.
debug subscriber-label	Clears debug tracking of unique subscriber session.
identifier	Clears the subscriber session information based on the identifier(s) you select.
access-interface	Clears the subscriber session based on the access interface name.
interface-type	Specifies the interface type whose subscriber sessions you want to delete.
interface-instance	Specifies either a physical interface instance or a virtual interface instance that you want to delete. The details of the interface instance are 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 (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0. • Virtual interface instance. Number range varies depending on interface type.
location	Clears the subscriber session information of a specific location.

node-id	Specifies the node whose subscriber sessions you want to delete. The node-id argument is entered in the rack/slot/module notation.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
network	execute

Examples

This example shows how to clear all the subscriber sessions in a particular node location:

```
RP/0/RSP0/CPU0:router# clear subscriber session all location 0/RSP0/CPU0
```

Related Commands

Command	Description
show subscriber session, on page 500	Displays the subscriber management session information.

INDEX

A

aaa accounting service command 7
aaa accounting subscriber command 9
aaa accounting system rp-failover command 11
aaa attribute format command 13
aaa authentication subscriber command 16
aaa authorization subscriber command 18
AAA commands 1
aaa group server radius 20
aaa intercept command 22
aaa radius attribute command 23
aaa radius attribute nas-port-type 29
aaa server radius dynamic-author command 27
aaa service-accounting command 25, 62
accounting aaa list command 3
accounting aaa list type service command 5
ACL and ABF Commands 65
activate dynamic-template command 112
Address Pool Service Commands 77
address-pool command 139
address-range command 78
AFTR-name command 140
authenticate command 114
authorize command 116

B

broadcast-flag policy check command 141

C

class command 143
class-map type control subscriber command 118
clear pppoe statistics command 444
clear subscriber session command 504
Control Policy Commands 111

D

deactivate command 120
DHCP Commands 137
dhcp ipv4 command 145
dhcp ipv6 command 146
dhcpv6 address-pool command 147
dhcpv6 delegated-prefix-pool command 149
dns-server command 150
domain-name (DHCP IPv6 pool) command 152
dynamic-template command 216
dynamic-template type ipsubscriber command 218
dynamic-template type ppp command 220
dynamic-template type service command 222

E

event command 122
Excessive Punt Flow Trap Commands 235
exclude command 80

F

framed-prefix-pool command 154

H

helper-address command 155, 178

I

igmp accounting command 319
igmp explicit-tracking command 320
igmp query-interval command 322
igmp query-max-response-time command 324
initiator dhcp command 256
initiator unclassified-source command 258

interface (DHCP) command 157
interface subscriber-pppoe profile command 159
IPoE Commands 255
ipsubscriber interface command 260
ipsubscriber ipv4 l2-connected command 262
ipsubscriber ipv4 routed command 264
ipsubscriber ipv6 l2-connected command 262
ipsubscriber session-limit command 266
ipv4 access-group command 66
ipv4 access-list command 69
IPv4 Commands 279
ipv4 mtu command 280
ipv4 unnumbered (point-to-point) command 282
ipv4 unreachables disable command 284
ipv4 verify unicast source reachable-via command 286
ipv6 access-group command 71
ipv6 access-list command 73
ipv6 enable command 288
ipv6 mtu command 290
ipv6 nd dad attempts command 338
ipv6 nd framed-prefix-pool command 341
ipv6 nd managed-config-flag command 342
ipv6 nd ns-interval command 344
ipv6 nd nud-enable command 346
ipv6 nd other-config-flag command 347
ipv6 nd ra-interval command 349, 351
ipv6 nd ra-lifetime command 353
ipv6 nd ra-unicast command 355
ipv6 nd reachable-time command 356
ipv6 nd suppress-cache-learning command 358
ipv6 nd suppress-ra command 359
ipv6 unreachables disable command 292

L

l2tp reassembly command 398
l2tp-class command 396
lease command 160
lease proxy client-lease-time command 186
limit lease per-circuit-id command 180
limit lease per-interface command 184
limit lease per-remote-id command 182
lpts punt excessive-flow-trap command 236, 238, 243
lpts punt excessive-flow-trap penalty-rate command 239
lpts punt excessive-flow-trap penalty-timeout command 241

M

match option command 162
match vrf command 164
monitor-session (interface) command 224
Multicast Commands 317
multicast qos-correlation | passive command 326

N

Neighbor Discovery Commands 337
network command 82

P

pado delay circuit-id command 428
pado delay command 426
pado delay remote-id command 430
pado delay service-name command 432
policy-map type control subscriber command 126
policy-map type pbr command 128
pool ipv4 command 90
pool ipv6 command 92
pool vrf command 88
ppp authentication command 362
ppp chap command 365
PPP Commands 361
ppp ipcp command 367
ppp lcp command 369
ppp max-bad-auth command 371
ppp max-configure command 373
ppp max-failure command 375
ppp ms-chap command 377
ppp timeout command 379
pppoe bba-group command 434
PPPoE Commands 425
pppoe enable bba-group command 437
PPPoE LAC-Specific Commands 395
pppoe sessions limit command 439
pppoe sessions throttle command 442
prefix-length command 84
prefix-pool command 165
prefix-range command 86
profile command 166

Q

qos account command 462
QoS Commands 461
qos output minimum-bandwidth command 464

R

radius source-interface command 53

radius-server attribute command 31
radius-server dead-criteria command 33
radius-server deadtime command 35
radius-server disallow null-username command 37
radius-server host command 38
radius-server ipv4 dscp command 41
radius-server key command 42
radius-server load-balance command 44
radius-server retransmit command 46
radius-server source-port command 48
radius-server throttle 51
radius-server timeout command 49
radius-server vsa attribute ignore unknown command 50
redundancy command 401
relay information authenticate command 168
relay information check command 170
relay information option allow-untrusted command 174
relay information option command 172
relay information policy command 176
router igmp vrf vrf_name traffic profile command 318

S

service-policy (interface) command 468
service-policy command 226, 466
service-policy type control subscriber command 130
session-limit command 402
show aaa trace command 55
show class-map command 132
show dhcp ipv4 proxy binding command 188
show dhcp ipv4 proxy interface command 191
show dhcp ipv4 proxy profile command 193
show dhcp ipv4 proxy statistics command 195
show dhcp ipv6 proxy binding command 197
show dhcp ipv6 proxy interface command 199
show dhcp ipv6 proxy profile command 201
show dhcp ipv6 proxy statistics command 203
show dhcp ipv6 server binding command 205
show dhcp ipv6 server interface command 208
show dhcp ipv6 server profile command 210
show dhcp ipv6 server statistics command 212
show igmp unicast-qos-adjust statistics command 330
show igmp vrf command 333
show ipsubscriber command 268, 275
show ipsubscriber interface command 271
show ipv4 interface command 294
show ipv4 traffic command 298
show ipv6 interface command 301
show ipv6 neighbors command 305
show ipv6 neighbors summary command 311
show ipv6 traffic command 313
show l2tpv2 command 412
show l2tpv2 redundancy command 414
show l2tpv2 redundancy mirroring command 416
show lpts punt excessive-flow-trap command 253
show lpts punt excessive-flow-trap command 244
show lpts punt excessive-flow-trap information command 247
show lpts punt excessive-flow-trap interface command 250
show policy-map command 134
show pool ipv4 name command 96
show pool ipv6 name command 100
show pool vrf command 107
show ppp interfaces command 381
show ppp statistics command 389
show ppp summary command 392
show pppoe interfaces command 446
show pppoe limits command 448
show pppoe statistics command 452
show pppoe summary command 455
show pppoe throttles command 457
show qos inconsistency command 470
show qos interface command 473
show qos shared-policy-instance command 478
show qos summary command 481
show radius command 57
show radius server-groups detail 60
show subscriber database command 486
show subscriber feature accounting command 491
show subscriber manager command 495
show subscriber manager sadb command 493
show subscriber running-config command 498
show subscriber session command 500
show vpdn command 418
show vpdn redundancy command 420
show vpdn redundancy mirroring command 422
Subscriber Commands 483
subscriber session limit command 484

T

template command 404
test radius coa activate command 228
test radius coa deactivate command 228
timeout idle command 230
tunnel command 406

U

unicast-qos-adjust command 328
utilization-mark command 94

V

vpdn command 399, 408
vpn command 410
vrf(dynamic-template) command 232