Broadband Network Gateway Command Reference for Cisco ASR 9000 Series Routers

First Published: 2017-10-01
Last Modified: 2019-04-01

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
# CONTENTS

## PREFACE

Preface  xv

Changes to This Document  xv

Communications, Services, and Additional Information  xv

## CHAPTER 1

BNG AAA Commands  1

- aaa accounting service  3
- aaa accounting subscriber  5
- aaa accounting system rp-failover  7
- aaa attribute format  8
- aaa authentication subscriber  11
- aaa authorization policy-intf  13
- aaa authorization prepaid  14
- aaa authorization subscriber  15
- aaa group server diameter (BNG)  17
- aaa group server radius (BNG)  18
- aaa intercept  20
- aaa radius attribute  21
- aaa service-accounting  22
- aaa server radius dynamic-author  23
- aaa radius attribute nas-port-type  25
- accounting aaa list  26
- accounting aaa list type service  28
- accounting prepaid  29
- radius-server attribute  31
- radius-server attribute 11 default direction inbound  32
- radius-server dead-criteria  33
show pool ipv6 name 88
show pool vrf 95

CHAPTER 4

Control Policy Commands 97
activate 98
authenticate (BNG) 100
authorize 101
class-map type control subscriber 103
deactivate 104
decode 106
event 107
match (class-map) 110
match option (DHCPv6) 112
policy-map type control subscriber 114
policy-map type pbr 115
service-policy type control subscriber 116
show class-map 117
show policy-map 119

CHAPTER 5

BNG DHCP Commands 121
aaa dhcp-option force-insert 123
address-pool 124
aftr-name 125
authentication username 126
broadcast-flag policy check (BNG) 128
class 130
delayed authentication 132
dhcp ipv4 (BNG) 133
dhcp ipv6 (BNG) 134
dhcp-to-aaa option list 135
dhcpp6-to-aaa option list 136
dhcpp6 address-pool 137
dhcpp6 delegated-prefix-pool 138
dns-server (BNG) 139
domain-name (DHCP IPv6 pool-BNG) 141
duid allowed-type 143
duplicate-mac-allowed 144
framed-prefix-pool 146
giaddr policy keep 147
helper-address (BNG) 148
inner-cos 150
interface (DHCP-BNG) 152
interface subscriber-pppoe profile 154
lease 155
lease proxy client-lease-time 157
linkaddress-from-ra-enable 158
limit lease per-circuit-id 160
limit lease per-interface 161
limit lease per-remote-id 162
match-default 163
match mode-class 165
match option 167
match option 60 169
match vrf 171
option 17 172
outer-cos 173
prefix-pool 174
profile (BNG) 175
rapid commit 177
relay information authenticate (BNG) 178
relay information check (BNG) 180
relay information option (BNG) 182
relay information option allow-untrusted (BNG) 184
relay information policy (BNG) 186
relay option interface-id 188
relay option link-layer-addr 190
relay option remote-id 191
relay option subscriber-id 193
### C H A P T E R  6

**BNG Interface Commands**  
- show dhcp ipv4 proxy binding  194
- show dhcp ipv4 proxy interface (BNG)  198
- show dhcp ipv4 proxy profile  200
- show dhcp ipv4 proxy statistics  201
- show dhcp ipv6 proxy binding (BNG)  202
- show dhcp ipv6 proxy interface (BNG)  204
- show dhcp ipv6 proxy profile  206
- show dhcp ipv6 proxy statistics  207
- show dhcp ipv6 server binding  209
- show dhcp ipv6 server interface  212
- show dhcp ipv6 server profile  214
- show dhcp ipv6 server statistics  215

### C H A P T E R  7

**DIAMETER Commands**  
- address (DIAMETER)  227
- clear diameter peer  228
- clear diameter statistics  229
- destination host  230
- destination realm  231
- diameter attribute list  232
- diameter gx  234
- diameter gx retransmit  235
- diameter gx tx-timer  236
- diameter gy  237
- diameter gy retransmit  238
- diameter gy tx-timer  239
- diameter origin host  240
- diameter origin realm  241
- diameter peer  242
C H A P T E R 8

Dynamic Template Commands 269

dynamic-template 270
dynamic-template type ipsubscriber 271
dynamic-template type ppp 272
dynamic-template type service 273
monitor-session (interface-dynamic-template-BNG) 274
service-policy (BNG) 276
test radius coa activate 278
timeout idle 280
vrf (dynamic-template-BNG) 282

C H A P T E R 9

Excessive Punt Flow Trap Commands 283

lptspuntexcessive-flow-trap 284
lptspuntexcessive-flow-trapdampening 285
lptspuntexcessive-flow-trapinterface-based-flow 286
lptspuntexcessive-flow-trapnon-subscriber-interfaces 287
lpts punt excessive-flow-trap penalty-rate  288
lpts punt excessive-flow-trap penalty-timeout  290
lpts punt excessive-flow-trap subscriber-interfaces  292
show lpts punt excessive-flow-trap  293
show lpts punt excessive-flow-trap information  296
show lpts punt excessive-flow-trap interface  299
show lpts punt excessive-flow-trap protocol  301

---

CHAPTER 10  IPOE Commands  303
initiator dhcp  304
initiator dhcp-snoop  306
initiator unclassified-ip  308
initiator unclassified-source  310
ipsubscriber interface  311
ipsubscriber l2-connected  312
ipsubscriber routed  314
ipsubscriber session-limit  316
ipsubscriber subscriber-templates  317
show ipsubscriber access-interface  318
show ipsubscriber interface  321
show ipsubscriber summary  325
show ipsubscriber template-interface  328

---

CHAPTER 11  IPv4 and IPv6 Commands  331
ipv4 mtu (BNG)  332
ipv4 unnumbered (point-to-point -BNG)  334
ipv4 unreachables disable (BNG)  336
ipv4 verify unicast source reachable-via (BNG)  338
ipv6 enable (BNG)  340
ipv6 mtu (BNG)  342
ipv6 unreachables disable (BNG)  344
show ipv4 interface (BNG)  346
show ipv4 traffic (BNG)  349
show ipv6 interface (BNG)  351
ppp chap 411
ppp ipcp 412
ppp lcp 414
ppp max-bad-auth (BNG) 415
ppp max-configure (BNG) 417
ppp max-failure (BNG) 419
ppp ms-chap 421
ppp timeout 422
show ppp interfaces (BNG) 424
show ppp statistics 430
show ppp summary 433

CHAPTER 15

PPPoE LAC-Specific Commands 435
12tp-class 436
12tp-source-ip 438
12tp reassembly 439
process-failures switchover 440
redundancy (BNG) 441
session-limit (BNG) 442
template (BNG) 443
tunnel 444
vpdn 445
vpn 446
show l2tpv2 447
show l2tpv2 redundancy 449
show l2tpv2 redundancy mirroring 451
show vpdn 453
show vpdn redundancy 456
show vpdn redundancy mirroring 457

CHAPTER 16

PPPoE Commands 459
pado delay 460
pado delay circuit-id 461
pado delay remote-id 463
pado delay service-name 465
pppo bba-group 467
pppo enable bba-group 470
pppo in-flight-window 471
pppo sessions limit 472
pppo sessions throttle 475
clear pppoe statistics 477
show pppoe interfaces 479
show pppoe limits 481
show pppoe statistics 485
show pppoe summary 488
show pppoe throttles 490

CHAPTER 17  QOS Commands 495
qos account 496
qos output minimum-bandwidth 498
service-policy (QoS-BNG) 499
service-policy (interface BNG) 502
shape average (BNG) 505
show qos inconsistency (BNG) 507
show qos interface (BNG) 509
show qos shared-policy-instance (BNG) 520
show qos summary BNG 522

CHAPTER 18  Subscriber and Session Redundancy Commands 525
access-tracking (BNG) 527
accounting interim variation 529
bng-interface (subscriber) 530
clear session-redundancy 531
clear subscriber session 532
core-tracking 534
disable (BNG) 535
enable-fast-switchover 537
hold-timer (BNG) 538
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>http-enrichment parameter-list</td>
<td>540</td>
</tr>
<tr>
<td>http-enrichment parameter-list (subscriber)</td>
<td>542</td>
</tr>
<tr>
<td>interface-list (BNG)</td>
<td>544</td>
</tr>
<tr>
<td>peer (BNG)</td>
<td>547</td>
</tr>
<tr>
<td>preferred-role (BNG)</td>
<td>549</td>
</tr>
<tr>
<td>peer route-disable</td>
<td>551</td>
</tr>
<tr>
<td>revertive-timer (BNG)</td>
<td>552</td>
</tr>
<tr>
<td>source-interface (BNG)</td>
<td>554</td>
</tr>
<tr>
<td>session redundancy</td>
<td>556</td>
</tr>
<tr>
<td>session redundancy group</td>
<td>557</td>
</tr>
<tr>
<td>session redundancy switchover</td>
<td>558</td>
</tr>
<tr>
<td>session redundancy synchronize</td>
<td>559</td>
</tr>
<tr>
<td>state-control-route</td>
<td>560</td>
</tr>
<tr>
<td>subscriber arp scale-mode-enable</td>
<td>563</td>
</tr>
<tr>
<td>subscriber arp uncond-proxy-arp-enable</td>
<td>564</td>
</tr>
<tr>
<td>subscriber featurette dhcp-renew-author</td>
<td>565</td>
</tr>
<tr>
<td>subscriber featurette identity-change</td>
<td>566</td>
</tr>
<tr>
<td>subscriber redundancy</td>
<td>567</td>
</tr>
<tr>
<td>subscriber redundancy group</td>
<td>568</td>
</tr>
<tr>
<td>subscriber redundancy switchover</td>
<td>569</td>
</tr>
<tr>
<td>subscriber redundancy synchronize</td>
<td>570</td>
</tr>
<tr>
<td>subscriber session limit</td>
<td>571</td>
</tr>
<tr>
<td>tracking-disable (BNG)</td>
<td>572</td>
</tr>
<tr>
<td>virtual-mac</td>
<td>573</td>
</tr>
<tr>
<td>virtual-mac-disable</td>
<td>574</td>
</tr>
<tr>
<td>virtual-mac-prefix</td>
<td>575</td>
</tr>
<tr>
<td>show sessionmon license</td>
<td>576</td>
</tr>
<tr>
<td>show subscriber database</td>
<td>577</td>
</tr>
<tr>
<td>show subscriber database template</td>
<td>578</td>
</tr>
<tr>
<td>show subscriber feature accounting</td>
<td>579</td>
</tr>
<tr>
<td>show subscriber manager sadb</td>
<td>580</td>
</tr>
<tr>
<td>show subscriber manager statistics</td>
<td>581</td>
</tr>
<tr>
<td>show subscriber redundancy group</td>
<td>582</td>
</tr>
<tr>
<td>show subscriber redundancy summary</td>
<td>583</td>
</tr>
</tbody>
</table>
show subscriber running-config  606
show subscriber session       608
show subscriber session filter 617
show subscriber session history 619
Preface

From Release 6.1.2 onwards, Cisco introduces support for the 64-bit Linux-based IOS XR operating system. Extensive feature parity is maintained between the 32-bit and 64-bit environments. Unless explicitly marked otherwise, the contents of this document are applicable for both the environments. For more details on Cisco IOS XR 64 bit, refer to the Release Notes for Cisco ASR 9000 Series Routers, Release 6.1.2 document.

The Preface contains these topics:

• Changes to This Document, on page xv
• Communications, Services, and Additional Information, on page xv

Changes to This Document

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

<table>
<thead>
<tr>
<th>Date</th>
<th>Change Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 2017</td>
<td>Initial release of this document.</td>
</tr>
<tr>
<td>July 2017</td>
<td>Republished for Release 6.2.2.</td>
</tr>
<tr>
<td>March 2018</td>
<td>Republished for Release 6.3.2.</td>
</tr>
<tr>
<td>March 2018</td>
<td>Republished for Release 6.4.1.</td>
</tr>
<tr>
<td>July 2018</td>
<td>Republished for Release 6.5.1.</td>
</tr>
<tr>
<td>January 2019</td>
<td>Republished for Release 6.5.2.</td>
</tr>
<tr>
<td>March 2019</td>
<td>Republished for Release 6.5.3.</td>
</tr>
<tr>
<td>April 2019</td>
<td>Republished for Release 6.6.2</td>
</tr>
</tbody>
</table>

Communications, Services, and Additional Information

• To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
• To get the business impact you’re looking for with the technologies that matter, visit Cisco Services.
• To submit a service request, visit Cisco Support.
• To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
• To obtain general networking, training, and certification titles, visit Cisco Press.
• To find warranty information for a specific product or product family, access Cisco Warranty Finder.

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

To use commands of this module, 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 any command, contact your AAA administrator for assistance.

- aaa accounting service, on page 3
- aaa accounting subscriber, on page 5
- aaa accounting system rp-failover, on page 7
- aaa attribute format, on page 8
- aaa authentication subscriber, on page 11
- aaa authorization policy-intf, on page 13
- aaa authorization prepaid, on page 14
- aaa authorization subscriber, on page 15
- aaa group server diameter (BNG), on page 17
- aaa group server radius (BNG), on page 18
- aaa intercept, on page 20
- aaa radius attribute, on page 21
- aaa service-accounting, on page 22
- aaa server radius dynamic-author, on page 23
- aaa radius attribute nas-port-type, on page 25
- accounting aaa list, on page 26
- accounting aaa list type service, on page 28
- accounting prepaid, on page 29
- radius-server attribute, on page 31
- radius-server attribute 11 default direction inbound, on page 32
- radius-server dead-criteria, on page 33
- radius-server deadtime(BNG), on page 34
- radius-server disallow null-username, on page 35
- radius-server host (BNG), on page 36
- radius-server ipv4 dscp, on page 38
- radius-server key(BNG), on page 39
• radius-server load-balance, on page 41
• radius-server retransmit(BNG), on page 42
• radius-server source-port, on page 43
• radius-server timeout(BNG), on page 44
• radius-server vsa attribute ignore unknown, on page 45
• radius-server throttle, on page 46
• radius source-interface(BNG), on page 47
• show aaa trace, on page 49
• show radius (BNG), on page 51
• show radius server-groups detail, on page 54
• statistics period service-accounting, on page 56
aaa accounting service

To create an accounting list for service accounting, use the `aaa accounting service` command in Global Configuration mode or Admin 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|diameter|radius}|group {group_name|diameter|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.
- **diameter**: Specifies the list of all DIAMETER peers.
- **radius**: Specifies the list of all RADIUS hosts.

**Command Default**

None

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.3.0</td>
<td>The <code>diameter</code> keyword was added for DIAMETER protocol support in BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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
```
This example shows how to configure the **aaa accounting service** command with DIAMETER protocol to carry subscriber service accounting records to DIAMETER server using base accounting application:

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

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>aaa accounting subscriber, on page 5</strong></td>
<td>Creates an accounting list for subscriber accounting.</td>
</tr>
</tbody>
</table>
### aaa accounting subscriber

To create an accounting list for subscriber accounting, use the `aaa accounting subscriber` command in Global Configuration mode. To disable this accounting list for subscriber accounting, use the `no` form of this command.

```plaintext
aaa accounting subscriber {list_name |default} {broadcast group {group_name |diameter |radius} |group {group_name |diameter |radius}}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Uses the listed authentication methods that follow this keyword as the default list of methods for authentication.</td>
</tr>
<tr>
<td>list-name</td>
<td>Represents the character string for the list name for AAA authentication.</td>
</tr>
<tr>
<td>broadcast</td>
<td>Specifies the broadcast accounting for subscriber.</td>
</tr>
<tr>
<td>group</td>
<td>Specifies the server-group.</td>
</tr>
<tr>
<td>group_name</td>
<td>Specifies the server group name.</td>
</tr>
<tr>
<td>diameter</td>
<td>Specifies the list of all DIAMETER peers.</td>
</tr>
<tr>
<td>radius</td>
<td>Specifies the list of all RADIUS hosts.</td>
</tr>
</tbody>
</table>

### Command Default

None

### Command Modes

Global Configuration mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.3.0</td>
<td>The <code>diameter</code> keyword was added for DIAMETER protocol support in BNG.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

No specific guidelines impact the use of this command.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>
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
```

This example shows how to configure the `aaa accounting subscriber` command with DIAMETER protocol to carry subscriber session accounting to DIAMETER server using base accounting application:

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aaa accounting system rp-failover</code>, on page 7</td>
<td>Creates an accounting list for system events.</td>
</tr>
</tbody>
</table>
aaa accounting system rp-failover

To create an accounting list to send rp-failover or rp-switchover start or stop accounting messages, use the
\texttt{aaa accounting system rp-failover} command in Global Configuration mode. To disable the system accounting
for rp-failover, use the \texttt{no} form of this command.

\texttt{aaa accounting system rp-failover \{list\_name \{start-stop|stop-only\}|default \{start-stop|stop-only\}}

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\texttt{list_name}</td>
<td>Specifies the accounting list name.</td>
</tr>
<tr>
<td>\texttt{default}</td>
<td>Specifies the default accounting list.</td>
</tr>
<tr>
<td>\texttt{start-stop}</td>
<td>Enables the start and stop records.</td>
</tr>
<tr>
<td>\texttt{stop-only}</td>
<td>Enables the stop records only.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Global Configuration mode</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>\texttt{Release}</td>
</tr>
<tr>
<td>Release 4.2.0</td>
</tr>
</tbody>
</table>

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

<table>
<thead>
<tr>
<th>Task</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This is an example of configuring the \texttt{aaa accounting system rp-failover} command for default
accounting list:

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

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa attribute format</td>
<td>Create an AAA attribute format name.</td>
</tr>
</tbody>
</table>
**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|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} ]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>format_name</code></td>
<td>Specifies the name of the format.</td>
</tr>
<tr>
<td><code>circuit-id</code></td>
<td>Specifies the construction of the AAA attribute format name for subscribers based on the circuit-ID.</td>
</tr>
<tr>
<td><code>format-string</code></td>
<td>Specifies the extended string format of the AAA attribute format name.</td>
</tr>
<tr>
<td><code>string</code></td>
<td>Specifies the regular ASCII characters that includes conversion specifiers. The value is enclosed in double quotes.</td>
</tr>
<tr>
<td><code>Identity-Attribute</code></td>
<td>Identifies a session.</td>
</tr>
<tr>
<td><code>length</code></td>
<td>Specifies the length of the formatted attribute string.</td>
</tr>
<tr>
<td><code>length</code></td>
<td>Length of the formatted string, in integer. The range is from 1 to 253.</td>
</tr>
<tr>
<td><code>mac-address</code></td>
<td>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).</td>
</tr>
<tr>
<td><code>remote-id</code></td>
<td>Specifies the construction of the AAA attribute format name for subscribers based on the remote-ID.</td>
</tr>
<tr>
<td><code>plus</code></td>
<td>Specifies the use of additional identifiers.</td>
</tr>
<tr>
<td><code>separator</code></td>
<td>Specifies the separator to be used between keys.</td>
</tr>
<tr>
<td><code>separator</code></td>
<td>Separator to be used between keys, default is a semicolon.</td>
</tr>
<tr>
<td><code>username-strip</code></td>
<td>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.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.2.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.2.1</td>
<td>The support for format-string keyword was added.</td>
</tr>
<tr>
<td>Release 6.2.1</td>
<td>Introduced support for a new MAC address format, client-mac-address-custom1, which is in 01.23.45.67.89.AB format.</td>
</tr>
<tr>
<td>Release 6.4.1</td>
<td>Introduced support for dhcpv6-client-id-enterprise-identifier, dhcpv6-vendor-class-spl, dhcpv4-client-id-spl and dhcpv4-vendor-class as part of enabling AAA username formation using DHCP option 1 and option 16.</td>
</tr>
</tbody>
</table>

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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"
RP/0/RSP0/CPU0:router(config-id-format)# username-strip prefix-delimiter @
```

This is an example of configuring MAC address in "01.23.45.67.89.AB" format:

```
RP/0/RSP0/CPU0:router(config)# aaa attribute format form1
RP/0/RSP0/CPU0:router(config-id-format)# format-string length 253 "%s"
client-mac-address-custom1
```

This example shows how to enable AAA username formation using DHCP option 1 and option 16 in BNG:
aaa attribute format format_v6
format-string length 233 "%s@%s"
dhcpv6-client-id-enterprise-identifier dhcpv6-vendor-class-string

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa accounting subscriber, on page 5</td>
<td>Creates an accounting list for subscriber accounting.</td>
</tr>
</tbody>
</table>
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 |diameter |radius}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>default</code></td>
<td>Uses the listed authentication methods that follow this keyword as the default list of methods for authentication.</td>
</tr>
<tr>
<td><code>list-name</code></td>
<td>Represents the character string for the list name for AAA authentication.</td>
</tr>
<tr>
<td><code>group</code></td>
<td>Specifies the server-group.</td>
</tr>
<tr>
<td><code>diameter</code></td>
<td>Specifies the list of all DIAMETER peers.</td>
</tr>
<tr>
<td><code>radius</code></td>
<td>Specifies the list of all RADIUS hosts.</td>
</tr>
<tr>
<td><code>server_group_name</code></td>
<td>Specifies the server group name.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.3.0</td>
<td>The <code>diameter</code> keyword was added for DIAMETER protocol support in BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This is an example of configuring the `aaa authentication subscriber` command in the Global Configuration mode:
This example shows how to configure the `aaa authentication subscriber` command with DIAMETER protocol to carry subscriber authentication with DIAMETER protocol using NASREQ application:

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aaa authorization subscriber, on page 15</code></td>
<td>Creates authorization-related configurations</td>
</tr>
</tbody>
</table>
aaa authorization policy-intf

To configure authorization lists for DIAMETER policy interface (Gx interface), use the **aaa authorization policy-intf** command in Global Configuration mode. To remove the authorization lists for DIAMETER policy interface (Gx interface), use the *no* form of this command.

```
aaa authorization policy-intf {list-name |default} group {server-group-name |diameter}
```

### Syntax Description

- **list-name**
  - Specifies the list name for AAA authorization.

- **default**
  - Specifies default list name for AAA authorization.

- **group**
  - Specifies the server-group.

- **server-group-name**
  - Specifies the server-group name.

- **diameter**
  - Specifies the list of all DIAMETER peers.

### Command Default

None

### Command Modes

Global Configuration mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

No specific guidelines impact the use of this command.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to configure authorization lists for DIAMETER policy interface (Gx interface) in BNG:

```
RP/0/RSP0/CPU0:router(config)# aaa authorization policy-intf default group diameter
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa authorization prepaid, on page 14</td>
<td>Configures authorization lists for DIAMETER prepaid interface (Gy interface).</td>
</tr>
</tbody>
</table>
aaa authorization prepaid

To configure authorization lists for DIAMETER prepaid interface (Gy interface), use the `aaa authorization prepaid` command in Global Configuration mode. To remove the authorization lists for DIAMETER prepaid interface (Gy interface), use the `no` form of this command.

```
aaa authorization prepaid {list-name |default} group {server-group-name |diameter}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>list-name</code></td>
<td>Specifies the list name for AAA authorization.</td>
</tr>
<tr>
<td><code>default</code></td>
<td>Specifies default list name for AAA authorization.</td>
</tr>
<tr>
<td><code>group</code></td>
<td>Specifies the server-group.</td>
</tr>
<tr>
<td><code>server-group-name</code></td>
<td>Specifies the server-group name.</td>
</tr>
<tr>
<td><code>diameter</code></td>
<td>Specifies the list of all DIAMETER peers.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to configure authorization lists for DIAMETER prepaid interface (Gy interface) in BNG:

```
RP/0/RSP0/CPU0:router(config)# aaa authorization prepaid default group diameter
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aaa authorization policy-intf, on page 13</code></td>
<td>Configures authorization lists for DIAMETER policy interface (Gx interface).</td>
</tr>
</tbody>
</table>
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 |diameter |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.

- **diameter**
  - Specifies the list of all DIAMETER peers.

- **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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.2.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 5.3.0</td>
<td>The <code>diameter</code> keyword was added for DIAMETER protocol support in BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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 sgl group sg2
```

This example shows how to configure the `aaa authorization subscriber` command to carry subscriber authorization with DIAMETER protocol using NASREQ application:
**RP/0/RSP0/CPU0:router(config)# aaa authorization subscriber default group diameter**

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>aaa authentication subscriber</strong>, on page 11</td>
<td>Creates a method list for subscriber authentication.</td>
</tr>
</tbody>
</table>
aaa group server diameter (BNG)

To configure the named server group for DIAMETER, and to enter the server group sub-mode, use the `aaa group server diameter` command in Global Configuration mode. To remove the named server group for DIAMETER, use the `no` form of this command.

```
aaa group server diameter server-group-name
```

**Syntax Description**

| server-group-name | Specifies the server-group name. |

**Command Default**

None

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read,</td>
</tr>
<tr>
<td></td>
<td>write</td>
</tr>
</tbody>
</table>

This example shows how to configure the named server group for DIAMETER, and to enter the server group sub-mode in BNG:

```
RP/0/RSP0/CPU0:router(config)# aaa group server diameter GX_SG
```
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 server_group_name [ { accounting | authorization | deadtime | load-balance | server | server-private | source-interface | throttle | vrf; } ]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server_group_name</td>
<td>Specifies the AAA group server RADIUS name.</td>
</tr>
<tr>
<td>accounting</td>
<td>Specifies a RADIUS attribute filter for accounting.</td>
</tr>
<tr>
<td>authorization</td>
<td>Specifies a RADIUS attribute filter for authorization.</td>
</tr>
<tr>
<td>deadtime</td>
<td>Specifies the time in minutes after which a RADIUS server will be marked up after it has gone dead.</td>
</tr>
<tr>
<td>load-balance</td>
<td>Specifies the radius load-balancing options.</td>
</tr>
<tr>
<td>server</td>
<td>Specifies the RADIUS server.</td>
</tr>
<tr>
<td></td>
<td>Accepts IP address (IPv4 and IPv6) or hostname of the RADIUS server. The hostname option is supported only for IPv4 domain address.</td>
</tr>
<tr>
<td>server-private</td>
<td>Specifies a private RADIUS server.</td>
</tr>
<tr>
<td></td>
<td>Accepts IP address (IPv4 and IPv6) or hostname of the RADIUS server. The hostname option is supported only for IPv4 domain address.</td>
</tr>
<tr>
<td>source-interface</td>
<td>Specifies interface for source address in RADIUS packet.</td>
</tr>
<tr>
<td>throttle</td>
<td>Specifies RADIUS throttling options.</td>
</tr>
<tr>
<td>vrf</td>
<td>Specifies the VRF to which the server group belongs.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.3.1</td>
<td>The command was modified to add IPv6 address support for <code>server</code> and <code>server-private</code> configuration, as part of RADIUS over IPv6 feature.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.
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-ag-radius)#server 99.1.1.10 auth-port 1812 acct-port 1813
RP/0/RSP0/CPU0:router(config-ag-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**

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.3.2</td>
<td>By default, Lawful Intercept (LI) is not a part of the Cisco IOS XR software. The LI package needs to be installed separately. So, this command is enabled only after installing and activating the asr9k-li-px.pie.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To use `aaa intercept` command, you must install and activate the `asr9k-li-px.pie`.

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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
<tr>
<td>li</td>
<td>read</td>
</tr>
</tbody>
</table>

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}}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>called-station-id</td>
<td>Specifies the AAA nas-port attribute.</td>
</tr>
<tr>
<td>calling-station-id</td>
<td>Specifies the AAA nas-port attribute.</td>
</tr>
<tr>
<td>nas-port</td>
<td>Specifies the AAA nas-port attribute.</td>
</tr>
<tr>
<td>nas-port-id</td>
<td>Specifies the AAA nas-port-id attribute.</td>
</tr>
<tr>
<td>format</td>
<td>Specifies the AAA nas-port attribute format.</td>
</tr>
<tr>
<td>e</td>
<td>Specifies the AAA format type.</td>
</tr>
<tr>
<td>format_name</td>
<td>Specifies a 32 character string representing the format to be used.</td>
</tr>
<tr>
<td>type</td>
<td>Specifies the AAA nas-port attribute format.</td>
</tr>
<tr>
<td>value</td>
<td>Specifies the Nas-Port-Type value to apply format string on. The nas port value ranges from 0-44.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Global Configuration mode

**Command History**

```
Release    Modification
4.2.0       This command was introduced.
```

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

```
Task ID    Operation
ip-services read, write
```

This is an example of configuring the **aaa radius attribute** command in the Global Configuration mode:

```
RP/0/RSP0/CP00: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 Admin Configuration mode. To disable this behavior, use the `no` form of this command.

`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 mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA accounting subscriber, on page 5</td>
<td>Creates an accounting list for subscriber accounting.</td>
</tr>
<tr>
<td>AAA accounting service, on page 3</td>
<td>Creates an accounting list for service accounting.</td>
</tr>
</tbody>
</table>
**aaa server radius dynamic-author**

To configure radius dynamic author server, use the `aaa server radius dynamic-author` command in Global Configuration mode or Admin Configuration mode. To disable this subscriber authentication method, use the `no` form of this command.

```
aaa server radius dynamic-author {client hostname |ignore {server-key |session-key}|port port_number |server-key {0 |7 |line_number}}
```

**Syntax Description**

- **session-key**: Specifies that the session-key could be ignored.
- **client**: Represents the CoA client configuration.
- **hostname**: Specifies the hostname (IPv4 address or domain or IPv6 address) of the CoA client. IPv6 domain name is not supported.
- **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 mode.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.2.1</td>
<td>The support for the keywords, auth-key and ignore {session-key} were removed.</td>
</tr>
<tr>
<td>5.3.1</td>
<td>The command was modified to add IPv6 address support for aaa server radius dynamic-author client configuration, as part of RADIUS over IPv6 feature.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If multiple session identification keys are present in the CoA request, an AND operation is performed such that all the keys participate in the session selection. That is, if the CoA request contains the Accounting-Session-ID attribute and a Framed-IP-Address, then these parameters must match on the targeted session. For example, if the Session-ID referenced is 00001111 and the Framed-IP-Address is 10.0.0.10, and...
if the BNG is having a subscriber session with ID as 00001111 but with address as 10.10.10.1, then the session is not subjected to the CoA action. A CoA NACK is returned in this case.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>write</td>
<td></td>
</tr>
</tbody>
</table>

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

### Syntax Description

```plaintext
aaa radius attribute nas-port-type {value string}
```

- **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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

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

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aaa radius attribute</code>, on page 21</td>
<td>Configures a format e encode string for particular interface or NAS-Port type.</td>
</tr>
</tbody>
</table>
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}
```

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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
```
### BNG AAA Commands

**accounting aaa list**

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>dynamic-template, on page 270</td>
<td>Enables the dynamic template configuration mode.</td>
</tr>
<tr>
<td></td>
<td>dynamic-template type ppp, on page 272</td>
<td>Enables the ppp dynamic template type.</td>
</tr>
<tr>
<td></td>
<td>dynamic-template type ipsubscriber, on page 271</td>
<td>Enables the ipsubscriber dynamic template type.</td>
</tr>
</tbody>
</table>
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]
```

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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

```
RP/0/RSP0/CP00:router# configure
RP/0/RSP0/CP00:router(config)# dynamic-template
RP/0/RSP0/CP00:router(config-dynamic-template)# type service s1
RP/0/RSP0/CP00:router(config-dynamic-template-type)# accounting aaa list l1 type service periodic-interval 600
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dynamic-template, on page 270</td>
<td>Enables the dynamic template configuration mode.</td>
</tr>
<tr>
<td>dynamic-template type service, on page 273</td>
<td>Specifies the service template type for a group of subscribers or services.</td>
</tr>
</tbody>
</table>
accounting prepaid

To configure accounting information for subscriber prepaid feature in BNG, use the `accounting prepaid` command in subscriber configuration mode. To remove this configuration, use the `no` form of this command.

```
accounting prepaid name [method-list authorization list-name | password password | quota-holding time quota-holding-time | quota-validity time quota-validity-time | threshold {time time-threshold | volume volume-threshold} | traffic {both | inbound | outbound}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Prepaid configuration name or default.</td>
</tr>
<tr>
<td>method-list</td>
<td>Specifies method list configuration.</td>
</tr>
<tr>
<td>authorization</td>
<td>Specifies authorization method list.</td>
</tr>
<tr>
<td>list-name</td>
<td>Name of the authorization method list.</td>
</tr>
<tr>
<td>password</td>
<td>Specifies the password to be used when placing prepaid authorization or re-authorization requests.</td>
</tr>
<tr>
<td>quota-holding time</td>
<td>Specifies quota holding time.</td>
</tr>
<tr>
<td>quota-validity time</td>
<td>Specifies quota validity time.</td>
</tr>
<tr>
<td>quota-holding-time</td>
<td>Quota holding time, in seconds. The range is from 0 to 99000; the default is 100.</td>
</tr>
<tr>
<td>quota-validity-time</td>
<td>Quota validity time, in seconds. The range is from 0 to 99000; the default is 50.</td>
</tr>
<tr>
<td>threshold</td>
<td>Specifies the threshold configuration for prepaid feature.</td>
</tr>
<tr>
<td>time</td>
<td>Specifies the time threshold.</td>
</tr>
<tr>
<td>time-threshold</td>
<td>Time threshold, in seconds. The range is 0 to 4294967295; the default is 100.</td>
</tr>
<tr>
<td>volume</td>
<td>Specifies the volume threshold.</td>
</tr>
</tbody>
</table>
### volume-threshold
Volume threshold, in bytes.
The range is 0 to 4294967295; the default is 100.

### traffic
Specifies the traffic direction to be considered while deriving the volume.
The default is **inbound**.

- **inbound**
  Considers inbound traffic while deriving the volume.

- **outbound**
  Considers outbound traffic while deriving the volume.

- **both**
  Considers both inbound and outbound traffic while deriving the volume.

---

**Command Default**
None

**Command Modes**
Subscriber configuration

**Command History**
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To configure the authorization method list, the accounting network name must already be created using `aaa accounting network` command in global configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to configure accounting information for subscriber prepaid feature in BNG:

```
RP/0/RSP0/CPU0:router(config)# subscriber
RP/0/RSP0/CPU0:router(config-subscriber)# accounting prepaid feat1
RP/0/RSP0/CPU0:router(config-prepaid)# traffic both
```
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}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>list</code></td>
<td>Specifies a list of attributes that are used in conjunction with server-groups to accept or reject a list of attributes.</td>
</tr>
<tr>
<td><code>list_name</code></td>
<td>Specifies the list name.</td>
</tr>
<tr>
<td><code>attribute</code></td>
<td>Specifies a list of Radius attributes.</td>
</tr>
<tr>
<td><code>list</code></td>
<td>Specifies the list of comma-delimited Radius attributes.</td>
</tr>
<tr>
<td><code>vendor-id</code></td>
<td>Specifies the vendor-id of the RADIUS attribute.</td>
</tr>
<tr>
<td><code>value</code></td>
<td>Specifies the vendor-id value. The value ranges from 0 to 429496729.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

- **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 attribute 11 default direction inbound

To change the direction in which the Remote Authentication Dial In User Service (RADIUS) filter-ID attribute is applied, use the `radius-server attribute 11 default direction inbound` command in Global Configuration mode.

### Syntax Description

This command has no keywords or arguments.

### Command Default

RADIUS filter-ID attribute is applied by default in the output direction of the corresponding subscriber interface.

### Command Modes

Global Configuration mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.3.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

No specific guidelines impact the use of this command.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Example

This example shows how to change the direction of the RADIUS filter-ID attribute:

```
RP/0/RSP0/CPU0:router # configure
RP/0/RSP0/CPU0:router(config)# radius-server attribute 11 default direction inbound
```
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}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>time</code></td>
<td>Specifies the minimum time that must elapse since a response was received from this RADIUS server.</td>
</tr>
<tr>
<td><code>value</code></td>
<td>Specifies the time in seconds. The value ranges from 1 to 120.</td>
</tr>
<tr>
<td><code>tries</code></td>
<td>Specifies the minimum number of transmissions (original attempts plus retransmits) to this RADIUS server.</td>
</tr>
<tr>
<td><code>number_of_tries</code></td>
<td>Specifies the number of tries. The range is from 1 to 100.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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 in Global Configuration mode. To set deadtime to 0, use the `no` form of this command.

```
radius-server deadtime minutes
```

**Syntax Description**

```
minutes  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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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**

The following 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.

**Example**

```plaintext
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]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntex Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip-address</strong></td>
<td>IP address of the RADIUS server host.</td>
</tr>
<tr>
<td><strong>auth-port</strong></td>
<td>(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.</td>
</tr>
<tr>
<td><strong>acct-port</strong></td>
<td>(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.</td>
</tr>
<tr>
<td><strong>timeout</strong></td>
<td>(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 <code>radius-server timeout</code> 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.</td>
</tr>
<tr>
<td><strong>retransmit</strong></td>
<td>(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 <code>radius-server retransmit</code> 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.</td>
</tr>
<tr>
<td><strong>key</strong></td>
<td>(Optional) Specifies the authentication and encryption key used between the router and the RADIUS server. This key overrides the global setting of the <code>radius-server key</code> command. If no key string is specified, the global value is used.</td>
</tr>
</tbody>
</table>

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 mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.2.0</td>
<td>This command was supported on BNG.</td>
</tr>
<tr>
<td>Release 5.3.1</td>
<td>The command was modified to add IPv6 address support for the RADIUS server host configuration.</td>
</tr>
</tbody>
</table>
Usage Guidelines

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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa accounting subscriber</td>
<td>Creates a method list for accounting.</td>
</tr>
<tr>
<td>aaa authentication subscriber</td>
<td>Creates a method list for authentication.</td>
</tr>
<tr>
<td>aaa authorization subscriber</td>
<td>Creates a method list for authorization.</td>
</tr>
<tr>
<td>radius-server key(BNG), on page 39</td>
<td>Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.</td>
</tr>
<tr>
<td>radius-server retransmit(BNG), on page 42</td>
<td>Specifies how many times Cisco IOS XR software retransmits packets to a server before giving up.</td>
</tr>
<tr>
<td>radius-server timeout(BNG), on page 44</td>
<td>Sets the interval a router waits for a server host to reply.</td>
</tr>
</tbody>
</table>
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
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>value</code></td>
<td>Specifies the differentiated services codepoint value. The value ranges from 1 to 63.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Global Configuration mode</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Release 4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Usage Guidelines</th>
<th>No specific guidelines impact the use of this command.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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 in Global Configuration mode. To disable the key, use the `no` form of this command.

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

**Syntax Description**

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

- **7 encrypted-key clear-text-key**
  - Specifies an 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
-----------  ---------------------------
3.7.2        This command was introduced.
```

**Usage Guidelines**

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.

**Examples**

The following 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
```

The following 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
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>key (RADIUS)</td>
<td>Specifies the authentication and encryption key that is used between the router and the RADIUS daemon running on the RADIUS server.</td>
</tr>
<tr>
<td>server-private (RADIUS)</td>
<td>Configures the IP address of the private RADIUS server for the group server.</td>
</tr>
</tbody>
</table>
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}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>method</code></td>
<td>Specifies the method by which the next host will be picked.</td>
</tr>
<tr>
<td><code>least-outstanding</code></td>
<td>Picks the server with the least transactions outstanding.</td>
</tr>
<tr>
<td><code>batch-size</code></td>
<td>Specifies the batch size for the selection of the server.</td>
</tr>
<tr>
<td><code>value</code></td>
<td>Specifies the batch size value. The value ranges from 1 to 1500. The default is 25.</td>
</tr>
<tr>
<td><code>ignore-preferred-server</code></td>
<td>Disables the preferred server for this server group.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Examples**

This is an example of configuring the `radius-server load-balance` command in the Global Configuration mode:

```
RP/0/RSP0/CPU0#radius-server load-balance method least-outstanding batch-size 25
RP/0/RSP0/CPU0#radius-server load-balance method least-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 in Global Configuration mode. To disable retransmission, use the `no` form of this command.

```
radius-server retransmit retries
```

**Syntax Description**
- `retries`  Maximum number of retransmission attempts. The range is from 1 to 100. Default is 3.

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

**Command Modes**
Global Configuration mode

**Command History**
- Release 3.7.2 This command was introduced.

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

**Examples**
The following 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>radius-server key(BNG), on page 39</code></td>
<td>Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.</td>
</tr>
<tr>
<td><code>retransmit (RADIUS)</code></td>
<td>Specifies the number of times a RADIUS request is resent to a server if the server is not responding or is responding slowly.</td>
</tr>
<tr>
<td><code>server-private (RADIUS)</code></td>
<td>Configures the IP address of the private RADIUS server for the group server.</td>
</tr>
</tbody>
</table>
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
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>extended</code></td>
</tr>
<tr>
<td>Specifies that the source-port can be extended to 50.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

**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 in Global Configuration mode. To restore the default, use the `no` form of this command.

```
radius-server timeout seconds
```

**Syntax Description**

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

**Command Default**

- 5 seconds

**Command Modes**

- Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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**

The following 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
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>radius-server key (BNG)</code>, on page 39</td>
<td>Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.</td>
</tr>
<tr>
<td><code>server-private (RADIUS)</code></td>
<td>Configures the IP address of the private RADIUS server for the group server.</td>
</tr>
<tr>
<td><code>timeout (RADIUS)</code></td>
<td>Specifies the number of seconds the router waits for the RADIUS server to reply before retransmitting.</td>
</tr>
</tbody>
</table>
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.

### Syntax Description
This command has no keywords or arguments.

### Command Default
None

### Command Modes
Global Configuration mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
No specific guidelines impact the use of this command.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

This is an example of configuring the `radius-server vsa attribute ignore unknown` command in the Global Configuration mode:

```
RP/0/RSP0/CP00: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}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>access</code></td>
<td>Controls the number of access requests sent to a radius server.</td>
</tr>
<tr>
<td><code>value</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>access-timeout</code></td>
<td>Specifies the number of timeouts exceeding which a throttled access request is dropped.</td>
</tr>
<tr>
<td><code>time</code></td>
<td>Specifies the number of timeouts for a transaction. The default value is 3.</td>
</tr>
<tr>
<td><code>accounting</code></td>
<td>Controls the number of accounting requests sent to a radius server.</td>
</tr>
<tr>
<td><code>acc_value</code></td>
<td>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.</td>
</tr>
</tbody>
</table>

### Command Default

None

### Command Modes

Global Configuration mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

No specific guidelines impact the use of this command.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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 in Global Configuration mode. 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-name [vrf vrf-id]
```

**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 3.7.2**: This command was introduced.

**Usage Guidelines**

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**

The following 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
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa group server tacacs+</td>
<td>Groups different RADIUS server hosts into distinct lists.</td>
</tr>
<tr>
<td>radius-server key(BNG), on page 39</td>
<td>Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>basic</td>
<td>Displays the data for AAA basic events.</td>
</tr>
<tr>
<td>errors</td>
<td>Displays the data for AAA client library errors.</td>
</tr>
<tr>
<td>file</td>
<td>Displays the specific file.</td>
</tr>
<tr>
<td>func</td>
<td>Displays the data for AAA function.</td>
</tr>
<tr>
<td>hexdump</td>
<td>Displays the traces in hexadecimal.</td>
</tr>
<tr>
<td>job</td>
<td>Displays the job ID.</td>
</tr>
<tr>
<td>last</td>
<td>Displays the last n entries.</td>
</tr>
<tr>
<td>location</td>
<td>Displays the card location.</td>
</tr>
<tr>
<td>reverse</td>
<td>Displays the latest traces first.</td>
</tr>
<tr>
<td>stats</td>
<td>Displays the statistics.</td>
</tr>
<tr>
<td>tailf</td>
<td>Displays the new traces as they were added.</td>
</tr>
<tr>
<td>unique</td>
<td>Displays the unique entries with counts.</td>
</tr>
<tr>
<td>verbose</td>
<td>Displays the internal debugging information.</td>
</tr>
<tr>
<td>wrapping</td>
<td>Displays the wrapping entries.</td>
</tr>
<tr>
<td></td>
<td>Displays the output modifiers.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accounting</td>
<td>Displays the RADIUS accounting data.</td>
</tr>
<tr>
<td>authentication</td>
<td>Displays the RADIUS authentication data.</td>
</tr>
<tr>
<td>dead-criteria</td>
<td>Displays the RADIUS dead-server detection criteria.</td>
</tr>
<tr>
<td>double-dip</td>
<td>Displays the RADIUS double-dip data.</td>
</tr>
<tr>
<td>location</td>
<td>Specifies the RADIUS instance location.</td>
</tr>
<tr>
<td>server-groups</td>
<td>Displays the RADIUS server group information.</td>
</tr>
<tr>
<td></td>
<td>Displays the output modifiers.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read</td>
</tr>
</tbody>
</table>

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 Detime: 0s Last Detime: 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/CP00>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**

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

**show radius (BNG)**
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 mode

**Command History**
```
Release  Modification
4.2.0     This command was introduced.
```

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**
```
Task  Operation
ID    
aaa   read
```

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Server IP address/UDP destination port for authentication requests/UDP destination port for accounting requests.</td>
</tr>
<tr>
<td>Deadtime</td>
<td>Length of time in minutes for a RADIUS server to remain marked dead.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Specifies the authentication details.</td>
</tr>
<tr>
<td>Automated TEST Stats</td>
<td>Specifies the total time taken for sending requests, total timeouts, and the response time.</td>
</tr>
</tbody>
</table>
statistics period service-accounting

To set collection period for statistics collectors, use the `statistics period service-accounting` command in Global Configuration mode or Admin Configuration mode. To disable this behavior, use the `no` form of this command.

```
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 mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>diag</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa accounting subscriber, on page 5</td>
<td>Creates an accounting list for subscriber accounting.</td>
</tr>
<tr>
<td>aaa accounting service, on page 3</td>
<td>Creates an accounting list for service accounting.</td>
</tr>
</tbody>
</table>
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.

To use commands of this module, 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 any command, contact your AAA administrator for assistance.

- ipv4 access-group (BNG), on page 58
- ipv4 access-list(BNG), on page 61
- ipv6 access-group(BNG), on page 63
- ipv6 access-list(BNG), on page 65
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]}
```

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

**Command Default**

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

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.2.0</td>
<td>This command was supported in the dynamic template configuration mode for BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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 the `dynamic-template` command in the Global Configuration mode (applicable only for BNG).

**Note**

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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>acl</td>
<td>read, write</td>
</tr>
<tr>
<td>network</td>
<td>read, write</td>
</tr>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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 interface configuration mode:

```
RP/0/RSP0/CPU0:router(config-if)# ipv4 access-group common acl-common acl-unique1 ingress
```
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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Name of the access list. Names cannot contain a space or quotation marks.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>No IPv4 access list is defined.</th>
</tr>
</thead>
</table>

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

Use the **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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>acl</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following 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-if)# 10 permit 192.168.34.0 0.0.0.255
RP/0/RSP0
/CPU0:router(config-if)# 20 permit 172.16.0.0 0.0.255.255
RP/0/RSP0
/CPU0:router(config-if)# 30 permit 10.0.0.0 0.255.255.255
RP/0/RSP0
```
/CPU0:router(config-if)# remark Block BGP traffic from 172.16 net.
RP/0/RSP0

/CP00:router(config-if)# deny tcp host 172.16.0.0 eq bgp host 192.168.202.203 range 1300 1400

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear access-list ipv4</td>
<td>Resets the IPv4 access list match counters.</td>
</tr>
<tr>
<td>deny (IPv4)</td>
<td>Sets the deny conditions for a named IPv4 access list.</td>
</tr>
<tr>
<td>ipv4 access-group</td>
<td>Filters incoming or outgoing IPv4 traffic on an interface.</td>
</tr>
<tr>
<td>permit (IPv4)</td>
<td>Sets the permit conditions for a named IPv4 access list.</td>
</tr>
<tr>
<td>remark (IPv4)</td>
<td>Inserts a helpful remark about an IPv4 access list entry.</td>
</tr>
<tr>
<td>resequence access-list ipv4</td>
<td>Changes the starting entry number of the first statement in an existing IPv4 access list, and the number by which subsequent statements are incremented.</td>
</tr>
<tr>
<td>show access-lists ipv4</td>
<td>Displays the contents of all current IPv4 access lists.</td>
</tr>
</tbody>
</table>
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]
```

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
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.

**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.
**ipv6 access-group(BNG)**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

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

```shell
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
```

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

```shell
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
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy access-list ipv6</td>
<td>Copies an existing IPv6 access list.</td>
</tr>
<tr>
<td>deny (IPv6)</td>
<td>Sets the deny conditions for an IPv6 access list.</td>
</tr>
<tr>
<td>ipv6 access-list(BNG), on page 65</td>
<td>Defines an IPv6 access list and enters IPv6 access list configuration mode.</td>
</tr>
<tr>
<td>permit (IPv6)</td>
<td>Sets conditions under which a packet passes a named IPv6 access list.</td>
</tr>
<tr>
<td>show ipv6 interface</td>
<td>Displays the usability status of interfaces configured for IPv6.</td>
</tr>
</tbody>
</table>
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 Global Configuration mode. To remove the access list, use the `no` form of this command.

```
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**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ipv6 access-list` command is similar to the `ipv4 access-list` command, except that it is IPv6-specific. The IPv6 access lists are used for traffic filtering based on source and destination addresses, IPv6 option headers, and optional, upper-layer protocol type information for finer granularity of control. IPv6 access lists are defined by using the `ipv6 access-list` command in 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.

Refer to the `deny (IPv6)` and `permit (IPv6)` commands for more information on filtering IPv6 traffic based on IPv6 option headers and optional, upper-layer protocol type information. 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.
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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>acl</td>
<td>read, write</td>
</tr>
<tr>
<td>ipv6</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following 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
/CP00:router(config)# ipv6 access-list list2
RP/0/RSP0
/CP00:router(config-ipv6-acl)# 10 deny fec0:0:0:2::/64 any
RP/0/RSP0
/CP00:router(config-ipv6-acl)# 20 permit any any
RP/0/RSP0
/CP00: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
/CP00:router(config)# interface gigabitethernet 0/2/0/2
RP/0/RSP0
/CP00:router(config-if)# ipv6 access-group list2 out
```
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.

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).

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny (IPv6)</td>
<td>Sets the deny conditions for an IPv6 access list.</td>
</tr>
<tr>
<td>permit (IPv6)</td>
<td>Sets permit conditions for an IPv6 access list.</td>
</tr>
<tr>
<td>remark (IPv6)</td>
<td>Inserts a helpful remark about an IPv6 access list entry.</td>
</tr>
</tbody>
</table>
ipv6 access-list(BNG)
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*.

To use commands of this module, 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 any command, contact your AAA administrator for assistance.

- address-range, on page 70
- exclude, on page 72
- network (BNG), on page 74
- prefix-length, on page 76
- prefix-range, on page 77
- pool vrf, on page 78
- pool ipv4, on page 80
- pool ipv6, on page 81
- utilization-mark, on page 82
- show pool ipv4 name, on page 84
- show pool ipv6 name, on page 88
- show pool vrf, on page 95
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  [block]
```

**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.
- `block` Dynamically blocks one of the networks in the address pool.

**Command Default**

None

**Command Modes**

Pool IPv4 configuration

Pool IPv6 configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.3.0</td>
<td>Support for IPv6 was added.</td>
</tr>
<tr>
<td>6.2.1</td>
<td>Modified the command to include <code>block</code> option.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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.

Dynamic soft pool migration as well as static IP address subscriber management work only if the identity change feature is enabled using `subscriber featurette identity-change` command. DHCP validates the IP address with DAPS and accordingly rejects the RENEW request from the client, only if the `block` command is enabled. For more details, refer DHCP soft pool migration feature in *Cisco ASR 9000 Series Aggregation Services Router Broadband Network Gateway Configuration Guide*.

**Task ID**

```
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>
```

This is an example of configuring the `address-range` command for IPv4 in the Global Configuration mode:

```
This is an example of configuring the `address-range` command for IPv6 in the Global Configuration mode:

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

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pool ipv4, on page 80</td>
<td>Enables distributed address pool service on ipv4.</td>
</tr>
<tr>
<td>pool vrf, on page 78</td>
<td>Enables distributed address pool service on vrf.</td>
</tr>
<tr>
<td>exclude, on page 72</td>
<td>Specifies a range of IP addresses that distributed address pool service should not assign to clients.</td>
</tr>
<tr>
<td>subscriber featurette identity-change, on page 566</td>
<td>Enables identity change for DHCP Remote-Id parameter, thereby allowing modification of the subscriber service</td>
</tr>
</tbody>
</table>
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.

```plaintext
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.3.0</td>
<td>Support for IPv6 was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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

```plaintext
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

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>pool ipv4, on page 80</td>
<td>Enables distributed address pool service on IPv4.</td>
</tr>
<tr>
<td></td>
<td>pool vrf, on page 78</td>
<td>Enables distributed address pool service on vrf.</td>
</tr>
<tr>
<td></td>
<td>network (BNG), on page 74</td>
<td>Specifies a set of addresses or prefixes inside a subnet.</td>
</tr>
</tbody>
</table>
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}
```

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.3.0</td>
<td>Support for IPv6 was added.</td>
</tr>
<tr>
<td></td>
<td>Support for IPv4 <code>default-router</code> was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>pool ipv4</code>, on page 80</td>
<td>Enables distributed address pool service on ipv4.</td>
</tr>
<tr>
<td><code>pool vrf</code>, on page 78</td>
<td>Enables distributed address pool service on vrf.</td>
</tr>
<tr>
<td><code>prefix-length</code>, on page 76</td>
<td>Specifies the length of the prefix that is assigned to the client.</td>
</tr>
</tbody>
</table>
**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
```

**Syntax Description**

| prefix_length | Specifies the length of the prefix. |

**Command Default**

None

**Command Modes**

Pool IPv6 configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pool ipv4, on page 80</td>
<td>Enables distributed address pool service on ipv4.</td>
</tr>
<tr>
<td>pool vrf, on page 78</td>
<td>Enables distributed address pool service on vrf.</td>
</tr>
<tr>
<td>network (BNG), on page 74</td>
<td>Specifies a set of addresses or prefixes inside a subnet.</td>
</tr>
</tbody>
</table>
**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}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>first_ipv6_range</code></td>
<td>Specifies the first IPv6 in the prefix range.</td>
</tr>
<tr>
<td><code>last_ipv6_range</code></td>
<td>Specifies the last IPv6 in the prefix range.</td>
</tr>
</tbody>
</table>

### Command Default

None

### Command Modes

Pool IPv6 configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pool ipv4, on page 80</td>
<td>Enables distributed address pool service on ipv4.</td>
</tr>
<tr>
<td>pool vrf, on page 78</td>
<td>Enables distributed address pool service on vrf.</td>
</tr>
<tr>
<td>prefix-length, on page 76</td>
<td>Specifies the length of the prefix that is assigned to the client.</td>
</tr>
</tbody>
</table>
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}
```

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

**Usage Guidelines**

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 cannot 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

This is an example of configuring the `pool vrf` command for IPv4 in the Global Configuration mode:
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)#

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pool ipv4, on page 80</td>
<td>Enables distributed address pool service on IPv4.</td>
</tr>
<tr>
<td>pool ipv6, on page 81</td>
<td>Enables distributed address pool service on IPv6.</td>
</tr>
</tbody>
</table>
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
```

**Syntax Description**

`pool_name` Specifies the name of the IPv4 pool.

**Command Default**

None

**Command Modes**

Global Configuration mode

**Command History**

Modification | Release  | Description
-------------|----------|--------------
This command was introduced. | 4.2.0     |

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pool vrf, on page 78</td>
<td>Enables distributed address pool service on vrf.</td>
</tr>
<tr>
<td>exclude, on page 72</td>
<td>Specifies a range of IP addresses that distributed address pool service should not assign to clients.</td>
</tr>
<tr>
<td>address-range, on page 70</td>
<td>Specifies a range of IP addresses.</td>
</tr>
</tbody>
</table>
**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
```

**Syntax Description**

- `pool_name`
  - Specifies the IPv6 pool name.

**Command Default**

None

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

- `ip-services read, write`

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pool vrf, on page 78</td>
<td>Enables distributed address pool service on vrf.</td>
</tr>
</tbody>
</table>
**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 }
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>high</code></td>
<td>Specifies the high mark in the threshold value.</td>
</tr>
<tr>
<td><code>high_value</code></td>
<td>Specifies the numerical value as percentage, for the low mark in the threshold.</td>
</tr>
<tr>
<td><code>low</code></td>
<td>Specifies the low mark in the threshold value.</td>
</tr>
<tr>
<td><code>low_value</code></td>
<td>Specifies the numerical value as percentage, for the low mark in the threshold.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Pool IPv4 configuration

Pool IPv6 configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.2.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.3.0</td>
<td>Support for IPv6 was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>pool ipv4, on page 80</code></td>
<td>Enables distributed address pool service on ipv4.</td>
</tr>
<tr>
<td><code>pool vrf, on page 78</code></td>
<td>Enables distributed address pool service on vrf.</td>
</tr>
<tr>
<td><code>exclude, on page 72</code></td>
<td>Specifies a range of IP addresses that distributed address pool service should not assign to clients.</td>
</tr>
</tbody>
</table>
**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.

**Command Default**
None

**Command Modes**
EXEC mode

**Command History**

```
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.2.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.3.0</td>
<td>Support for IPv6 was added.</td>
</tr>
</tbody>
</table>
```

**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**

```
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read</td>
</tr>
</tbody>
</table>
```

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

Broadband Network Gateway Command Reference for Cisco ASR 9000 Series Routers
<table>
<thead>
<tr>
<th>Address</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0.0.31</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.32</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.33</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.34</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.35</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.36</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.37</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.38</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.39</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.40</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.41</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.42</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.43</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.44</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.45</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.46</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.47</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.48</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.49</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.50</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.51</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.52</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.53</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.54</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.55</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.56</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.57</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.58</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.59</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.60</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.61</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.62</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.63</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.64</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.65</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.66</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.67</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.68</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.69</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.70</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.71</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.72</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.73</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.74</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.75</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.76</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.77</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.78</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.79</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.80</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.81</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.82</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.83</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.84</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.85</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.86</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.87</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.88</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.89</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.90</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.91</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.92</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.93</td>
<td>PPP</td>
</tr>
<tr>
<td>12.0.0.94</td>
<td>PPP</td>
</tr>
</tbody>
</table>
This table describes the significant fields shown in the display.

Table 4: `show pool ipv4 name` Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF</td>
<td>Specifies the VRF the pool is associated with.</td>
</tr>
<tr>
<td>Pool ID</td>
<td>The unique pool ID of a specific pool.</td>
</tr>
<tr>
<td>Pool Scope</td>
<td>Pool scope belongs to the VRF specific pool.</td>
</tr>
<tr>
<td>Prefix Length</td>
<td>Length of the prefix specified.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pool vrf, on page 78</td>
<td>Enables distributed address pool service on vrf.</td>
</tr>
<tr>
<td>pool ipv4, on page 80</td>
<td>Enables distributed address pool service on ipv4.</td>
</tr>
<tr>
<td>exclude, on page 72</td>
<td>Specifies a range of IP addresses that distributed address pool service should not assign to clients.</td>
</tr>
<tr>
<td>address-range, on page 70</td>
<td>Specifies a range of IP addresses.</td>
</tr>
</tbody>
</table>
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 mode

**Command History**
- `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
```

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

```
RP/0/RSP0/CPU0:router# show pool ipv6 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
<table>
<thead>
<tr>
<th>IPv6 Address</th>
<th>Service Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>19::23</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::24</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::25</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::26</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::27</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::28</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::29</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::2a</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::2b</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::2c</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::2d</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::2e</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::2f</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::30</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::31</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::32</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::33</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::34</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::35</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::36</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::37</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::38</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::39</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::3a</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::3b</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::3c</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::3d</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::3e</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::3f</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::40</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::41</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::42</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::43</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::44</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::45</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::46</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::47</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::48</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::49</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::4a</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::4b</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::4c</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::4d</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::4e</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::4f</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::50</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::51</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::52</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::53</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::54</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::55</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::56</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::57</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::58</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::59</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::5a</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::5b</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::5c</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::5d</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::5e</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::5f</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::60</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::61</td>
<td>DHCPv6</td>
</tr>
<tr>
<td>19::62</td>
<td>DHCPv6</td>
</tr>
</tbody>
</table>
Address Pool Service Commands

show pool ipv6 name
show pool ipv6 name
| 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::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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF</td>
<td>Specifies the VRF the pool is associated with.</td>
</tr>
<tr>
<td>Pool ID</td>
<td>The unique pool ID of a specific pool.</td>
</tr>
<tr>
<td>Pool Scope</td>
<td>Pool scope belongs to the VRF specific pool.</td>
</tr>
<tr>
<td>Prefix Length</td>
<td>Length of the prefix specified.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pool vrf, on page 78</td>
<td>Enables distributed address pool service on vrf.</td>
</tr>
<tr>
<td>pool ipv6, on page 81</td>
<td>Enables distributed address pool service on ipv6.</td>
</tr>
<tr>
<td>exclude, on page 72</td>
<td>Specifies a range of IP addresses that distributed address pool service should not assign to clients.</td>
</tr>
<tr>
<td>address-range, on page 70</td>
<td>Specifies a range of IP addresses.</td>
</tr>
</tbody>
</table>
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 mode

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.2.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.3.0</td>
<td>Support for IPv6 was added.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read</td>
</tr>
</tbody>
</table>

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%
```
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

<table>
<thead>
<tr>
<th>Used</th>
<th>Excl</th>
<th>Free</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0</td>
<td>31999</td>
<td>32001</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0%</td>
</tr>
</tbody>
</table>

```
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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF</td>
<td>Specifies the VRF the pool is associated with.</td>
</tr>
<tr>
<td>Pool ID</td>
<td>The unique pool ID of a specific pool.</td>
</tr>
<tr>
<td>Pool Name</td>
<td>The name of the IPv6 pool.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pool vrf, on page 78</td>
<td>Enables distributed address pool service on vrf.</td>
</tr>
<tr>
<td>pool ipv4, on page 80</td>
<td>Enables distributed address pool service on ipv4.</td>
</tr>
<tr>
<td>exclude, on page 72</td>
<td>Specifies a range of IP addresses that distributed address pool service should not assign to clients.</td>
</tr>
<tr>
<td>address-range, on page 70</td>
<td>Specifies a range of IP addresses.</td>
</tr>
</tbody>
</table>
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.

To use commands of this module, 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 any command, contact your AAA administrator for assistance.

- activate, on page 98
- authenticate (BNG), on page 100
- authorize, on page 101
- class-map type control subscriber, on page 103
- deactivate, on page 104
- decode, on page 106
- event, on page 107
- match (class-map), on page 110
- match option (DHCPv6), on page 112
- policy-map type control subscriber, on page 114
- policy-map type pbr, on page 115
- service-policy type control subscriber, on page 116
- show class-map, on page 117
- show policy-map, on page 119
activate

To activate the dynamic template in the class map sub-configuration mode, use the `activate` command. To deactivate the dynamic template, use the `deactivate` command.

`activate dynamic-template {name aaa list {list_name|default}} service-from-line`  

**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.
- `service-from-line`: Activates the service encoded in the DHCP Remote-Id parameter.

**Command Default**

None

**Command Modes**

Class map sub-configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>6.2.1</td>
<td>Modified the command to include <code>service-from-line</code> option.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You must configure `decode` command to decode (as per the defined AAA attribute format) the service encoded in the DHCP Remote-Id parameter. This particular service is the one referred as `service-from-line` in this context.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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

This is an example of activating the service that was encoded in the DHCP Remote-Id parameter:

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 do-until-failure
RP/0/RSP0/CPU0:router(config-pmap-c)# 1 decode remote-id format my-format
RP/0/RSP0/CPU0:router(config-pmap-c)# 2 activate dynamic-template service-from-line
RP/0/RSP0/CPU0:router(config-pmap-c)# 3 authorize aaa list default identifier remote-id password blank

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deactivate, on page 104</td>
<td>Deactivates the dynamic template mode in the class map sub-configuration mode.</td>
</tr>
<tr>
<td>decode, on page 106</td>
<td>Decodes DHCP parameter based on the defined AAA attribute format.</td>
</tr>
</tbody>
</table>
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}
```

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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}})
```

**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 username 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.
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-c)# 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
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>class-map name</code></td>
<td>Specifies the class map name.</td>
</tr>
<tr>
<td><code>match-all</code></td>
<td>Configures the match all criteria for this class.</td>
</tr>
<tr>
<td><code>match-any</code></td>
<td>Configures the match any criteria for this class.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

From Cisco IOS XR Software Release 5.2.2 and later, you can edit the class associated with the subscriber policy even while the sessions are active. Prior to this, new class map actions were not editable if the sessions were up, and any such dynamic policy-map changes resulted in clearing off the subscriber sessions.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>policy-map type control subscriber</code></td>
<td>Enables the policy-map.</td>
</tr>
<tr>
<td><code>event</code></td>
<td>Enables the event in a policy-map.</td>
</tr>
</tbody>
</table>
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}|service-from-line}
```

### 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.
- **service-from-line**: Deactivates the service encoded in the DHCP Remote-Id parameter.

### Command Default

None

### Command Modes

Global Configuration mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>6.2.1</td>
<td>Modified the command to include <code>service-from-line</code> option.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

You must configure `decode` command to decode (as per the defined AAA attribute format) the service encoded in the DHCP Remote-Id parameter. This particular service is the one referred as `service-from-line` in this context.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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-c)# class type control subscriber CL2
RP/0/RSP0/CPU0:router(config-pmap-c)# 1 deactivate dynamic-template DL1 aaa list default
```
This is an example of deactivating an old service and activating the new service that was encoded in the DHCP Remote-id parameter:

```plaintext
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-identity-change match-first
RP/0/RSP0/CPU0:router(config-pmap-e)# class type control subscriber CL2 do-until-failure
RP/0/RSP0/CPU0:router(config-pmap-c)# 1 decode remote-id format my-format
RP/0/RSP0/CPU0:router(config-pmap-c)# 2 deactivate dynamic-template service-from-line
RP/0/RSP0/CPU0:router(config-pmap-c)# 3 activate dynamic-template service-from-line
RP/0/RSP0/CPU0:router(config-pmap-c)# 4 authorize aaa list default identifier remote-id password blank
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>activate, on page 98</td>
<td>Activates the dynamic template mode in the class map sub-configuration mode.</td>
</tr>
<tr>
<td>decode, on page 106</td>
<td>Decodes DHCP Remote-Id parameter based on the defined AAA attribute format.</td>
</tr>
</tbody>
</table>
To decode the DHCP parameter based on the defined AAA attribute format, use the `decode` command in policy-map event class configuration mode. To disable this feature, use the `no` form of this command.

```
decode identity format format-name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>identity</code></td>
<td>Specifies the DHCP parameter to be decoded.</td>
</tr>
<tr>
<td><code>format format-name</code></td>
<td>Specifies the AAA attribute format based on which the DHCP parameter is to be decoded.</td>
</tr>
</tbody>
</table>

**Note**

Currently, only Remote-Id or Circuit-Id parameter is supported for decoding.

**Command Default**

None

**Command Modes**

Policy-map event class configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to decode the DHCP Remote-Id parameter based on the defined AAA attribute format:

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)#aaa attribute format my-format format-string length 253 "\^[}\|[}\^[\[}|" username service-name
RP/0/RSP0/CPU0:router(config)#policy-map type control subscriber S1
RP/0/RSP0/CPU0:router(config-pmap)#event session-start match-first
RP/0/RSP0/CPU0:router(config-pmap-c)#class type control subscriber CL1 do-until-failure
RP/0/RSP0/CPU0:router(config-pmap-c)#1 decode remote-id format my-format
RP/0/RSP0/CPU0:router(config-pmap-c)#2 activate dynamic-template service-from-line
RP/0/RSP0/CPU0:router(config-pmap-c)#3 authorize aaa list default identifier remote-id password blank
```
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.

```plaintext
```

### Syntax Description

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>account-logoff</td>
<td>Specifies an account logoff event.</td>
</tr>
<tr>
<td>account-logon</td>
<td>Specifies an account logon event.</td>
</tr>
<tr>
<td>authenticate-dhcp-renew</td>
<td>Specifies the session renewal event.</td>
</tr>
<tr>
<td>authentication-failure</td>
<td>Specifies an authentication failure event.</td>
</tr>
<tr>
<td>authentication-no-response</td>
<td>Specifies an authentication no response event.</td>
</tr>
<tr>
<td>authorization-failure</td>
<td>Specifies an authorization failure event.</td>
</tr>
<tr>
<td>authorization-no-response</td>
<td>Specifies an authorization no response event.</td>
</tr>
<tr>
<td>exception</td>
<td>Specifies a service rollback failure event due to a multi-action CoA (MA - CoA) request failure.</td>
</tr>
<tr>
<td>idle-timeout</td>
<td>Specifies an idle timeout event.</td>
</tr>
<tr>
<td>service-start</td>
<td>Specifies a service start event.</td>
</tr>
<tr>
<td>service-stop</td>
<td>Specifies a service stop event.</td>
</tr>
<tr>
<td>session-activate</td>
<td>Specifies session activate event.</td>
</tr>
<tr>
<td>session-identity-change</td>
<td>Specifies an identity change event.</td>
</tr>
<tr>
<td>session-start</td>
<td>Specifies session start event.</td>
</tr>
<tr>
<td>session-stop</td>
<td>Specifies session start event.</td>
</tr>
<tr>
<td>timer-expiry</td>
<td>Specifies the timer expiry event.</td>
</tr>
</tbody>
</table>

### Command Default

None

### Command Modes

Policy-map configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
The idle-timeout event was added. **Release 5.1**

The exception event was added for service rollback failure due to multi-action CoA request failure. **Release 5.2.0**

The command was modified to include session-identity-change event, for controlling subscriber plans using protocol options. **Release 6.2.1**

The command was modified to include authenticate-dhcp-renew event, that enables AAA authorization feature at the time of session lease renewal. **Release 6.4.1**

**Usage Guidelines**

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.

The exception event with the action as `disconnect`, specifies that the subscriber sessions be removed when a service rollback fails due to a multi-action Coa (MA-CoA) request failure. The default action is to retain the session.

For more details on authenticate-dhcp-renew event, see the Establishing Subscriber Sessions chapter in the Cisco ASR 9000 Series Aggregation Services Router Broadband Network Gateway Configuration Guide.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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

```
RP/0/RSP0/CPU0:router(config)# policy-map type control subscriber poll
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-untill-failure
RP/0/RSP0/CPU0:router(config-cmap-c)# 1 activate dynamic-template ip_temp
dhcp_id_format password xya
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 poll
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
```

This example shows how to configure the exception event in policy configuration mode, with the action as `disconnect`:

```
RP/0/RSP0/CPU0:router(config)# policy-map type control subscriber poll
RP/0/RSP0/CPU0:router(config-pmap)# event exception
RP/0/RSP0/CPU0:router(config-pmap-e)# class type control subscriber ip_dhcp
RP/0/RSP0/CPU0:router(config-cmap-c)# 1 disconnect
```
RP/0/RSP0/CPU0:router(config-pmap)# event exception match-first
event session-identity-change match-first
RP/0/RSP0/CPU0:router(config-pmap-e)# class type control subscriber coa-rollback-failure
do-all
class type control subscriber CL2 do-until-failure
10 disconnect
RP/0/RSP0/CPU0:router(config-pmap-c)#
RP/0/RSP0/CPU0:router(config-pmap-c)#
RP/0/RSP0/CPU0:router(config-pmap-c)# 10 disconnect

This example shows how to handle identity change of DHCP Remote-id parameter, to enable
modification of subscriber service. For more details, refer the section on controlling subscriber plans
using protocol options, inCisco ASR 9000 Series Aggregation Services Router Broadband Network
Gateway Configuration Guide.

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 authenticate-dhcp-renew match-all
RP/0/RSP0/CPU0:router(config-pmap-e)# authorize aaa list default identifier remote-id
table
RP/0/RSP0/CPU0:router(config-pmap-c)#
RP/0/RSP0/CPU0:router(config-pmap-c)#
RP/0/RSP0/CPU0:router(config-pmap-c)#
RP/0/RSP0/CPU0:router(config-pmap-c)#

This example shows how to enable AAA authorization on DHCP RENEW or REBIND:

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# policy-map type control subscriber dhcpv4_policy
RP/0/RSP0/CPU0:router(config-pmap)# event authenticate-dhcp-renew match-all
RP/0/RSP0/CPU0:router(config-pmap-e)# authorize aaa list default identifier remote-id

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>class-map type control subscriber, on page 103</td>
<td>Enables the class-map.</td>
</tr>
<tr>
<td>policy-map type control subscriber, on page 114</td>
<td>Enables the policy-map.</td>
</tr>
</tbody>
</table>
**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|regexp string } | format format_name | not | protocol { dhcpv4|dhcpv6 } | service-name { service-name|regexp string } | source-address { ipv4|mac } | timer { string|regexp string } | username { string|regexp string } }
```

**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.
- `service-name` Specifies the service name.
- `source-address` Service name as a string.
- `timer` Specifies the timer.
- `username` Specifies the name of the user.

**Command Default**

None

**Command Modes**

Class-map configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
The command was modified to add new keyword, `service-name`.

**Usage Guidelines**

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

These are the usage guidelines for `match service-name`:

- It works only for service activations through CoA. For services defined in dynamic-template and activated by `action` in policy-maps, the service-activate event is not enabled, and a class map with `match service-name` is not useful in that case.

- It does not work in multi-action CoA (MA-CoA) where multiple services are enabled by a single CoA request.

- The order of configuration must be such that, the `match service-name` is configured in a class-map and then the class-map is linked in the policy-map. The class-map must ideally be placed to match during a service-start or service-stop event, where the service being started or stopped matches to the service names configured in the class-map. With other events, the class-map with match service-name is irrelevant.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos</td>
<td></td>
<td>read, write</td>
</tr>
</tbody>
</table>

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

```plaintext
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
```

This is an example of configuring the `service-name` matching in the class-map (type subscriber) configuration mode:

```plaintext
RP/0/RSP0/CPU0:router(config)# class-map type control subscriber match-any match-svc
RP/0/RSP0/CPU0:router(config-cmap)# match service-name idle-to
RP/0/RSP0/CPU0:router(config-cmap)# match service-name regexp id*
RP/0/RSP0/CPU0:router(config-cmap)# match service-name regexp .*
```
match option (DHCPv6)

To enable DHCP option 16 filtering feature in BNG, use the `match option enterprise-id` or `match option vendor-class` or both commands in DHCP IPv6 server profile configuration mode. To disable this feature, use the `no` form of this command.

```
machine option enterprise-id {default|hex hex-string} action {allow|drop}
machine option enterprise-id {default|string string-value} action {allow|drop}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Defines a default behavior for incoming DHCP SOLICIT packets.</td>
</tr>
<tr>
<td>hex hex-string</td>
<td>Specifies the hexadecimal pattern of enterprise-ID in the DHCP option 16 to be matched.</td>
</tr>
<tr>
<td>string string-value</td>
<td>Specifies the string value of vendor-class data in the DHCP option 16 to be matched.</td>
</tr>
<tr>
<td>action</td>
<td>Specifies the action to be performed on DHCP SOLICIT packets.</td>
</tr>
<tr>
<td>allow</td>
<td>Allows the DHCP SOLICIT packets based on the DHCP option 16 information.</td>
</tr>
<tr>
<td>drop</td>
<td>Drops the DHCP SOLICIT packets based on the DHCP option 16 information.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

DHCP IPv6 server profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.4.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

These configurations are invalid and are not supported:

- `match vendor-class-data default action drop`
- `match enterprise-ID default action allow`

- `match vendor-class-data default action allow`
- `match enterprise-ID default action drop`

- `match vendor-class-data default action drop`
This example shows how to enable DHCPv6 option 16 filtering feature in BNG. In this example, the BNG router drops all the DHCP SOLICIT packets by default, except the ones that are explicitly configured to be allowed.

```
RP/0/RSP0/CPU0:router(configure)# dhcp ipv6
RP/0/RSP0/CPU0:router(config-dhcpv6)# profile server_profile server
RP/0/RSP0/CPU0:router(config-dhcpv6-server-profile)# match vendor-class-data string "ABC*" action allow
RP/0/RSP0/CPU0:router(config-dhcpv6-server-profile)# match enterprise-ID hex FFF action allow
RP/0/RSP0/CPU0:router(config-dhcpv6-server-profile)# match vendor-class-data default action drop
RP/0/RSP0/CPU0:router(config-dhcpv6-server-profile)# match enterprise-ID default action drop
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>duid allowed-type, on page 143</td>
<td>Specifies the permitted DUID type for the incoming DHCP SOLICIT packets, as part of enabling DHCP option 16 filtering feature in BNG.</td>
</tr>
</tbody>
</table>
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
```

**Syntax Description**

- `policy-map name` Represents the policy map name.

**Command Default**

None

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

From Cisco IOS XR Software Release 5.2.2 and later, you can edit the class associated with the subscriber policy even while the sessions are active. Prior to this, new class map actions were not editable if the sessions were up, and any such dynamic policy-map changes resulted in clearing off the subscriber sessions.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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 poll
RP/0/RSP0/CPU0:router(config-cmap-c)# end-policy-map
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>class-map type control subscriber</code>, on page 103</td>
<td>Enables the class-map.</td>
</tr>
<tr>
<td><code>event</code>, on page 107</td>
<td>Enables the event in the policy-map.</td>
</tr>
</tbody>
</table>
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
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>policy-map name</code> Represents the policy map name.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>class-map type control subscriber, on page 103</td>
<td>Enables the class-map.</td>
</tr>
<tr>
<td>event, on page 107</td>
<td>Enables the event in the policy-map.</td>
</tr>
</tbody>
</table>
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
```

**Syntax Description**
- `name`: Represents the policy map name.

**Command Default**
None

**Command Modes**
Interface configuration mode

**Command History**

Release   Modification
4.2.0      This command was introduced.

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>class-map type control subscriber, on page 103</td>
<td>Enables the class-map.</td>
</tr>
<tr>
<td>event, on page 107</td>
<td>Enables the event in the policy-map.</td>
</tr>
</tbody>
</table>
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
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>Displays the type of classmap.</td>
</tr>
<tr>
<td>control</td>
<td>Displays all the control class maps.</td>
</tr>
<tr>
<td>subscriber</td>
<td>Displays all the subscriber control class maps.</td>
</tr>
<tr>
<td>name</td>
<td>Displays the class map name.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>EXEC mode</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

| Usage Guidelines     | No specific guidelines impact the use of this command. |

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos</td>
<td>read</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ClassMap</td>
<td>Specifies the class map name.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the type of the class map.</td>
</tr>
</tbody>
</table>
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>class-map type control subscriber, on page 103</td>
<td>Determines the list of actions to be executed for the class and enters the class-map configuration mode.</td>
</tr>
</tbody>
</table>
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
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>Displays the type of policy-map.</td>
</tr>
<tr>
<td>control</td>
<td>Displays the control type policy-map.</td>
</tr>
<tr>
<td>subscriber</td>
<td>Displays the subscriber control type policy-map.</td>
</tr>
<tr>
<td>pmap_name</td>
<td>Specifies the policy-map name.</td>
</tr>
<tr>
<td>name</td>
<td>Displays the policy map name.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>EXEC mode</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

| Usage Guidelines    | No specific guidelines impact the use of this command. |

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos</td>
<td>read</td>
</tr>
</tbody>
</table>

This table describes the significant fields shown in the display.

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

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
        ! activate dynamic-template PPP_PTA_TEMPLATE
    !
    end-policy-map
!
```

The show policy-map output is as follows:

```
```

This table describes the significant fields shown in the display.
### Table 8: show policy-map Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy-map</td>
<td>Specifies the policy map name.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the type of the class type control subscriber.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy-map type control subscriber, on page 114</td>
<td>Determines the list of events that are applicable to the subscriber lifecycle and to enter the policy-map configuration mode.</td>
</tr>
</tbody>
</table>
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*.

To use commands of this module, 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 any command, contact your AAA administrator for assistance.

- aaa dhcp-option force-insert, on page 123
- address-pool, on page 124
- afr-name, on page 125
- authentication username, on page 126
- broadcast-flag policy check (BNG), on page 128
- class, on page 130
- delayed authentication, on page 132
- dhcp ipv4 (BNG), on page 133
- dhcp ipv6 (BNG), on page 134
- dhcp-to-aaa option list, on page 135
- dhcpv6-to-aaa option list, on page 136
- dhcpv6 address-pool, on page 137
- dhcpv6 delegated-prefix-pool, on page 138
- dns-server (BNG), on page 139
- domain-name (DHCP IPv6 pool-BNG), on page 141
- duid allowed-type, on page 143
- duplicate-mac-allowed, on page 144
- framed-prefix-pool, on page 146
- giaddr policy keep, on page 147
- helper-address (BNG), on page 148
- inner-cos, on page 150
- interface (DHCP-BNG), on page 152
- interface subscriber-pppoe profile, on page 154
- lease, on page 155
- lease proxy client-lease-time, on page 157
- linkaddress-from-ra-enable, on page 158
• limit lease per-circuit-id, on page 160
• limit lease per-interface, on page 161
• limit lease per-remote-id, on page 162
• match-default, on page 163
• match mode-class, on page 165
• match option, on page 167
• match option 60, on page 169
• match vrf, on page 171
• option 17, on page 172
• outer-cos, on page 173
• prefix-pool, on page 174
• profile (BNG), on page 175
• rapid commit, on page 177
• relay information authenticate (BNG), on page 178
• relay information check (BNG), on page 180
• relay information option (BNG), on page 182
• relay information option allow-untrusted (BNG), on page 184
• relay information policy (BNG), on page 186
• relay option interface-id, on page 188
• relay option link-layer-addr, on page 190
• relay option remote-id, on page 191
• relay option subscriber-id, on page 193
• show dhcp ipv4 proxy binding, on page 194
• show dhcp ipv4 proxy interface (BNG), on page 198
• show dhcp ipv4 proxy profile, on page 200
• show dhcp ipv4 proxy statistics, on page 201
• show dhcp ipv6 proxy binding (BNG), on page 202
• show dhcp ipv6 proxy interface (BNG), on page 204
• show dhcp ipv6 proxy profile, on page 206
• show dhcp ipv6 proxy statistics, on page 207
• show dhcp ipv6 server binding, on page 209
• show dhcp ipv6 server interface, on page 212
• show dhcp ipv6 server profile, on page 214
• show dhcp ipv6 server statistics, on page 215
aaa dhcp-option force-insert

To enable the insertion of DHCP options while replying to the DHCP client, regardless of the request from the DHCP host, use the `aaa dhcp-option force-insert` command in DHCP IPv4 or IPv6 server profile configuration mode. To disable this functionality, use the `no` form of this command.

### Syntax Description
This command has no keywords or arguments.

### Command Default
None

### Command Modes
- DHCP IPv4 server profile
- DHCP IPv6 server profile

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.4.1</td>
<td>The command was extended for DHCP IPv6 server profile configuration mode.</td>
</tr>
<tr>
<td>Release 6.1.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
If DHCP server profile is configured on BNG, the per-subscriber-based DHCP options get preference over that.

You can configure a maximum of 8 DHCPv6 options for a single user profile. The AAA server can send a maximum of 120 hexadecimal bytes and 240 ASCII characters (approximately) to the BNG router.

For more information on Rich DHCP Option on RADIUS VSA feature, see the *Establishing Subscriber Sessions* chapter in the *Cisco ASR 9000 Series Aggregation Services Router Broadband Network Gateway Configuration Guide*.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to enable rich DHCP option feature on BNG:

```
RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)# aaa dhcp-option force-insert
```
address-pool

To specify the name of an address pool by integrating the DHCPv6 server 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
```

**Syntax Description**
- `pool_name` Specifies the name of a address pool.

**Command Default**
None

**Command Modes**
- DHCP IPv6 server profile class configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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**

- `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
```
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
```

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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
```
authentication username

To specify the username format of IPv4 or IPv6 subscriber for authentication with the AAA server (as part of enabling DHCP L3 snoop feature in BNG), use the **authentication username** command in DHCP IPv4 (or IPv6) proxy profile configuration mode. To remove this configuration, use the **no** form of this command.

For IPv4:

```
authentication username {giaddr|mac}
```

For IPv6:

```
authentication username DUID
```

**Syntax Description**

- **giaddr**: Specifies gateway address as the username for IPv4 subscriber. A combination of gateway address and MAC address is used as the authorization username to enable DHCP L3 snooping in BNG.
- **mac**: Specifies MAC address as the username for IPv4 subscriber.
- **DUID**: Specifies DUID as the username for IPv6 subscriber.

**Command Default**

None

**Command Modes**

DHCP IPv4 proxy profile

DHCP IPv6 proxy profile

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This is supported only on Cisco IOS XR 64-bit operating system.

The **DUID** option is applicable only for IPv6 subscribers, and is available only in DHCP IPv6 proxy profile configuration mode. Similarly, the **giaddr** and **mac** options are applicable only for IPv4 subscribers, and are available only in DHCP IPv4 proxy profile configuration mode.

The **DUID** option is mainly useful in routed DHCPv6-initiated sessions in case the MAC information is not available to BNG through DHCP Option 79.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to specify the MAC address-gateway address combination as the authorization username of IPv4 subscriber, to enable DHCP L3 snoop feature in BNG:
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>delayed authentication, on page 132</td>
<td>Delays the client authorization until DHCP REQUEST message is received from the client.</td>
</tr>
</tbody>
</table>
To configure Dynamic Host Configuration Protocol (DHCP) IPv4 Relay to broadcast only BOOTREPLY packets if the DHCP IPv4 broadcast 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 }
```

**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 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**
No specific guidelines impact the use of this command.

**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
```
**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp ipv4 (BNG), on page 133</td>
<td>Enables DHCP for IPv4 and enters DHCP IPv4 configuration mode.</td>
</tr>
<tr>
<td>helper-address</td>
<td>Configures the DHCP relay agent to relay packets to a specific DHCP server.</td>
</tr>
<tr>
<td>relay information check (BNG), on page 180</td>
<td>Configures a DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.</td>
</tr>
<tr>
<td>relay information option (BNG), on page 182</td>
<td>Enables the system to insert a DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.</td>
</tr>
<tr>
<td>relay information option allow-untrusted (BNG), on page 184</td>
<td>Configures the DHCP component to not drop BOOTREQUEST messages that have the relay information option set and the giaddr set to zero.</td>
</tr>
<tr>
<td>relay information policy (BNG), on page 186</td>
<td>Configures how a relay agent processes BOOTREQUEST messages that already contain a relay information option.</td>
</tr>
</tbody>
</table>
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}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>class_name</code></td>
<td>Specifies the class name.</td>
</tr>
<tr>
<td><code>helper-address</code></td>
<td>Specifies the server address to relay packets.</td>
</tr>
<tr>
<td><code>match</code></td>
<td>Inserts a match keyword.</td>
</tr>
<tr>
<td><code>address-pool</code></td>
<td>Specifies the name of the address pool.</td>
</tr>
<tr>
<td><code>dns-server</code></td>
<td>Specifies the name of a dns server.</td>
</tr>
<tr>
<td><code>domain-name</code></td>
<td>Specifies the name of a domain.</td>
</tr>
<tr>
<td><code>prefix-pool</code></td>
<td>Specifies the name of the prefix pool.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.3.0</td>
<td>The support for IPv6 was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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.
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
```
delayed authentication

To delay the client authorization until DHCP REQUEST message is received from the client, use the `delayed authentication` command in DHCP IPv4 proxy profile configuration mode. This is used while enabling DHCP L3 snooping feature in BNG. To disable this configuration, use the `no` form of this command.

### Syntax Description
This command has no keywords or arguments.

### Command Default
None

### Command Modes
DHCP IPv4 proxy profile

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
This command is supported only for DHCPv4; not for DHCPv6. Also, it is supported only on Cisco IOS XR 64-bit operating system.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to delay the client authorization while enabling DHCP L3 snooping in BNG:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# profile example-profile proxy
RP/0/RSP0/CPU0:router(config-dhcpv4-proxy-profile)# delayed authentication
RP/0/RSP0/CPU0:router(config-dhcpv4-proxy-profile)# commit
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication username, on page 126</td>
<td>Specifies the username format of IPv4 or IPv6 subscriber for authentication with the AAA server, as part of enabling DHCP L3 snoop feature in BNG.</td>
</tr>
</tbody>
</table>
**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
```

**Syntax Description**
This command has no keywords or arguments.

**Command Modes**
- None
- Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.2.0</td>
<td>This command was supported for BNG.</td>
</tr>
</tbody>
</table>

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

**Task ID**
- Operations: 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)#
```
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
```

**Syntax Description**

This command has no keywords or arguments.

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.1.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.3.0</td>
<td>This command was supported for BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the *dhcp ipv6* command to enter DHCP IPv6 configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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)#
```
dhcp-to-aaa option list

To enable control over the subscriber DHCP options to be sent to the AAA server by the BNG router, use the `dhcp-to-aaa option list` command in DHCP IPv4 server profile or proxy profile configuration mode. To disable this feature, use the `no` form of this command.

```
dhcp-to-aaa option list {all option-value}
```

**Syntax Description**
- `all` Enables the functionality to send all DHCPv4 options from the subscriber to the AAA server.
- `option-value` Specifies the particular DHCPv4 options from the subscriber to be sent to the AAA server.

**Command Default**
None

**Command Modes**
- DHCP IPv4 proxy profile
- DHCP IPv4 server profile

**Command History**

Release 6.4.1 This command was introduced.

**Usage Guidelines**
The BNG router sends all or the specified DHCPv4 options to the AAA server, if this command is configured. You can send a maximum of 13 options (12 DHCP options and a DHCP header) to the AAA server. The header portion of the DHCP control packet is encoded as option type 0. The first 108 bytes of the header are sent to the AAA server.

**Task ID**
- `ip-services` read, write

This example shows how to enable control over the subscriber DHCP options to be sent to the AAA server:

```
Router# configure
Router(config)# dhcp ipv4
```

```
Router(config-dhcpv4)# profile server-profile server
```

```
Router(config-dhcpv4-server-profile)# dhcp-to-aaa option list 90 50
```

```
Router(config-dhcpv4-server-profile)# commit
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aaa dhcp-option force-insert, on page 123</code></td>
<td>Enables the insertion of DHCP options while replying to the DHCP client, regardless of the request from the DHCP host.</td>
</tr>
</tbody>
</table>
dhcpv6-to-aaa option list

To enable control over the subscriber DHCPv6 options to be sent to the AAA server by the BNG router, use the `dhcpv6-to-aaa option list all` command in DHCP IPv6 server profile or proxy profile configuration mode. To disable this feature, use the `no` form of this command.

```
dhcpv6-to-aaa option list {all | option-value}
```

**Syntax Description**

- `all`: Enables the functionality to send all DHCPv6 options from the subscriber to the AAA server.
- `option-value`: Specifies the particular DHCPv6 options from the subscriber to be sent to the AAA server.

**Command Default**

None

**Command Modes**

- DHCP IPv6 proxy profile
- DHCP IPv6 server profile

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.6.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The BNG router sends all or specified DHCPv6 options to the AAA server, if this command is configured. You can send a maximum of 13 options (12 DHCP options and a DHCP header) to the AAA server. The header portion of the DHCP control packet is encoded as option type 0. The first 108 bytes of the header are sent to the AAA server.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to enable control over the subscriber DHCP options to be sent to the AAA server:

```
Router# configure
Router(config)# dhcp ipv6
Router(config-dhcpv6)# profile server-profile server
Router(config-dhcpv6-server-profile)# dhcpv6-to-aaa option list 90 50
Router(config-dhcpv6-server-profile)# commit
```
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
```

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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**
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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-template
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-template
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# dhcpv6 address-pool my-ipsub-addr-pool
```
dhcv6 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 `dhcv6 delegated-prefix-pool` command in the dynamic template configuration mode. To remove the delegated prefix pool name, use the `no` form of this command.

```
dhcv6 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To enter the dynamic template configuration mode, enter `dynamic-template` command in the Global Configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This is an example of creating a delegated prefix-pool name using the `dhcv6 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)# dhcv6 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
```

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.3.0</td>
<td>This command was supported in DHCP IPv6 server profile and class configuration mode in BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read,</td>
<td>write</td>
</tr>
</tbody>
</table>

**Examples**

This is an example of setting the DNS server name using the `dns-server` command:

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv6 pool pool1
RP/0/RSP0/CPU0:router(config-dhcpv6-pool)# dns-server 10:10::10
```

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
```

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was supported in DHCP IPv6 server profile and class configuration mode in BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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`
duid allowed-type

To specify the permitted DUID type for the incoming DHCP SOLICIT packets in BNG, use the `duid allowed-type` command in DHCP IPv6 server profile configuration mode. To disable this feature, use the `no` form of this command.

```
duid allowed-type type
```

**Syntax Description**

- `type` Specifies the permitted DUID type of the DHCP solicit packet.

**Command Default**

None

**Command Modes**

DHCP IPv6 server profile

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

- `ip-services` read, write

This example shows how to specify the permitted DUID type for the incoming DHCP SOLICIT packets, as part of enabling DHCP option 16 filtering feature in BNG:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dhcp ipv6
RP/0/RSP0/CPU0:router(config-dhcpv6)# profile server-profile server
RP/0/RSP0/CPU0:router(config-dhcpv6-server-profile)# duid allowed-type 1
RP/0/RSP0/CPU0:router(config-dhcpv6-server-profile)# commit
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>match option (DHCPv6), on page 112</td>
<td>Enables DHCP option 16 filtering feature in BNG.</td>
</tr>
</tbody>
</table>
duplicate-mac-allowed

To allow duplicate client MAC addresses across different VLANs and interfaces, use the `duplicate-mac-allowed` command in the DHCP IPv4 configuration mode. To disallow duplicate client MAC addresses, use the `no` form of this command.

```
duplicate-mac-allowed [{exclude-vlan|include-giaddr}]
```

**Syntax Description**

- **exclude-vlan**: Excludes VLANs from the client key; only MAC address and interface form the client key.
- **include-giaddr**: Enables support for duplicate sessions having the same MAC address but different `gi-address` values, mainly in the case of routed sessions.

**Command Default**

By default, duplicate MAC address support is disabled.

**Command Modes**

DHCP IPv4 configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.3.2</td>
<td>Modified the command to include <code>include-giaddr</code> option as part of DHCP L3 snooping feature in BNG.</td>
</tr>
<tr>
<td>Release 6.1.2</td>
<td>This command was introduced in BNG, with an addition of <code>exclude-vlan</code> option to exclude VLANs from the client key.</td>
</tr>
<tr>
<td>Release 4.3.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can enable duplicate MAC addresses on relay, proxy, server, and snoop DHCP modes.

Do not enable the `duplicate-mac-allowed` command for mobile subscribers.

With `exclude-vlan` option enabled, both inner and outer VLANs get excluded. You cannot exclude just one of them.

The `include-giaddr` option is used for DHCP L3 snooping feature in BNG. It is supported only on Cisco IOS XR 64-bit operating system.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>
**Example**

This example shows how to allow duplicate client MAC addresses across different VLANs and interfaces, using the `duplicate-mac-allowed` command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# duplicate-mac-allowed exclude-vlan
```

This example shows how to enable support for duplicate sessions having the same MAC address but different `gi-address` values, for DHCP L3 snooping in BNG:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# duplicate-mac-allowed include-giaddr
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>dhcp ipv4 (BNG), on page 133</td>
<td>Enables Dynamic Host Configuration Protocol (DHCP) for IPv4 and enters DHCP IPv4 configuration mode.</td>
</tr>
</tbody>
</table>
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
```

### Syntax Description

- `pool_name` Specifies the name of a prefix pool.

### Command Default

None

### Command Modes

Dynamic template configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

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.

### 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
```
giaddr policy keep

While in proxy mode, to retain the gateway address in the DHCP control packets received at BNG from the relay agent, use the `giaddr policy keep` command in DHCP IPv4 proxy profile configuration mode. This is used while enabling DHCP L3 snooping feature in BNG. To disable this configuration, use the `no` form of this command.

**giaddr policy keep**

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
None

**Command Modes**
DHCP IPv4 proxy profile

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
This is supported only on Cisco IOS XR 64-bit operating system.

Without this configuration, the `gi-address` value received at BNG while in proxy mode, is modified and a new value is set based on the router configuration.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to retain the gateway address in the DHCP control packets received at BNG from the relay agent:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# profile example-profile proxy
RP/0/RSP0/CPU0:router(config-dhcpv4-proxy-profile)# giaddr policy keep
RP/0/RSP0/CPU0:router(config-dhcpv4-proxy-profile)# commit
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>initiator dhcp-snoop, on page 306</td>
<td>Configures DHCP to pass the control packets from BNG to the DHCP server to enable DHCP L3 snooping for an IP subscriber.</td>
</tr>
</tbody>
</table>
**helper-address (BNG)**

To configure the Dynamic Host Configuration Protocol (DHCP) IPv4 or IPv6 relay agent to relay DHCP 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]
```

**Syntax Description**

- `vrf-name` (Optional) Specifies the name of a particular VRF.
- `address` IPv4 and IPv6 address in four part, dotted decimal format.
- `giaddr gateway-address` (Optional) Specifies the gateway address to use in packets relayed to server. This keyword is applicable for IPv4 helper address.

**Command Default**

Helper address is not configured.

**Command Modes**

- DHCP IPv6 proxy profile class configuration
- DHCP IPv6 profile relay configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.2.0</td>
<td>This command was supported for BNG.</td>
</tr>
<tr>
<td>Release 4.3.0</td>
<td>The support for IPv6 was added in BNG.</td>
</tr>
<tr>
<td>Release 5.2.2</td>
<td>This command is supported in DHCPv6 profile relay configuration submode.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A maximum of up to eight helper addresses can be configured.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>dhcp ipv4 (BNG), on page 133</strong></td>
<td>Enables Dynamic Host Configuration Protocol (DHCP) for IPv4 and enters DHCP IPv4 configuration mode.</td>
</tr>
<tr>
<td><strong>relay information check (BNG), on page 180</strong></td>
<td>Configures a DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.</td>
</tr>
<tr>
<td><strong>relay information option (BNG), on page 182</strong></td>
<td>Enables the system to insert a DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.</td>
</tr>
<tr>
<td><strong>relay information option allow-untrusted (BNG), on page 184</strong></td>
<td>Configures the DHCP component to not drop BOOTREQUEST messages that have the relay information option set and the giaddr set to zero.</td>
</tr>
<tr>
<td><strong>relay information policy (BNG), on page 186</strong></td>
<td>Configures how a relay agent processes BOOTREQUEST messages that already contain a relay information option.</td>
</tr>
</tbody>
</table>
**inner-cos**

To reset the default inner-cos value for DHCPv4 control packets sent on BNG subscriber interfaces, use the `inner-cos` command in DHCP IPv4 configuration mode. To set the inner-cos value back to the default value, use the `no` form of this command.

**Syntax Description**

```
inner-cos  value
```

- **value**: Value of inner-cos for DHCPv4 control packets.
  - The range is from 0 to 7.

**Command Default**

None

**Command Modes**

DHCP IPv4 configuration

**Command History**

- **Release 4.3.2**: This command was introduced.
- **Release 5.3.1**: This command was modified.

**Usage Guidelines**

The inner and outer Class of Service (CoS) values can be configured for DHCPv4 control packets. For broadcast packets, both the `inner-cos` and `outer-cos` commands can be used to configure CoS values. For unicast packets, the `inner-cos` command cannot be directly used. The outer CoS value configured using the `outer-cos` command is also set as the inner CoS value.

In the following example, for all broadcast DHCP control packets, the inner CoS value will be set as 5 and the outer CoS value will be set as 7. However, for unicast DHCP control packets, both inner and outer CoS values will be set as 7 (the `inner-cos` 5 command does not affect the unicast packets).

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# inner-cos 5
RP/0/RSP0/CPU0:router(config-dhcpv4)# outer-cos 7
RP/0/RSP0/CPU0:router(config-dhcpv4)#
```

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to reset the default inner-cos value for DHCPv4 control packets sent on BNG subscriber interfaces:

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

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>outer-cos, on page 173</td>
<td>Resets the default outer-cos value for DHCPv4 control packets sent on BNG subscriber interfaces.</td>
</tr>
</tbody>
</table>
To enable Dynamic Host Configuration Protocol (DHCP) for IPv4 or IPv6 on an interface, use the `interface` command in the appropriate configuration mode. To disable DHCPv4 or DHCPv6 on an interface, use the `no` form of the command.

```
interface  type  interface-path-id  {base|proxy|relay|server|snoop}
profile  profile-name
```

**Syntax Description**

- `type` Interface type. For more information, use the question mark (?) online help function.
- `interface-path-id` Physical interface or virtual interface.

**Note**

Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

- `server` Attaches a server profile for the specified interface.
- `relay` Attaches a relay profile for the specified interface.
- `snoop` Attaches a snoop profile for the specified interface.
- `proxy` Attaches the proxy profile to an interface.
- `base` Attaches a base profile for the specified interface.

`profile profile-name` Specifies the profile name.

**Command Default**

None

**Command Modes**

DHCP IPv6 configuration

DHCP IPv4 configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.1.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.3.0</td>
<td>The support for IPv6 was added in BNG.</td>
</tr>
<tr>
<td>Release 5.1</td>
<td>Support for <code>server</code> profile was added.</td>
</tr>
</tbody>
</table>
**Release**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.2.2</td>
<td>Support for DHCP IPv6 relay was added. The keyword base was added as part of DHCPv4 Service Based Mode Selection feature.</td>
</tr>
<tr>
<td>Release 6.2.1</td>
<td>Support for DHCP IPv6 base profile was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The support for base profile option for DHCP IPv6 is available in BNG from Release 6.2.1 and later. For more details, refer PPP Class-based DHCPv6 Mode Selection feature in Cisco ASR 9000 Series Aggregation Services Router Broadband Network Gateway Configuration Guide.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This is an example of attaching a base profile to an interface:

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# interface gigabitEthernet 0/0/0/0 base profile BASE_PROFILE
```

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
```

This example shows how to attach a base profile to an interface, in DHCPv6 mode:

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv6
RP/0/RSP0/CPU0:router(config-dhcpv6)# interface Bundle-Ether302.2501 base profile base_TEST
```
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
```

**Syntax Description**

- `profile_name` Specifies the name of the profile.

**Command Default**

VRF is disabled.

**Command Modes**

DHCP IPv6 configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

- Task ID: `ip-services`
  - Operations: `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 at a global server profile level or class profile level, use the `lease` command in DHCPv6 server profile or class profile configuration mode. To disable the client lease time, use the `no` form of this command.

```
lease {days [hours minutes]}infinite
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>days</td>
<td>Specifies the number of days for the lease time. The value ranges from 1 to 365.</td>
</tr>
<tr>
<td>hours</td>
<td>Specifies the number of hours for the lease time. The value ranges from 0 to 23.</td>
</tr>
<tr>
<td>minutes</td>
<td>Specifies the number of minutes for the lease time. The value ranges from 0 to 59.</td>
</tr>
<tr>
<td>infinite</td>
<td>Specifies an infinite amount of lease.</td>
</tr>
</tbody>
</table>

**Command Default**

By default, the lease is 86400 seconds (one day).

**Command Modes**

- DHCPv6 server profile configuration
- DHCPv6 server class profile configuration

**Command History**

- **Release 6.4.1**: The command was extended for lease timer support for class profile as well.
- **Release 4.3.0**: This command was introduced.

**Usage Guidelines**

The lease time is applied only to the class and not to the whole profile. When both profile and class lease time configurations are present, then the class lease time takes precedence. The default lease time is 1 day, if lease time is not configured.

The lease time is specified in seconds or date format.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to configure lease time for 1 day and 6 hours:

```
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
```
This example shows how to configure lease time for class profile:

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

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv6
RP/0/RSP0/CPU0:router(config-dhcpv6)# profile server-profile server
RP/0/RSP0/CPU0:router(config-dhcpv6-server-profile)# class class1
RP/0/RSP0/CPU0:router(config-dhcpv6-server-profile-class1)# lease 0 0 20
RP/0/RSP0/CPU0:router(config-dhcpv6-server-profile-class1)# address-pool poolv6
RP/0/RSP0/CPU0:router(config-dhcpv6-server-profile-class1)# dns-server 2001:DB8::1
```
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
```

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp ipv4 (BNG), on page 133</td>
<td>Enables the Dynamic Host Configuration Protocol (DHCP) for IPv4.</td>
</tr>
</tbody>
</table>
linkaddress-from-ra-enable

To enable DHCP IPv6 proxy mode Point to Point Protocol on Ethernet (PPPoE) session to send the link local address for SOLICIT message or renew request message, use the `linkaddress-from-ra-enable` command.

**linkaddress-from-ra-enable**

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
None

**Command Modes**
DHCP IPv6 proxy profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
By default this feature is disabled. You can use `show profile profile_name proxy` command to see if this feature is enabled or not.

**Note**
The link address configured in proxy profile or class level will take precedence over the link address while using the `linkaddress-from-ra-enable` command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

RP/0/RSP0/CPU0:router# configure
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)# helper-address vrf default 4000::7:2c:2
RP/0/RSP0/CPU0:router(config-dhcpv6-proxy-profile)# linkaddress-from-ra-enable

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp ipv6 (BNG), on page 134</td>
<td>To enable Dynamic Host Configuration Protocol (DHCP) for IPv6 and to enter DHCP IPv6 configuration mode</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>helper-address (BNG), on page 148</td>
<td>To configure the Dynamic Host Configuration Protocol (DHCP) IPv4 or IPv6 relay agent to relay DHCP packets to a specific DHCP server</td>
</tr>
</tbody>
</table>
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
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>value</code></td>
</tr>
<tr>
<td>Specifies the limit up to which the lease value can be extended.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

DHCP IPv4 configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp ipv4 (BNG), on page 133</td>
<td>Enables the Dynamic Host Configuration Protocol (DHCP) for IPv4.</td>
</tr>
</tbody>
</table>
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
```

**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
---------  ---------------
4.2.1      This command was introduced.
```

**Usage Guidelines**

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

**Task ID**

```
Task ID  Operation
--------  ----------
ip-services   read, write
```

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp ipv4 (BNG), on page 133</td>
<td>Enables the Dynamic Host Configuration Protocol (DHCP) for IPv4.</td>
</tr>
</tbody>
</table>
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
```

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp ipv4 (BNG), on page 133</td>
<td>Enables the Dynamic Host Configuration Protocol (DHCP) for IPv4.</td>
</tr>
</tbody>
</table>
match-default

To specify the default profile to match the subscriber's PPPoE/IPoE class information for IPv4/IPv6 prefix allocation to the end user, use the **match-default** command in the DHCP IPv4/IPv6 base profile configuration mode. To disable the match option, use the **no** form of the command.

```
match-default profile profile-name server
```

**Syntax Description**

- **class-name** Specifies the name of the class.
- **profile** Specifies the profile to select for a particular class.
- **profile-name** Specifies the name of the profile.
- **server** Specifies the server mode.

**Command Default**

None

**Command Modes**

DHCP IPv4/IPv6 base profile configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced for DHCPv6.</td>
</tr>
<tr>
<td>6.6.2</td>
<td>This command was introduced for DHCPv4.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This is an example of using the **match-default** command in the DHCP IPv4 base profile configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# profile BASE_PROFILE base
RP/0/RSP0/CPU0:router(config-dhcpv4-base-profile)# match mode-class SERVER_CLASS profile SERVER_PROFILE server
RP/0/RSP0/CPU0:router(config-dhcpv4-base-profile)# match mode-class PROXY_CLASS profile PROXY_PROFILE proxy
RP/0/RSP0/CPU0:router(config-dhcpv4-base-profile)# match-default profile DEFAULT_SERVER server
RP/0/RSP0/CPU0:router(config-dhcpv4-base-profile)# dhcp-to-aaa option list 12 55 60 61 124
RP/0/RSP0/CPU0:router(config-dhcpv4-base-profile)# exit
RP/0/RSP0/CPU0:router(config-dhcpv4)# interface bundle-ether1.10 base profile BASE_PROFILE
RP/0/RSP0/CPU0:router(config-dhcpv4)# interface pw-ether25000.10 base profile BASE_PROFILE
RP/0/RSP0/CPU0:router(config-dhcpv4)# commit
```
This is an example of using the `match-default` command in the DHCP IPv6 base profile configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv6
RP/0/RSP0/CPU0:router(config-dhcpv6)# profile BASE_PROFILE base
RP/0/RSP0/CPU0:router(config-dhcpv6-base-profile)# match mode-class SERVER_CLASS profile SERVER_PROFILE server
RP/0/RSP0/CPU0:router(config-dhcpv6-base-profile)# match mode-class PROXY_CLASS profile PROXY_PROFILE proxy
RP/0/RSP0/CPU0:router(config-dhcpv6-base-profile)# match-default profile DEFAULT_SERVER server
RP/0/RSP0/CPU0:router(config-dhcpv6-base-profile)# dhcpv6-to-aaa option list all
RP/0/RSP0/CPU0:router(config-dhcpv6-base-profile)# exit
RP/0/RSP0/CPU0:router(config-dhcpv6)# interface bundle-ether1.10 base profile BASE_PROFILE
RP/0/RSP0/CPU0:router(config-dhcpv6)# interface pw-ether25000.10 base profile BASE_PROFILE
RP/0/RSP0/CPU0:router(config-dhcpv6)# commit
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>match mode-class</code>, on page 165</td>
<td>Matches the subscriber’s PPPoE/IPoE class information for IPv4/IPv6 prefix allocation.</td>
</tr>
<tr>
<td><code>dhcp ipv4 (BNG), on page 133</code></td>
<td>Enables the Dynamic Host Configuration Protocol (DHCP) for IPv4.</td>
</tr>
<tr>
<td><code>dhcp ipv6 (BNG), on page 134</code></td>
<td></td>
</tr>
<tr>
<td><code>interface (DHCP-BNG), on page 152</code></td>
<td></td>
</tr>
</tbody>
</table>
match mode-class

To match the subscriber's PPPoE/IPoE class information in order to select the corresponding profile to perform the server or proxy functionality for IPv4/IPv6 prefix allocation to the end user, use the `match mode-class` command in the DHCP IPv4/IPv6 base profile configuration mode. To disable the match option, use the `no` form of the command.

```
match mode-class class-name profile profile-name {server | proxy}
```

**Syntax Description**
- `class-name`: Specifies the name of the class.
- `profile`: Specifies the profile to select for a particular class.
- `profile-name`: Specifies the name of the profile.
- `server`: Specifies the server mode.
- `proxy`: Specifies the proxy mode.

**Command Default**
None

**Command Modes**
DHCP IPv4/IPv6 base profile configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.2.1</td>
<td>This command was introduced for DHCPv6.</td>
</tr>
<tr>
<td>Release 6.6.2</td>
<td>This command was introduced for DHCPv4.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**
- `ip-services`: `read, write`

This is an example of using the `match mode-class` command in the DHCP IPv4 base profile configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dhcp_ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# profile BASE_PROFILE base
RP/0/RSP0/CPU0:router(config-dhcpv4-base-profile)# match mode-class SERVER_CLASS profile SERVER_PROFILE server
RP/0/RSP0/CPU0:router(config-dhcpv4-base-profile)# match mode-class PROXY_CLASS profile PROXY_PROFILE proxy
RP/0/RSP0/CPU0:router(config-dhcpv4-base-profile)# match-default profile DEFAULT_SERVER
RP/0/RSP0/CPU0:router(config-dhcpv4-base-profile)# dhcp-to-aaa option list 12 55 60 61 124
RP/0/RSP0/CPU0:router(config-dhcpv4-base-profile)# exit
```
This is an example of using the **match mode-class** command in the DHCP IPv6 base profile configuration mode:

```console
RP/0/RSP0/CPU0:router(config)# dhcp ipv6
RP/0/RSP0/CPU0:router(config)# profile BASE_PROFILE base
RP/0/RSP0/CPU0:router(config-dhcpv6-base-profile)# match mode-class SERVER_CLASS profile SERVER_PROFILE server
RP/0/RSP0/CPU0:router(config-dhcpv6-base-profile)# match mode-class PROXY_CLASS profile PROXY_PROFILE proxy
RP/0/RSP0/CPU0:router(config-dhcpv6-base-profile)# match-default profile DEFAULT_SERVER server
RP/0/RSP0/CPU0:router(config-dhcpv6-base-profile)# dhcpv6-to-aaa option list all
RP/0/RSP0/CPU0:router(config-dhcpv6-base-profile)# exit
RP/0/RSP0/CPU0:router(config-dhcpv6)# interface bundle-ether1.10 base profile BASE_PROFILE
RP/0/RSP0/CPU0:router(config-dhcpv6)# interface pw-ether25000.10 base profile BASE_PROFILE
RP/0/RSP0/CPU0:router(config-dhcpv6)# commit
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>match-default, on page 163</td>
<td>Specifies the default profile to match the subscriber’s PPPoE/IPoE class information for IPv4/IPv6 prefix allocation.</td>
</tr>
<tr>
<td>dhcp ipv4 (BNG), on page 133</td>
<td>Enables the Dynamic Host Configuration Protocol (DHCP) for IPv4.</td>
</tr>
<tr>
<td>dhcp ipv6 (BNG), on page 134</td>
<td></td>
</tr>
<tr>
<td>interface (DHCP-BNG), on page 152</td>
<td></td>
</tr>
</tbody>
</table>
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
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>124</td>
<td>Inserts option 124 vendor-identifying vendor class.</td>
</tr>
<tr>
<td>125</td>
<td>Inserts option 125 vendor-identifying vendor-specific info.</td>
</tr>
<tr>
<td>60</td>
<td>Inserts option 60 vendor class ID.</td>
</tr>
<tr>
<td>77</td>
<td>Inserts option 124 user class.</td>
</tr>
<tr>
<td><strong>hex</strong></td>
<td>Inserts a hex pattern.</td>
</tr>
<tr>
<td><strong>hex_string</strong></td>
<td>Specifies the hex pattern string.</td>
</tr>
<tr>
<td><strong>mask</strong></td>
<td>Inserts bit mask pattern.</td>
</tr>
<tr>
<td><strong>bit_mask_string</strong></td>
<td>Specifies the bit mask pattern string. The string pattern is between 0 and 4294967295.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

DHCP IPv4 proxy profile class configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>class, on page 130</td>
<td>Creates a proxy profile class and enters the proxy profile class sub configuration mode.</td>
</tr>
</tbody>
</table>
**match option 60**

To enable option 60-based DISCOVER packet filter in DHCPv4, use the `match option 60` command in DHCP IPv4 profile (server, proxy, base or dynamic) configuration mode. To disable this feature, use the `no` form of this command.

For server or proxy profile mode:

```
match option 60 {default |hex hex-string} action {allow |drop}
```

For base or dynamic profile mode:

```
match option 60 {default hex-string} action {allow |drop}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>default</strong></td>
<td>Defines a default behavior in case any Vendor-Id specific option 60 filter is not configured.</td>
</tr>
<tr>
<td><strong>hex</strong></td>
<td>Specifies the hexadecimal pattern in DHCP option 60 to be matched.</td>
</tr>
<tr>
<td><strong>hex-string</strong></td>
<td>Specifies the action to be performed on DISCOVER packets.</td>
</tr>
<tr>
<td><strong>action</strong></td>
<td>Specifies the action to be performed on DISCOVER packets.</td>
</tr>
<tr>
<td><strong>allow</strong></td>
<td>Allows the DISCOVER packets based on DHCP option 60 information.</td>
</tr>
<tr>
<td><strong>drop</strong></td>
<td>Drops the DISCOVER packets based on DHCP option 60 information.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

DHCP IPv4 proxy profile configuration
DHCP IPv4 server profile configuration
DHCP IPv4 base profile configuration
DHCP IPv4 dynamic profile configuration

**Command History**

Release 6.1.2 This command was introduced.

**Usage Guidelines**

The DHCP option 60 filtering feature kicks in only for DISCOVER packets that have option 60 field available. In case of dynamic mode, the preference is given to the base profile filter list over proxy or server mode filter list, if available.

**Task ID**

```
Task ID Operation
ip-services read, write
```
This example shows how to whitelist (allow) DHCP client packets with option 60 hex string "1234" and "1256", and blacklist (drop) all others.

```
RP/0/RSP0/CPU0:router(config-dhcpv4-proxy-profile)# match option 60 hex 1234 action allow
RP/0/RSP0/CPU0:router(config-dhcpv4-proxy-profile)# match option 60 hex 1256 action allow
RP/0/RSP0/CPU0:router(config-dhcpv4-proxy-profile)# match option 60 default action drop
```

This example shows how to blacklist (drop) DHCP client packets with option 60 hex string "1234" and "1256", and whitelist (allow) all others.

```
RP/0/RSP0/CPU0:router(config-dhcpv4-proxy-profile)# match option 60 hex 1234 action drop
RP/0/RSP0/CPU0:router(config-dhcpv4-proxy-profile)# match option 60 hex 1256 action drop
RP/0/RSP0/CPU0:router(config-dhcpv4-proxy-profile)# match option 60 default action allow
```
**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
```

**Syntax Description**

<table>
<thead>
<tr>
<th>vrf_name</th>
<th>Specifies the VRF name.</th>
</tr>
</thead>
</table>

**Command Default**

None

**Command Modes**

DHCP IPv4 proxy profile class configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>match option, on page 167</td>
<td>Matches the proxy with the configured pattern.</td>
</tr>
</tbody>
</table>
option 17

To deliver the URL for self-configuration from the BNG to CPEs through DHCPv6 Option 17, use the option 17 command in the DHCP IPv6 server profile configuration mode. To remove the configuration, use the no form of this command.

```
option 17 hex hex-string
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hex hex-string</td>
<td>Specifies URL in hexadecimal format, with a maximum length of 1000 hex nibbles or 500 characters.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

DHCP IPv6 server profile

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to send the URL for self-configuration from BNG to CPEs through DHCPv6 Option 17:

```
RP/0/RSP0/CPU0:router (config)# dhcp ipv6
RP/0/RSP0/CPU0:router (config-dhcpv6)# profile dhcp_server1 server
RP/0/RSP0/CPU0:router (config-dhcpv6-server-profile)# option 17 hex
0000168b0001002068747470733a2f2f6f70657261746f722e636f6d2f6465766963652f61636d70
```

The value used as encoded string in this example represents these:

- 0x00000de9—enterprise number=3561—The Broadband Forum
- 0x0001—opt-code=1
- 0x0020—option-len=32
- 0x68747470733a2f2f6f70657261746f722e636f6d2f6465766963652f61636d70—option-data=https://operator.com/device/acmp
### outer-cos

To reset the default outer-cos value for DHCPv4 control packets sent on BNG subscriber interfaces, use the `outer-cos` command in DHCP IPv4 configuration mode. To set the outer-cos value back to the default value, use the `no` form of this command.

```
outer-cos  value
```

**Syntax Description**

| `value` | Value of outer-cos for DHCPv4 control packets.  
|         | The range is from 0 to 7.  |

**Command Default**

None

**Command Modes**

DHCP IPv4 configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.3.2</td>
<td>This command was modified.</td>
</tr>
<tr>
<td>5.3.1</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The inner and outer Class of Service (CoS) values can be configured for DHCPv4 control packets. For broadcast packets, both the `inner-cos` and `outer-cos` commands can be used to configure CoS values. For unicast packets, the `inner-cos` command cannot be directly used. The outer CoS value configured using the `outer-cos` command is also set as the inner CoS value.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to reset the default outer-cos value for DHCPv4 control packets sent on BNG subscriber interfaces:

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>inner-cos</code>, on page 150</td>
<td>Resets the default inner-cos value for DHCPv4 control packets sent on BNG subscriber interfaces.</td>
</tr>
</tbody>
</table>
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
```

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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 { base | proxy | server }
```

**Syntax Description**

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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.3.0</td>
<td>Support was added for IPv6.</td>
</tr>
<tr>
<td>6.2.1</td>
<td>Support for base profile was added for DHCP IPv6 in BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `profile-name` and the `class-name` should be unique per base profile.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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:

```bash
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-profile-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)#
```

This example shows how to create a DHCPv6 base profile:

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

This command aids to enable or disable the rapid commit option of the DHCP server. Enabling it renders the DHCPv6 server to use the two message exchange feature to address/prefix an assignment. Including the rapid commit option in the SOLICIT message and enabling the same in the server profile, enables the server to respond with the REPLY message. Else, it follows the normal four message exchange procedure to assign address/prefix an assignment.

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
None

**Command Modes**
DHCP IPv6 server profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| Release 5.2.0 | This command was introduced.

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
This is an example of enabling rapid-commit 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)# rapid-commit
```
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}
```

**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 4.3.1** This command was introduced.

**Usage Guidelines**
No specific guidelines impact the use of this command.

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

**Examples**
This example shows how to 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-dhcpv4-proxy-profile)# relay information authenticate received
```

**Related Commands**
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp ipv4 (BNG), on page 133</td>
<td>Enables Dynamic Host Configuration Protocol (DHCP) for IPv4 and enters DHCP IPv4 configuration mode.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>relay information check (BNG), on page 180</td>
<td>Configures a DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.</td>
</tr>
<tr>
<td>relay information option (BNG), on page 182</td>
<td>Enables the system to insert a DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.</td>
</tr>
<tr>
<td>relay information option allow-untrusted (BNG), on page 184</td>
<td>Configures the DHCP component to not drop BOOTREQUEST messages that have the relay information option set and the giaddr set to zero.</td>
</tr>
<tr>
<td>relay information policy (BNG), on page 186</td>
<td>Configures how a relay agent processes BOOTREQUEST messages that already contain a relay information option.</td>
</tr>
</tbody>
</table>
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**

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.2.0</td>
<td>This command was supported for BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
<tr>
<td>basic-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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

```plaintext
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp ipv4 (BNG), on page 133</td>
<td>Enables DHCP for IPv4 and enters DHCP IPv4 configuration mode.</td>
</tr>
<tr>
<td>helper-address</td>
<td>Configures the DHCP relay agent to relay packets to a specific DHCP Server.</td>
</tr>
<tr>
<td>profile (BNG)</td>
<td>Configures a relay profile for the DHCP IPv4 component.</td>
</tr>
</tbody>
</table>
### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>relay information option (BNG), on page 182</td>
<td>Enables the system to insert a DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.</td>
</tr>
<tr>
<td>relay information option allow-untrusted (BNG), on page 184</td>
<td>Configures the DHCP component to not drop BOOTREQUEST messages that have the relay information option set and the giaddr set to zero.</td>
</tr>
</tbody>
</table>
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**

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

| 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.

If 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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
<tr>
<td>basic-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>
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
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BNG DHCP Commands</td>
<td>dhcp ipv4 (BNG), on page 133</td>
<td>Enables DHCP for IPv4 and enters DHCP IPv4 configuration mode.</td>
</tr>
<tr>
<td></td>
<td>helper-address</td>
<td>Configures the DHCP relay agent to relay packets to a specific DHCP Server.</td>
</tr>
<tr>
<td></td>
<td>relay information check (BNG), on page 180</td>
<td>Configures a DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.</td>
</tr>
<tr>
<td></td>
<td>relay information option allow-untrusted (BNG), on page 184</td>
<td>Configures the DHCP component to not drop BOOTREQUEST messages that have the relay information option set and the giaddr set to zero.</td>
</tr>
</tbody>
</table>
**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
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

The packet is dropped if the relay information is set and the giaddr is set to zero.

**Command Modes**

- DHCP IPv4 relay profile configuration
- DHCP IPv4 profile snoop configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.2.0</td>
<td>This command was supported for BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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.

**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
```
**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp ipv4 (BNG), on page 133</td>
<td>Enables DHCP for IPv4 and enters DHCP IPv4 configuration mode.</td>
</tr>
<tr>
<td>helper-address</td>
<td>Configures the DHCP relay agent to relay packets to a specific DHCP Server.</td>
</tr>
<tr>
<td>relay information check (BNG), on page 180</td>
<td>Configures a DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.</td>
</tr>
<tr>
<td>relay information option (BNG), on page 182</td>
<td>Enables the system to insert a DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.</td>
</tr>
</tbody>
</table>
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}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>drop</td>
<td>Directs the DHCP IPv4 Relay to discard BOOTREQUEST packets with the existing relay information option.</td>
</tr>
<tr>
<td>keep</td>
<td>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.</td>
</tr>
<tr>
<td>encapsulate</td>
<td>Encapsulates the DHCP relay agent information option received from a prior relay agent in forwarded BOOTREQUEST messages.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command was introduced.</td>
</tr>
<tr>
<td></td>
<td>This command was supported for BNG.</td>
</tr>
<tr>
<td></td>
<td>The <code>encapsulate</code> keyword was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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.

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

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp ipv4 (BNG), on page 133</td>
<td>Enables DHCP for IPv4 and enters DHCP IPv4 configuration mode.</td>
</tr>
<tr>
<td>helper-address</td>
<td>Configures the DHCP relay agent to relay packets to a specific DHCP Server.</td>
</tr>
<tr>
<td>relay information check (BNG), on page 180</td>
<td>Configures a DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.</td>
</tr>
<tr>
<td>relay information option (BNG), on page 182</td>
<td>Enables the system to insert a DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.</td>
</tr>
<tr>
<td>relay information option allow-untrusted (BNG), on page 184</td>
<td>Configures the DHCP component to not drop BOOTREQUEST messages that have the relay information option set and the giaddr set to zero.</td>
</tr>
</tbody>
</table>
**relay option interface-id**

To insert Interface-Id DHCPv6 option (option 18) in the Relay-forward message sent from BNG DHCPv6 proxy to the external DHCPv6 server, use the `relay option interface-id` command in the DHCP IPv6 proxy profile configuration mode. To disable this, use the `no` form of this command.

```
relay option interface-id insert {local|pppoe|received}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>insert</code></td>
<td>Inserts Interface-Id DHCPv6 option (option 18) in the Relay-forward message sent from BNG DHCPv6 proxy to the external DHCPv6 server.</td>
</tr>
<tr>
<td><code>local</code></td>
<td>Inserts locally generated or configured Interface-Id value.</td>
</tr>
<tr>
<td><code>pppoe</code></td>
<td>Inserts the Interface-Id value received from the SADB.</td>
</tr>
<tr>
<td><code>received</code></td>
<td>Inserts the received Interface-Id value.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

DHCP IPv6 proxy profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is valid only for PPPoE subscriber sessions.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to insert DHCPv6 option (Interface-Id) in the Relay-forward message sent from BNG DHCPv6 proxy to the external DHCPv6 server.

```
RP/0/RSP0/CPU0:router#config
RP/0/RSP0/CPU0:router(config)#dhcp ipv6
RP/0/RSP0/CPU0:router(config-dhcpv6)#profile P1 proxy
RP/0/RSP0/CPU0:router(config-dhcpv6-proxy-profile)#relay option interface-id insert pppoe
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>relay option link-layer-addr</code>, on page 190</td>
<td>Sets MAC address as the Link-layer address in the Relay-forward message sent from BNG DHCPv6 to the external DHCPv6 server.</td>
</tr>
</tbody>
</table>
### Command Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>relay option remote-id, on page 191</td>
<td>Identifies the remote host end of the circuit in the DHCPv6 relay agents.</td>
</tr>
<tr>
<td>relay option subscriber-id, on page 193</td>
<td>Sets the Relay-Agent-Subscriber-Id option (DHCPv6 option 38) in the Relay-forward message sent from BNG DHCPv6 proxy to the external DHCPv6 server.</td>
</tr>
</tbody>
</table>
relay option link-layer-addr

To set the MAC address as the Link-layer address DHCPv6 option in the Relay-forward message sent from BNG DHCPv6 proxy to the external DHCPv6 server, use the **relay option link-layer-addr** command in the DHCP IPv6 proxy profile configuration mode. To disable this feature, use the **no** form of this command.

```
relay option remote-id set
```

**Syntax Description**

- **set** Sets the MAC address as the Link-layer address in the Relay-forward message sent from BNG DHCPv6 to the external DHCPv6 server.

**Command Default**

None

**Command Modes**

DHCP IPv6 proxy profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.1.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is valid for both IPoE and PPPoE subscriber sessions.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to set DHCPv6 option 79 (Link-layer address) in the Relay-forward message sent from BNG DHCPv6 proxy to the external DHCPv6 server:

```
RP/0/RSP0/CPU0:router#config
RP/0/RSP0/CPU0:router(config)#dhcp ipv6
RP/0/RSP0/CPU0:router(config-dhcpv6)#profile P1 proxy
RP/0/RSP0/CPU0:router(config-dhcpv6-proxy-profile)#relay option link-layer-addr
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>relay option interface-id, on page 188</td>
<td>Inserts Interface-Id DHCPv6 option (option 18) in the Relay-forward message sent from BNG DHCPv6 proxy to the external DHCPv6 server.</td>
</tr>
<tr>
<td>relay option remote-id, on page 191</td>
<td>Identifies the remote host end of the circuit in the DHCPv6 relay agents.</td>
</tr>
<tr>
<td>relay option subscriber-id, on page 193</td>
<td>Sets the Relay-Agent-Subscriber-Id option (DHCPv6 option 38) in the Relay-forward message sent from BNG DHCPv6 proxy to the external DHCPv6 server.</td>
</tr>
</tbody>
</table>
# 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.

```plaintext
relay option remote-id (remote-id-string|pppoe)
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>remote-id-string</td>
<td>Specifies the string value for the Remote-Id.</td>
</tr>
<tr>
<td>pppoe</td>
<td>Specifies Remote-Id attribute in PPPoE session.</td>
</tr>
</tbody>
</table>

**Command Default**

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

**Command Modes**

DHCP IPv6 proxy profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.1.2</td>
<td>Modified the command to include <code>pppoe</code> option.</td>
</tr>
<tr>
<td>Release 4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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:

```plaintext
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-dhcpv6-proxy-profile)# relay option remote-id my-remote-id my-remote-id-12345
```

This example shows how to facilitate identification of subscriber based on the Remote-Id attribute in PPPoE session:
**related commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>relay information option (BNG), on page 182</td>
<td>Enables the system to insert a DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.</td>
</tr>
<tr>
<td>relay option interface-id, on page 188</td>
<td>Inserts Interface-Id DHCPv6 option (option 18) in the Relay-forward message sent from BNG DHCPv6 proxy to the external DHCPv6 server.</td>
</tr>
<tr>
<td>relay option link-layer-addr, on page 190</td>
<td>Sets MAC address as the Link-layer address in the Relay-forward message sent from BNG DHCPv6 to the external DHCPv6 server.</td>
</tr>
<tr>
<td>relay option subscriber-id, on page 193</td>
<td>Sets the Relay-Agent-Subscriber-Id option (DHCPv6 option 38) in the Relay-forward message sent from BNG DHCPv6 proxy to the external DHCPv6 server.</td>
</tr>
</tbody>
</table>
relay option subscriber-id

To set the Relay-Agent-Subscriber-Id option (DHCPv6 option 38) in the Relay-forward message sent from BNG DHCPv6 proxy to the DHCPv6 server, use the `relay option subscriber-id` command in the DHCP IPv6 proxy profile configuration mode. To disable this feature, use the `no` form of this command.

```
relay option subscriber-id pppoe
```

**Syntax Description**
- **pppoe**: Specifies Relay-Agent-Subscriber-Id for PPPoE subscribers.

**Command Default**
None

**Command Modes**
DHCP IPv6 proxy profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
This command is valid only for PPPoE subscribers.

**Examples**
This example shows how to set DHCPv6 option 38 in the Relay-forward message sent from BNG DHCPv6 proxy to the DHCPv6 server:

```
RP/0/RSP0/CPU0:router(config)#config
RP/0/RSP0/CPU0:router(config)#dhcp ipv6
RP/0/RSP0/CPU0:router(config-dhcpv6)#profile P1 proxy
RP/0/RSP0/CPU0:router(config-dhcpv4-proxy-profile)#relay option subscriber-id pppoe
```

**Related Commands**
- **relay option interface-id**, on page 188: Inserts Interface-Id DHCPv6 option (option 18) in the Relay-forward message sent from BNG DHCPv6 proxy to the external DHCPv6 server.
- **relay option link-layer-addr**, on page 190: Sets MAC address as the Link-layer address in the Relay-forward message sent from BNG DHCPv6 to the external DHCPv6 server.
- **relay option remote-id**, on page 191: Identifies the remote host end of the circuit in the DHCPv6 relay agents.
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]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>circuit-id</td>
<td>Displays the DHCP IPv4 proxy client binding based on circuit ID.</td>
</tr>
<tr>
<td>circuit_id_name</td>
<td>Displays the name of the circuit ID.</td>
</tr>
<tr>
<td>detail</td>
<td>Displays detailed binding information for DHCP proxy.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies the interface based on which the DHCP bindings are filtered.</td>
</tr>
<tr>
<td>ipspecifier</td>
<td>Displays the name of the interface.</td>
</tr>
<tr>
<td>location</td>
<td>Specifies the node location of the DHCP proxy.</td>
</tr>
<tr>
<td>locationspecifier</td>
<td>Displays the name of the location.</td>
</tr>
<tr>
<td>mac-address</td>
<td>Displays detailed client binding information based on mac-address.</td>
</tr>
<tr>
<td>remote-id</td>
<td>Displays the DHCP IPv4 proxy client binding based on remote ID.</td>
</tr>
<tr>
<td>summary</td>
<td>Displays the summary binding information for proxy.</td>
</tr>
<tr>
<td>vrf</td>
<td>Displays the VRF information.</td>
</tr>
<tr>
<td>vrf_name</td>
<td>Displays the name of the VRF.</td>
</tr>
<tr>
<td></td>
<td>Displays the output modifiers.</td>
</tr>
</tbody>
</table>

**Command Default**

Displays brief information about all DHCP proxy client bindings.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

This is the sample output of the `show dhcp ipv4 proxy binding` command:
show dhcp ipv4 proxy binding

The show dhcp ipv4 proxy binding output is as follows:

MAC Address | IP Address | State | Remaining | Interface | VRF
-------------|------------|-------|-----------|-----------|------
0000.6602.0102 | 1.1.1.1 | BOUND | 3495 | Gi0/1/0/0 | default

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

show dhcp ipv4 proxy binding circuit-id CCCCCCCCC

MAC Address: 0000.6602.0102
IP Address: 1.1.1.1
circuit-id: CCCCCCCCC
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

show dhcp ipv4 proxy binding remote-id RRRRRRRRRR

MAC Address: 0000.6602.0102
IP Address: 1.1.1.1
Profile: foo
circuit-id: CCCCCCCCC
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

show dhcp ipv4 proxy binding detail

MAC Address: ca01.3fcd.0000
VRF: default
This is the sample output of the `show dhcp ipv4 proxy binding detail` command, that displays the detailed information of the IPoEV4 clients created as part of the dual-stack subscriber session. The IP-address, MAC-address, VRF-name, the interface on which the client is created and so on, are displayed as part of this command output.
InsertedVSI0: -
Auth. on received relay info: FALSE
Profile: IPoEV4
State: BOUND
Proxy lease: 3600 secs (01:00:00)
Proxy lease remaining: 3403 secs (00:56:43)
Client ID: 0x00-0x00-0x64-0x01-0x01-0x02
Access Interface: Bundle-Ether1.10
Access VRF: default
VLAN Id: 10
Subscriber Label: 0x55
Subscriber Interface: Bundle-Ether1.10.ip22

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp ipv4 (BNG), on page 133</td>
<td>Enables the Dynamic Host Configuration Protocol (DHCP) for IPv4.</td>
</tr>
<tr>
<td>show dhcp ipv6 proxy binding (BNG), on page 202</td>
<td>Shows the client bindings for Dynamic Host Configuration Protocol (DHCP) proxy.</td>
</tr>
</tbody>
</table>
**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 mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was supported for BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lease Limit</td>
<td>Specifies the lease limit value sent from AAA server.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Count</td>
<td>Specifies the number of sessions on the router having the specific Circuit-ID received from the AAA server.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Displays the detailed proxy profile information.</td>
</tr>
<tr>
<td>profile_name</td>
<td>Specifies the profile name.</td>
</tr>
<tr>
<td></td>
<td>Displays the output modifiers.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Release 4.2.0  This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command displays the proxy profiles created for DHCP IPv4.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP IPv4 Proxy Profiles</td>
<td>Specifies all the DHCP IPv4 proxy profiles.</td>
</tr>
</tbody>
</table>
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 mode

**Command History**

- Release 4.2.0 This command was introduced.

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

- `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

<table>
<thead>
<tr>
<th>VRF</th>
<th>RX</th>
<th>TX</th>
<th>DR</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>nVSatellite</strong></td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

This table describes the significant fields shown in the display.

*Table 11: show dhcp ipv4 proxy statistics Field Descriptions*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF</td>
<td>Specifies the VRF in the DHCP proxy. The default is nVSatellite.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Displays detailed bindings for proxy.</td>
</tr>
<tr>
<td>duid</td>
<td>Displays client bindings for DUID.</td>
</tr>
<tr>
<td>interface</td>
<td>Displays client bindings by Interface.</td>
</tr>
<tr>
<td>interface-id</td>
<td>Displays client bindings by Interface ID.</td>
</tr>
<tr>
<td>location</td>
<td>Specifies the node location.</td>
</tr>
<tr>
<td>mac-address</td>
<td>Displays detailed client binding information.</td>
</tr>
<tr>
<td>remote-id</td>
<td>Displays client binding by Remote ID.</td>
</tr>
<tr>
<td>summary</td>
<td>Displays summary bindings for proxy.</td>
</tr>
<tr>
<td>vrf</td>
<td>Displays client bindings by VRF name.</td>
</tr>
</tbody>
</table>

### Command Default

None

### Command Modes

EXEC mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.3.0</td>
<td>This command was supported for BNG.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

No specific guidelines impact the use of this command.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read</td>
</tr>
</tbody>
</table>

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 (G10/0/0/1)  
DUID: 00030001ca004a2d0000  
IAID: 00020001  
lifetime: 2592000  
expiration: Nov 25 2010 16:47

RP/0/RSP0/CP0:router# show dhcp ipv6 proxy binding summary

Total number of clients: 2

<table>
<thead>
<tr>
<th>STATE</th>
<th>COUNT</th>
<th>IA-NA</th>
<th>IA-PD</th>
</tr>
</thead>
<tbody>
<tr>
<td>INIT</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>SUB VALIDATING</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>ADDR/PREFIX ALLOCATING</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>REQUESTING</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>SESSION RESP PENDING</td>
<td>2</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>ROUTE UPDATING</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>BOUND</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
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}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>type</code></td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>interface-path-id</code></td>
<td>Physical interface or virtual interface.</td>
</tr>
</tbody>
</table>

**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 mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Interface</th>
<th>Mode</th>
<th>Profile Name</th>
<th>Amb</th>
<th>Lease Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>BE1.100</td>
<td>P</td>
<td>pxy1</td>
<td>No</td>
<td>None</td>
</tr>
<tr>
<td>BE1.200</td>
<td>P</td>
<td>pxy1</td>
<td>No</td>
<td>None</td>
</tr>
<tr>
<td>BE1.250</td>
<td>P</td>
<td>pxy1</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>BE1.400</td>
<td>P</td>
<td>pxy1</td>
<td>Yes</td>
<td>None</td>
</tr>
</tbody>
</table>
```
show dhcp ipv6 proxy interface (BNG)
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Displays the detailed proxy profile information for the profile.</td>
</tr>
<tr>
<td>profile_name</td>
<td>Specifies the name of the profile.</td>
</tr>
<tr>
<td>location</td>
<td>Displays the node location by Interface.</td>
</tr>
<tr>
<td>location</td>
<td>Displays the fully qualified location specification of an interface.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read</td>
</tr>
</tbody>
</table>

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 mode

Command History
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines
No specific guidelines impact the use of this command.

Task ID
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read</td>
</tr>
</tbody>
</table>

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 |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>23</td>
<td>28</td>
</tr>
<tr>
<td>red</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>blue</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>green</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>orange</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>test_vrf</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dhcpclient</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
### show dhcp ipv6 proxy statistics

| dhcpserver | 0 | 0 | 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 mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

No specific guidelines impact the use of this command.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read</td>
</tr>
</tbody>
</table>

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
```
show dhcp ipv6 server binding

Total number of clients: 3

<table>
<thead>
<tr>
<th>STATE</th>
<th>COUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>INIT</td>
<td>0</td>
</tr>
<tr>
<td>SUB VALIDATING</td>
<td>0</td>
</tr>
<tr>
<td>ADDR/PREFIX ALLOCATING</td>
<td>0</td>
</tr>
<tr>
<td>REQUESTING</td>
<td>0</td>
</tr>
<tr>
<td>SESSION RESP PENDING</td>
<td>0</td>
</tr>
<tr>
<td>ROUTE UPDATING</td>
<td>0</td>
</tr>
<tr>
<td>BOUND</td>
<td>3</td>
</tr>
</tbody>
</table>

show dhcp ipv6 server binding detail

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)

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)

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)

BNG DHCP Commands
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>type</code></td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>interface-path-id</code></td>
<td>Either a physical interface instance or a virtual interface instance as follows:</td>
</tr>
<tr>
<td></td>
<td>- Physical interface instance. Naming notation is <code>rack/slot/module/port</code> and a slash between values is required as part of the notation.</td>
</tr>
<tr>
<td></td>
<td>- <code>rack</code>: Chassis number of the rack.</td>
</tr>
<tr>
<td></td>
<td>- <code>slot</code>: Physical slot number of the modular services card or line card.</td>
</tr>
<tr>
<td></td>
<td>- <code>module</code>: Module number. A physical layer interface module (PLIM) is always 0.</td>
</tr>
<tr>
<td></td>
<td>- <code>port</code>: Physical port number of the interface.</td>
</tr>
<tr>
<td><code>location</code></td>
<td>Displays the node location by Interface.</td>
</tr>
<tr>
<td><code>location</code></td>
<td>Displays the fully qualified location specification of an interface.</td>
</tr>
</tbody>
</table>

**Syntax Description**

<table>
<thead>
<tr>
<th>Note</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note</td>
<td>• 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.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read</td>
</tr>
</tbody>
</table>
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 mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read</td>
</tr>
</tbody>
</table>

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 mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**
- **Operation**: read
- **Task ID**: ip-services

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

<table>
<thead>
<tr>
<th>VRF</th>
<th>RX</th>
<th>TX</th>
<th>DR</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>10003</td>
<td>11651</td>
<td>3</td>
</tr>
<tr>
<td>red</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>blue</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>green</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>orange</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>test_vrf</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dhcpclient</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
**BNG DHCP Commands**

**show dhcp ipv6 server statistics**

| dhcpserver | 0 | 0 | 0 | 0 | 0 |
BNG Interface Commands

This module describes the Cisco IOS XR software commands used to configure and verify the interfaces 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*.

To use commands of this module, 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 any command, contact your AAA administrator for assistance.

- encapsulation ambiguous dot1ad, on page 218
- encapsulation ambiguous dot1q, on page 220
- show ethernet tags, on page 222
encapsulation ambiguous dot1ad

To configure encapsulated ambiguous VLANs with IEEE 802.1ad Provider Bridging (PB) encapsulation type on an access-interface, use the `encapsulation ambiguous dot1ad` command in the interface configuration mode. To remove the encapsulated ambiguous VLANs, use the `no` form of this command.

```
encapsulation ambiguous dot1ad {any vlan-id vlan-range} [dot1q {any vlan-range}]
```

**Syntax Description**

- `any` Specifies the matching criteria as any VLAN tag in the range 1 to 4094.
- `vlan-id` VLAN-ID for the outer VLAN.
- `vlan-range` VLAN range for the outer and inner VLANs.
  - The range is given in comma-separated, or hyphen-separated format, or a combination of both.
- `dot1q` Indicates that the IEEE 802.1q standard encapsulation type is used for the inner tag.

**Command Default**

None

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.2.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 5.2.0</td>
<td>The support for outer VLAN range was added in BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The valid combinations of ambiguous VLAN configurations in BNG, with IEEE 802.1ad Provider Bridging (PB) encapsulation type are:

- `encapsulation ambiguous dot1ad {any | vlan-range}`
- `encapsulation ambiguous dot1ad vlan-id dot1q {any | vlan-range}`
- `encapsulation ambiguous dot1ad vlan-range dot1q any`

**Note**

Although `encapsulation ambiguous dot1ad` is supported, it is not commonly used in BNG deployments.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>

These examples show how to configure ambiguous VLANs with IEEE 802.1ad Provider Bridging (PB) encapsulation type on an access-interface.
Single-tagged ambiguous VLAN configuration where the matching criteria for the outer VLAN is specified as any:

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)#interface Bundle-Ether100.10
RP/0/RSP0/CPU0:router(config-subif)#encapsulation ambiguous dot1ad any
```

Ambiguous VLAN configuration where the match criteria for outer VLAN is specified as VLAN-Id and that for inner VLAN is specified as a range:

```
RP/0/RSP0/CPU0:router(config-subif)#encapsulation ambiguous dot1ad 14 dot1q 100,200,300-400
```

Ambiguous VLAN configuration with outer VLAN range:

```
(config-subif)#encapsulation ambiguous dot1ad 1-1000 dot1q any
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>encapsulation ambiguous dot1q, on page 220</td>
<td>Configures encapsulated ambiguous VLANs with IEEE 802.1q encapsulation type, on an access-interface in BNG.</td>
</tr>
</tbody>
</table>
encapsulation ambiguous dot1q

To configure encapsulated ambiguous VLANs with IEEE 802.1q encapsulation type on an access-interface, use the `encapsulation ambiguous dot1q` command in the interface configuration mode. To remove the encapsulated ambiguous VLANs, use the `no` form of this command.

```
encapsulation ambiguous dot1q {any vlan-id vlan-range} [second-dot1q {any vlan-id vlan-range}]
```

### Syntax Description

- **any**: Specifies the matching criteria as `any` VLAN tag in the range 1 to 4094.
- **vlan-id**: VLAN-ID for the outer and inner VLANs. The range is from 0 to 4094.
- **vlan-range**: VLAN range for the outer and inner VLANs. The range is given in comma-separated, or hyphen-separated format, or a combination of both.

### Command Default

None

### Command Modes

Interface configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.2.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.3.1</td>
<td>The support for `encapsulation ambiguous dot1q any second-dot1q { any</td>
</tr>
<tr>
<td>Release 5.2.0</td>
<td>The support for outer VLAN range was added in BNG.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The valid combinations of ambiguous VLAN configurations in BNG, with IEEE 802.1q encapsulation type are:

- `encapsulation ambiguous dot1q {any | vlan-range}
- `encapsulation ambiguous dot1q vlan-id second-dot1q { any | vlan-range}
- `encapsulation ambiguous dot1q any second-dot1q { any | vlan-id}
- `encapsulation ambiguous dot1q vlan-range second-dot1q any

For ambiguous VLAN dot1q configuration where the match criteria is explicitly configured for inner and outer VLAN tags or where a range is specified or where `any` is used for outer VLAN tag, the MTU is calculated by adding 8 bytes (2xdot1q tags) to the default MTU. That is, if default is 1514, the MTU is set to 1522 bytes in such scenarios. Whereas, for configurations where the match criteria for inner VLAN is specified as `any`, the MTU on the sub-interface is calculated by adding 4 (and not 8) bytes to the main interface MTU. That is, 1514 + 4 = 1518 bytes. This behavior is applicable for both physical interfaces and bundle sub-interfaces.
These examples show how to configure ambiguous VLANs with IEEE 802.1q encapsulation type on an access-interface.

Single-tagged ambiguous VLAN configuration where the match criteria for outer VLAN is specified as any:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether100.10
RP/0/RSP0/CPU0:router(config-subif)# encapsulation ambiguous dot1q any
```

Ambiguous VLAN configuration where the match criteria for outer VLAN is specified as VLAN-ID and that for inner VLAN is specified as a range:

```
RP/0/RSP0/CPU0:router(config-subif)# encapsulation ambiguous dot1q 14 second-dot1q 100-200
```

Ambiguous VLAN configuration where the match criteria for outer VLAN and inner VLAN is specified as any:

```
(config-subif)# encapsulation ambiguous dot1q any second-dot1q any
```

Ambiguous VLAN configuration with a single outer VLAN range and inner VLAN specified as any:

```
(config-subif)# encapsulation ambiguous dot1q 1-1000 dot1q any
```

Ambiguous VLAN configuration with 9 outer VLAN ranges and inner VLAN specified as any:

```
(config-subif)# encapsulation ambiguous dot1q 9-18, 19-25, 26, 27-30, 32, 33-40, 42, 43-50, 52 second-dot1q any
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>encapsulation ambiguous dot1ad, on page 218</td>
<td>Configures encapsulated ambiguous VLANs with IEEE 802.1ad Provider Bridging (PB) encapsulation type, on an access-interface in BNG.</td>
</tr>
</tbody>
</table>
show ethernet tags

To display the ethernet tag match information, use the **show ethernet tags** command in EXEC mode.

**show ethernet tags** [interface-type interface-path-id] [detail] [location node-id] [match-order]

**Syntax Description**

- **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.

- **match-order**: Displays the high priority matches first.

**Command Default**

None

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

For ambiguous VLAN dot1q configuration where the match criteria is explicitly configured for inner and outer VLAN tags or where a range is specified or where **any** is used for outer VLAN tag, the MTU is calculated by adding 8 bytes (2xdot1q tags) to the default MTU. That is, if default is 1514, the MTU is set to 1522 bytes in such scenarios. Whereas, for configurations where the match criteria for inner VLAN is specified as **any**, the MTU on the sub-interface is calculated by adding 4 (and not 8) bytes to the main interface MTU. That is, 1514 + 4 = 1518 bytes. This behavior is applicable for both physical interfaces and bundle sub-interfaces.

**Task ID**

- **Task ID**: ethernet-services
- **Operation**: read

This is a sample output of the **show ethernet tags** command:

```
RP/RSP0/CPU0:router#show ethernet tags tengigE 0/0/0/0.1
St:  AD - Administratively Down, Dn - Down, Up - Up
Ly:  L2 - Switched layer 2 service, L3 - Terminated layer 3 service,
     Xtra C - Match on Cos, E - Match on Ethertype, M - Match on source MAC
     -,+, Ingress rewrite operation; number of tags to pop and push respectively

<table>
<thead>
<tr>
<th>Interface</th>
<th>St</th>
<th>MTU</th>
<th>Ly</th>
<th>Outer</th>
<th>Inner</th>
<th>Xtra -,+</th>
</tr>
</thead>
<tbody>
<tr>
<td>Te0/0/0/0.1</td>
<td>Up</td>
<td>1522</td>
<td>L3</td>
<td>.1Q:10</td>
<td>.1Q:100-200</td>
<td>0 0</td>
</tr>
</tbody>
</table>
```
This is a sample output of the `show ethernet tags detail` command for BNG outer VLAN range feature:

```
RP/0/RSP0/CPU0:router#show ethernet tags tengigE 0/1/0/10.12 detail
GigabitEthernet0/1/0/10.12 is up, service is L3
    Interface MTU is 1518
    Outer Match: Dot1Q VLAN 11-20,21-30,31-60,61-100,101-140,141-180,181-220,221-260,261-300
    Inner Match: Dot1Q VLAN any
    Local traffic encap: -
    Pop 0 tags, push none
```
show ethernet tags
DIAMETER Commands

This module describes the Cisco IOS XR software commands used to configure DIAMETER interface 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.

To use commands of this module, 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 any command, contact your AAA administrator for assistance.

- address (DIAMETER), on page 227
- clear diameter peer, on page 228
- clear diameter statistics, on page 229
- destination host, on page 230
- destination realm, on page 231
- diameter attribute list, on page 232
- diameter gx, on page 234
- diameter gx retransmit, on page 235
- diameter gx tx-timer, on page 236
- diameter gy, on page 237
- diameter gy retransmit, on page 238
- diameter gy tx-timer, on page 239
- diameter origin host, on page 240
- diameter origin realm, on page 241
- diameter peer, on page 242
- diameter tls trustpoint, on page 243
- diameter vendor supported, on page 244
- ip vrf forwarding, on page 245
- peer-type, on page 246
- prepaid-config, on page 247
- server (DIAMETER), on page 248
- source-interface (DIAMETER), on page 249
- test aaa group diameter, on page 250
- timer (DIAMETER), on page 252
- transport (DIAMETER), on page 254
- transport security-type, on page 255
• show diameter, on page 256
• show diameter gx, on page 257
• show diameter gy, on page 259
• show diameter nas, on page 261
• show diameter peer, on page 264
• show checkpoint dynamic process (DIAMETER), on page 266
address (DIAMETER)

To configure IPv4 or IPv6 address of DIAMETER peer, use the `address` command in DIAMETER peer configuration mode. To remove the IPv4 or IPv6 address of DIAMETER peer, use the `no` form of this command.

```
address {ipv4 |ipv6} ipaddress
```

**Syntax Description**

*ipaddress* Specifies the IPv4 or IPv6 address of DIAMETER peer.

**Command Default**

None

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to configure an IPv4 address for DIAMETER peer in BNG:

```
RP/0/RSP0/CPU0:router(config)# diameter peer diam_server_1
RP/0/RSP0/CPU0:router(config-dia-peer)# address ipv4 2.2.2.2
```
**clear diameter peer**

To reset DIAMETER peer connection in BNG, use the `clear diameter peer` command in EXEC mode.

```
clear diameter peer  peer-name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer-name</td>
<td>The DIAMETER peer name.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command resets the peer connection. The connection to the peer is re-established after the connection timeout.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>write</td>
</tr>
</tbody>
</table>

This example shows how to reset DIAMETER peer connection in BNG:

```
RP/0/RSP0/CPU0:router# clear diameter peer peer1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear diameter statistics, on page 229</td>
<td>Clears DIAMETER peer statistics in BNG</td>
</tr>
</tbody>
</table>
clear diameter statistics

To clear DIAMETER peer statistics in BNG, use the **clear diameter statistics** command in EXEC mode.

```
clear diameter statistics [{gx|gy|nas}]  
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>gx</td>
<td>(Optional) Clears the statistics of Gx application.</td>
</tr>
<tr>
<td>gy</td>
<td>(Optional) Clears the statistics of Gy application.</td>
</tr>
<tr>
<td>nas</td>
<td>(Optional) Clears the statistics of NAS application.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Executing the **clear diameter statistics** command without any arguments, clears all the DIAMETER peer statistics.

**Task ID**

```
Task ID  Operation
aaa      write
```

This example shows how to clear NAS statistics:

```
RP/0/RSP0/CPU0:router# clear diameter statistics nas
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear diameter peer, on page 228</td>
<td>Resets DIAMETER peer connection in BNG</td>
</tr>
</tbody>
</table>
destination host

To configure the hostname of the DIAMETER peer in BNG, use the destination host command in DIAMETER peer configuration mode. To remove the hostname of the DIAMETER peer, use the no form of this command.

```
destination host  host-name
```

**Syntax Description**

- **host-name**: Specifies the hostname of the DIAMETER peer in Fully Qualified Domain Name (FQDN) format. This value is sent in various messages, so that intermediate proxies can route the packets properly.

**Command Default**

None

**Command Modes**

DIAMETER peer configuration.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to configure the hostname of the DIAMETER peer in BNG:

```
RP/0/RSP0/CPU0:router(config)# diameter peer diam_server_1
RP/0/RSP0/CPU0:router(config-dia-peer)# destination host dcca1.cisco.com
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>destination realm, on page 231</td>
<td>Configures the realm to which the DIAMETER peer belongs to.</td>
</tr>
</tbody>
</table>
destination realm

To configure the realm to which the DIAMETER peer belongs to, use the `destination realm` command in DIAMETER peer configuration mode. To remove the realm configuration, use the `no` form of this command.

```
destination realm realm-string
```

**Syntax Description**
- `realm-string`: Specifies the hostname of the DIAMETER peer in Fully Qualified Domain Name (FQDN) format.
  
  This value is sent in various messages, so that intermediate proxies can route the packets properly.

**Command Default**
- None

**Command Modes**
- DIAMETER peer configuration.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The destination realm is added by the AAA clients while sending a request to AAA server, using `AAA_AT_DESTINATION_REALM` attribute. If this attribute is not present, then the realm information is retrieved using the `User name` field. If the clients do not add the attribute, then the value configured in the peer mode is used while sending messages to the destination peer.

**Task ID**

```
read, write
```

This example shows how to configure the realm to which the DIAMETER peer belongs to:

```
RP/0/RSP0/CPU0:router(config)# diameter peer diam_server_1
RP/0/RSP0/CPU0:router(config-dia-peer)# destination realm GX_REALM
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>destination host, on page 230</td>
<td>Configures the hostname of the DIAMETER peer in BNG.</td>
</tr>
</tbody>
</table>
To configure attribute list parameters for DIAMETER test command in BNG, use the `diameter attribute list` command in Global Configuration mode. To remove this configuration, use the `no` form of this command.

```
diameter attribute list  list-num  [attribute  {attr-id|vendor-id  vendor-id}  attr-format  attr-value  [mandatory]]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>list-num</code></td>
<td>DIAMETER attribute list number. The range is from 0 to 99.</td>
</tr>
<tr>
<td><code>attribute</code></td>
<td>Specifies an attribute definition.</td>
</tr>
<tr>
<td><code>attr-id</code></td>
<td>Attribute ID value. The range is from 1 to 65535.</td>
</tr>
<tr>
<td><code>vendor-id</code></td>
<td>Specifies the vendor ID.</td>
</tr>
<tr>
<td><code>vendor-id</code></td>
<td>Vendor ID value. The range is from 0 to 4294967295.</td>
</tr>
<tr>
<td><code>attr-format</code></td>
<td>Specifies the attribute format. The options are:</td>
</tr>
<tr>
<td></td>
<td>• address</td>
</tr>
<tr>
<td></td>
<td>• binary</td>
</tr>
<tr>
<td></td>
<td>• boolean</td>
</tr>
<tr>
<td></td>
<td>• diameter-identity</td>
</tr>
<tr>
<td></td>
<td>• enum</td>
</tr>
<tr>
<td></td>
<td>• grouped</td>
</tr>
<tr>
<td></td>
<td>• string</td>
</tr>
<tr>
<td></td>
<td>• ulong</td>
</tr>
<tr>
<td><code>attr-value</code></td>
<td>Attribute value as per the attribute format.</td>
</tr>
<tr>
<td></td>
<td>For boolean, enum and ulong formats, the range is from 0 to 4294967295.</td>
</tr>
<tr>
<td></td>
<td>For grouped formats, the range is from 0 to 99.</td>
</tr>
</tbody>
</table>

### Command Default

None
**Command Modes**

- **Global Configuration mode**

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is used along with the `test aaa group diameter` command, to define the attribute list. Based on the attribute list number, the attributes are sent as part of the test command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to configure attribute list parameters for DIAMETER test command in BNG:

```
RP/0/RSP0/CPU0:router(config)# diameter attribute list 1
RP/0/RSP0/CPU0:router(config-dia-attr-list)# attribute vendor-id 0 8 address 5.6.7.8 mandatory
RP/0/RSP0/CPU0:router(config-dia-attr-list)# attribute vendor-id 0 416 enum 1 mandatory
RP/0/RSP0/CPU0:router(config-dia-attr-list)# attribute vendor-id 9 14000 string abcd:abcd:abcd
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>test aaa group diameter</code>, on page 250</td>
<td>Tests various DIAMETER application behaviors in BNG.</td>
</tr>
</tbody>
</table>
**diameter gx**

To enable Gx application in BNG under the DIAMETER process, use the `diameter gx` command in Global Configuration mode. To disable Gx application in BNG, use the `no` form of this command, followed by a DIAMETER process restart.

```
diameter gx
```

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
None

**Command Modes**
Global Configuration mode

**Command History**
```
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

**Note**
The `no` form of this command does not have any impact until followed by a DIAMETER process restart.

The `no diameter gx` command must not be executed when there are active subscriber sessions on the router.

**Task ID**
```
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>
```

This example shows how to enable Gx application in BNG under the DIAMETER process:

```
RP/0/RSP0/CPU0:router(config)# diameter gx
```

**Related Commands**
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>diameter gy, on page 237</code></td>
<td>Enables Gy application in BNG under the DIAMETER process.</td>
</tr>
</tbody>
</table>
```
diameter gx retransmit

To configure the retransmit count for Gx application, use the `diameter gx retransmit` command in Global Configuration mode. To remove this configuration, use the `no` form of this command.

```
diameter gx retransmit count
```

**Syntax Description**

`count` Specifies the value of the retransmit count, in seconds. The range is from 1 to 10; the default is 1.

**Command Default**

If the retransmit count is not configured, it is 1 second, by default.

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to set the retransmit count value to 8 seconds, for Gx application:

```
RP/0/RSP0/CPU0:router(config)# diameter gx retransmit 8
```
diameter gx tx-timer

To configure the transaction timer for Gx application, use the `diameter gx tx-timer` command in Global Configuration mode. To remove this configuration, use the `no` form of this command.

```
diameter gx tx-timer timer-value
```

**Syntax Description**

| timer-value | Specifies the value of the transaction timer in seconds. The range is from 6 to 1000; the default is 15. |

**Command Default**

If the timer value is not configured, it is 15 seconds, by default.

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to set the transaction timer value to 7 seconds for Gx application:

```
RP/0/RSP0/CPU0:router(config)# diameter gx tx-timer 7
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>diameter gy tx-timer, on page 239</td>
<td>Configures the transaction timer for Gy application.</td>
</tr>
</tbody>
</table>
diameter gy

To enable Gy application in BNG under the DIAMETER process, use the `diameter gy` command in Global Configuration mode. To disable Gy application in BNG under the DIAMETER process, use the `no` form of this command, followed by a DIAMETER process restart.

```
diameter gy
```

Syntax Description

The `no` form of this command does not have any impact until followed by a process restart of DIAMETER process.

The `no diameter gy` command must not be executed when there are active subscriber sessions on the router.

Command Default

None

Command Modes

Global Configuration mode

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command is introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Example

This example shows how to enable Gy application in BNG under the DIAMETER process:

```
RP/0/RSP0/CPU0:router(config)# diameter gy
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>diameter gx, on page 234</code></td>
<td>Enables Gx application in BNG under the DIAMETER process.</td>
</tr>
</tbody>
</table>
diameter gy retransmit

To configure the retransmit count for Gy application, use the `diameter gy retransmit` command in Global Configuration mode. To remove this configuration, use the `no` form of this command.

```
diameter gy retransmit count
```

**Syntax Description**

- `count` Specifies the value of the retransmit count, in seconds. The range is from 1 to 10; the default is 1.

**Command Default**

If the retransmit count is not configured, it is 1 second, by default.

**Command Modes**

Global Configuration mode

**Command History**

- **Release 5.3.0**
  - This command was introduced.

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

- `aaa` read, write

This example shows how to set the retransmit count to 8 seconds, for Gy application:

```
RP/0/RSP0/CPU0:router(config)# diameter gy retransmit 8
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>diameter gx retransmit, on page 235</code></td>
<td>Configures the retransmit count for Gx application.</td>
</tr>
</tbody>
</table>
diameter gy tx-timer

To configure the transaction timer for Gy application, use the `diameter gy tx-timer` command in Global Configuration mode. To remove this configuration, enter the `no` form of this command.

```
diameter gy tx-timer timer-value
```

**Syntax Description**

| timer-value | Specifies the value of the transaction timer in seconds. The range is from 6 to 1000; the default is 15. |

**Command Default**

If the timer value is not configured, it is 15 seconds, by default.

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.3.0</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to set the transaction timer value to 7 seconds for Gy application.

```
RP/0/RSP0/CPU0:router(config)# diameter gy tx-timer 7
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>diameter gx tx-timer</code>, on page 236</td>
<td>Configures the transaction timer for Gx application.</td>
</tr>
</tbody>
</table>
diameter origin host

To configure the origin host information of DIAMETER server in BNG, use the `diameter origin host` command in Global Configuration mode. To remove this origin host information of DIAMETER server, use the no form of this command.

```
diameter origin host host-name
```

**Syntax Description**

- `host-name`: Specifies the DIAMETER server's origin host either as a fully qualified domain name (FQDN) or as an IPv4 or IPv6 address.

**Command Default**

The origin host is set as a null string.

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If you do not specify the origin host, a null string is assumed as the origin host name. Therefore, this is a mandatory configuration.

**Task ID**

- aaa: read, write

**Example**

This example shows how to configure the DIAMETER origin host information in BNG:

```
RP/0/RSP0/CPU0:router(config)# diameter origin host BNG-1.cisco.com
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>diameter origin realm, on page 241</td>
<td>Configures the origin realm information of DIAMETER server in BNG.</td>
</tr>
</tbody>
</table>
**diameter origin realm**

To configure the origin realm information of DIAMETER server in BNG, use the `diameter origin realm` command in Global Configuration mode. To remove this origin realm information of DIAMETER server, use the **no** form of this command.

```
diameter origin realm realm-string
```

**Syntax Description**

- **realm-string**: Specifies the DIAMETER origin realm string either as a fully qualified domain name (FQDN) or as an IPv4 or IPv6 address.

**Command Default**

The default realm name string is a null string.

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command is introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If you do not specify the origin realm, a null string is assumed as the origin realm name. Therefore, this is a mandatory configuration.

**Example**

This example shows how to configure the origin realm information of DIAMETER server in BNG:

```
RP/0/RSP0/CPU0:router(config)# diameter origin realm cisco.com
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>diameter origin host, on page 240</td>
<td>Configures the origin host information of DIAMETER server in BNG.</td>
</tr>
</tbody>
</table>
diameter peer

To configure a DIAMETER peer and to enter the DIAMETER peer sub-configuration mode in BNG, use the `diameter peer` command in Global Configuration mode. To remove the diameter peer configuration, use the `no` form of this command.

```
diameter peer peer-name
```

**Syntax Description**

| peer-name | Specifies the name of the diameter peer. |

**Command Default**

None

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to configure a DIAMETER peer in BNG:

```
RP/0/RSP0/CPU0:router(config)# diameter peer diam_server_1
RP/0/RSP0/CPU0:router(config-dia-peer)#
```
diameter tls trustpoint

To configure the trustpoint name to be used in the certificate to be used for DIAMETER TLS exchange, use the **diameter tls trustpoint** command in Global Configuration mode. To remove the DIAMETER trustpoint configuration, use the **no** form of this command.

```
diameter tls trustpoint label
```

**Syntax Description**

<table>
<thead>
<tr>
<th>label</th>
<th>Specifies the trustpoint label name to be used for DIAMETER TLS exchange.</th>
</tr>
</thead>
</table>

**Command Default**

None

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If no trustpoint is provided, then the default trustpoint is used.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to configure the trustpoint label name to be used for DIAMETER TLS exchange:

```
RP/0/RSP0/CPU0:router(config)# diameter tls trustpoint trustpoint1
```
diameter vendor supported

To specify the vendor attribute-value pairs (AVPs) that the DIAMETER node can recognize, use the diameter vendor supported command in Global Configuration mode. This information is passed to the peer in capability exchange messages. To remove this configuration, use the no form of this command.

```
diameter vendor supported {cisco etsi 3gpp vodafone}
```

**Syntax Description**

- `cisco` Specifies that Cisco AVPs are recognized by the DIAMETER node.
- `etsi` Specifies that ETSI AVPs are recognized by the DIAMETER node.
- `3gpp` Specifies that 3GPP AVPs are recognized by the DIAMETER node.
- `vodafone` Specifies that Vodafone AVPs are recognized by the DIAMETER node.

**Command Default**

None

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.3.0</td>
<td>This command is introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can have multiple vendors' AVPs supported. So, you can run this command multiple times with a different vendor ID on each instance.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to specify that the DIAMETER node recognizes Cisco AVPs:

```
RP/0/RSP0/CPU0:router(config)# diameter vendor supported cisco
```
ip vrf forwarding

To configure the VRF associated with the DIAMETER peer, to establish connections with the peers immediately after configuring them, use the `ip vrf forwarding` command in DIAMETER peer configuration mode. To remove the VRF associated with the peer, use the `no` form of this command.

```
ip vrf forwarding  vrf_table_name
```

**Syntax Description**
- `vrf_table_name` Name of the VRF table.

**Command Default**
None

**Command Modes**
DIAMETER peer configuration.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
If this command is not configured, then the global routing table is used for establishing the connection with the peer.

If the VRF associated with the name is not configured, then an error message mentioning so is displayed, and this command does not have any effect.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to configure the VRF associated with the DIAMETER peer:

```
RP/0/RSP0/CPU0:router(config)# diameter peer diam_server_1
RP/0/RSP0/CPU0:router(config-dia-peer)# ip vrf forwarding VRF1
```
peer-type

To configure the DIAMETER peer type in BNG, use the `peer-type` command in DIAMETER peer configuration mode. To remove the DIAMETER peer type configuration, use the `no` form of this command.

```
peer-type server
```

**Syntax Description**

- `server` Specifies that the DIAMETER peer is a server.

**Command Default**

None

**Command Modes**

DIAMETER peer configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

By default, the `peer-type` is `server`.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read,</td>
</tr>
<tr>
<td></td>
<td>write</td>
</tr>
</tbody>
</table>

This example shows how to configure the DIAMETER peer type in BNG:

```
RP/0/RSP0/CPU0:router(config)# diameter peer diam_server_1
RP/0/RSP0/CPU0:router(config-dia-peer)# peer-type server
```
**prepaid-config**

To configure prepaid feature in BNG, use the `prepaid-config` command in dynamic template type service configuration mode. To remove this prepaid feature configuration, use the `no` form of this command.

```
prepaid-config feature-name
```

**Syntax Description**
- `feature-name` Pre-configured prepaid feature name.

**Command Default**
None

**Command Modes**
Dynamic template type service

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
You must use already defined subscriber prepaid feature to program the feature name in dynamic template. Service accounting configuration (using `accounting aaa list default type service` command) is mandatory for the functioning of prepaid services.

**Task ID**
- **Task ID**: config-services
- **Operation**: read, write

This example shows how to configure prepaid feature in BNG:

```
RP/0/RSP0/CPU0:router(config)# dynamic-template
RP/0/RSP0/CPU0:router(config-dynamic-template)# type service service1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# prepaid-config feature1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# accounting aaa list default type service
```
server (DIAMETER)

To attach the globally configured DIAMETER server (having the same name) to the server group, use the `server` command in DIAMETER server group configuration mode. To detach the globally configured DIAMETER server from the server group, use the `no` form of this command.

```
server peer-name
```

**Syntax Description**
- `peer-name`: Specifies the name of DIAMETER peer.

**Command Default**
None

**Command Modes**
DIAMETER server group configuration

**Command History**
- **Release 5.3.0**: This command was introduced.

**Usage Guidelines**
If a server is not configured globally with the same `peer_name`, then an error message saying so is displayed.

To configure the DIAMETER server globally, use `diameter peer peer_name` command in global configuration mode.

Unlike for RADIUS, DIAMETER does not have private servers. DIAMETER considers a server that does not have a VRF name configured, as a global server, and it uses global routing table for that particular server.

**Task ID**

```
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>
```

This example shows how to attach the globally configured DIAMETER server (having the same name) to the server group in BNG:

```
RP/0/RSP0/CPU0:router(config)# aaa group server diameter GX_SG
RP/0/RSP0/CPU0:router(config-sg-diameter)# server GX_SERVER
```
source-interface (DIAMETER)

To configure the source-interface to be used for the DIAMETER connection in BNG, use the source-interface command in DIAMETER peer configuration mode. To remove the source-interface used for the DIAMETER connection, use the no form of this command.

```
source-interface  interface-type  interface-instance
```

**Syntax Description**

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

- DIAMETER peer configuration
- Global Configuration mode (when used with `diameter` keyword)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The DIAMETER client uses this source address and port to initiate the TCP connection to the peer.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to configure the source-interface (in DIAMETER peer configuration mode) to be used for the DIAMETER connection in BNG:

```
RP/0/RSP0/CPU0:router(config)# diameter peer diam_server_1
RP/0/RSP0/CPU0:router(config-dia-peer)# source-interface bundle-ether 1.1
```

This example shows how to configure the source-interface (in global configuration mode) to be used for the DIAMETER connection in BNG:

```
RP/0/RSP0/CPU0:router(config)# diameter source-interface bundle-ether 1.1
```
test aaa group diameter

To test various DIAMETER application behaviors in BNG, use the test aaa group diameter command in EXEC mode.

test aaa group diameter {dcca|policy-if} list-num server-group timeout timeout-val

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dcca</td>
<td>Tests DIAMETER DCCA application messages.</td>
</tr>
<tr>
<td>policy-if</td>
<td>Tests DIAMETER policy interface application messages.</td>
</tr>
<tr>
<td>list-num</td>
<td>DIAMETER attribute list number.</td>
</tr>
<tr>
<td>server-group</td>
<td>Specifies the configured server group to be used for testing.</td>
</tr>
<tr>
<td>timeout</td>
<td>Specifies the duration that the test process need to wait for the response.</td>
</tr>
<tr>
<td>timeout-val</td>
<td>Timeout value, in seconds. The range is from 1 to 99. The value must be greater than or equal to 5.</td>
</tr>
</tbody>
</table>

Command Default

None

Command Modes

EXEC mode

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

You must use diameter attribute list command, to define the attribute list required for this test command.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to execute the test aaa group diameter command in BNG:
RP/0/RSP0/CPU0:router# test aaa group diameter policy-if 1 default timeout 5

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>diameter attribute list, on page 232</td>
<td>Configures attribute list parameters for DIAMETER test command in BNG.</td>
</tr>
</tbody>
</table>
timer (DIAMETER)

To configure various DIAMETER base protocol timers, use the `timer` command in DIAMETER peer configuration mode or in Global Configuration mode (along with `diameter` keyword). To remove the DIAMETER base protocol timers, use the `no` form of this command.

```
timer {connection|transaction|watchdog} timer-value
```

**Syntax Description**
- **connection**: Specifies the DIAMETER base protocol timer used for setting the frequency of transport connection attempts with the peer when there is no active connection to the peer. This timer is used to delay the connection establishment or re-establishment of client with the DIAMETER server.
- **transaction**: Specifies the timer used for setting the frequency of transaction attempts. That is, the duration for which the client waits for any response message from the peer.
- **watchdog**: Specifies the timer used to periodically send the Device-Watch-Dog to the DIAMETER server to test the link status.
- **timer-value**: Specifies the value for various DIAMETER base protocol timers. The range, in seconds, for `transaction` timer is from 1 to 1000; the default is 5. The range, in seconds, for `connection` timer and `watchdog` timer is from 6 to 1000; the default is 30.

**Command Default**
None

**Command Modes**
- DIAMETER peer configuration.
- Global Configuration mode (when used with `diameter` keyword).
A connection timer value of zero (0) does not trigger any retry for the connection establishment. When the `no` form of connection timer command is issued, a default timer of 30 seconds is started. The connection retry does not trigger immediately.

The algorithm used for sending the watchdog messages, is based on RFC3539.

The DIAMETER base protocol timers can be configured globally and at the peer level. By default, the peers inherit the globally configured timer values. But, if the timer values are configured at peer level as well, then the peer level timer values take precedence over the globally configured timer values.

This example shows how to configure the DIAMETER base protocol watchdog timer (in DIAMETER peer configuration mode) in BNG:

```
RP/0/RSP0/CPU0:router(config)# diameter peer diam_server_1
RP/0/RSP0/CPU0:router(config-dia-peer)# timer watchdog 300
```

This example shows how to configure the DIAMETER base protocol watchdog timer (in global configuration mode) in BNG:

```
RP/0/RSP0/CPU0:router(config)# diameter timer watchdog 300
```
transport (DIAMETER)

To configure the DIAMETER transport protocol to be used for establishing connection with the peer, use the transport command in DIAMETER peer configuration mode. To remove the DIAMETER transport protocol configuration, use the no form of this command.

`transport tcp port port_num`

### Syntax Description

`port_num` Specifies the port number that the remote peer uses for DIAMETER messages. The range is from 1 to 65535; the default is 3868.

### Command Default

If the `port_num` is not configured, 3868 becomes the default port number.

### Command Modes

DIAMETER peer configuration.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Currently, only tcp is supported as the DIAMETER transport protocol in BNG.

When the `no` form of the command is issued, all the sessions that are bound to the peer cannot use the connection anymore. In that case, the applications that initiated the pending messages, if any in the queue, are notified so that they can try alternate peers.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to configure the DIAMETER transport protocol to be used for establishing connection with the peer:

```
RP/0/RSP0/CPU0:router (config)# diameter peer diam_server_1
RP/0/RSP0/CPU0:router (config-dia-peer)# transport tcp port 3868
```
transport security-type

To configure the security protocol to be used for the DIAMETER connection in BNG, use the transport security-type command in DIAMETER peer configuration mode. To remove the DIAMETER security protocol configuration, use the no form of this command.

**transport security-type tls**

**Syntax Description**

| tls | Specifies Transport Layer Security (TLS) as the security protocol to be used for the DIAMETER connection. |

**Command Default**

None

**Command Modes**

DIAMETER peer configuration.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Currently, only tls is supported as the security protocol to be used for the DIAMETER connection in BNG. The default security mechanism is none. When the security mechanism is changed dynamically, the connection to the peer is torn down and re-established.

If the destination host is configured under the peer, that is also verified against the server certificate.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read,</td>
</tr>
<tr>
<td></td>
<td>write</td>
</tr>
</tbody>
</table>

This example shows how to configure the security protocol to be used for the DIAMETER connection in BNG:

```
RP/0/RSP0/CPU0:router(config)# diameter peer diam_server_1
RP/0/RSP0/CPU0:router(config-dia-peer)# transport security-type tls
```
show diameter

To display global DIAMETER statistics in BNG, use the show diameter command in EXEC mode.

show diameter

Syntax Description
This command has no keywords or arguments.

Command Default
None

Command Modes
EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines
No specific guidelines impact the use of this command.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read</td>
</tr>
</tbody>
</table>

This is a sample output for the show diameter command:

```
RP/0/RSP0/CPU0:router# show diameter
Origin Host : abc@xyz.com
Origin Realm : xyz.com
Source Interface :
TLS Trustpoint :
Connection timer value : 30 seconds
Watchdog timer value : 30 seconds
Transaction timer value : 5 seconds
Number of Peers:2
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show diameter peer, on page 264</td>
<td>Displays DIAMETER peer information in BNG.</td>
</tr>
<tr>
<td>show diameter gx, on page 257</td>
<td>Displays the status of DIAMETER Gx application in BNG.</td>
</tr>
<tr>
<td>show diameter gy, on page 259</td>
<td>Displays the status of DIAMETER Gy application in BNG.</td>
</tr>
<tr>
<td>show diameter nas, on page 261</td>
<td>Displays the DIAMETER Network Access Server (NAS) information in BNG.</td>
</tr>
<tr>
<td>show checkpoint dynamic process (DIAMETER), on page 266</td>
<td>Displays the checkpoint information of DIAMETER process.</td>
</tr>
</tbody>
</table>
**show diameter gx**

To display the status of DIAMETER Gx application in BNG, use the `show diameter gx` command in EXEC mode.

`show diameter gx [checkpoint session-id|session session-id|statistics ]`

**Syntax Description**

- `checkpoint session-id` (Optional) Displays checkpoint information of Gx application.
- `session session-id` (Optional) Displays session information of Gx application.
- `statistics` (Optional) Displays Gx application statistics.

**Command Default**
None

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read</td>
</tr>
</tbody>
</table>

This is a sample output for the `show diameter gx statistics` command:

```
RP/0/RSP0/CPU0:router# show diameter gx statistics
CCR Initial Messages : 1
CCR Initial Messages Sent Failed : 0
CCR Initial Messages Timed Out : 0
CCR Initial Messages Retry : 0
CCR Update Messages : 0
CCR Update Messages Sent Failed : 0
CCR Update Messages Timed Out : 0
CCR Update Messages Retry : 0
CCR Terminate Messages : 0
CCR Terminate Messages Sent Failed : 0
CCR Terminate Messages Timed Out : 0
CCR Terminate Messages Retry : 0
CCA Initial Messages : 1
CCA Initial Messages Error : 0
CCA Update Messages : 0
CCA Update Messages Error : 0
CCA Terminate Messages : 0
CCA Terminate Messages Error : 0
```
RAR Received Messages : 0
RAR Received Messages Error : 0
RAA Sent Messages : 0
RAA Sent Messages Error : 0
ASR Received Messages : 0
ASR Received Messages Error : 0
ASA Sent Messages : 0
ASA Sent Messages Error : 0
Session Termination Messages Recvd : 0
Unknown Request Messages : 0
Restored Sessions : 0
Total Opened Sessions : 1
Total Closed Sessions : 0
Total Active Sessions : 1

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show diameter gy, on page 259</td>
<td>Displays the status of DIAMETER Gy application in BNG.</td>
</tr>
<tr>
<td>show diameter nas, on page 261</td>
<td>Displays the DIAMETER Network Access Server (NAS) information in BNG.</td>
</tr>
</tbody>
</table>
**show diameter gy**

To display the status of DIAMETER Gy application in BNG, use the `show diameter gy` command in EXEC mode.

```
show diameter gy [{checkpoint session-id} [session session-id] statistics]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>checkpoint</td>
<td>(Optional) Displays checkpoint information of specific Gx application.</td>
</tr>
<tr>
<td>session session-id</td>
<td>(Optional) Displays specific Gy application information.</td>
</tr>
<tr>
<td>statistics</td>
<td>(Optional) Displays Gy application statistics.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read</td>
</tr>
</tbody>
</table>

This is a sample output for the `show diameter gy statistics` command:

```
RP/0/RSP0/CPU0:router# show diameter gy statistics

CCR Initial Messages : 1
CCR Initial Messages Sent Failed : 0
CCR Initial Messages Timed Out : 0
CCR Initial Messages Retry : 0
CCR Update Messages : 4
CCR Update Messages Sent Failed : 0
CCR Update Messages Timed Out : 0
CCR Update Messages Retry : 0
CCR Terminate Messages : 1
CCR Terminate Messages Sent Failed : 0
CCR Terminate Messages Timed Out : 0
CCR Terminate Messages Retry : 0
CCA Initial Messages : 1
CCA Initial Messages Error : 0
CCA Update Messages : 4
CCA Update Messages Error : 0
CCA Terminate Messages : 1
CCA Terminate Messages Error : 0
RAR Received Messages : 0
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show diameter gx, on page 257</td>
<td>Displays the status of DIAMETER Gx application in BNG.</td>
</tr>
<tr>
<td>show diameter nas, on page 261</td>
<td>Displays the DIAMETER Network Access Server (NAS) information in BNG.</td>
</tr>
</tbody>
</table>
show diameter nas

To display the DIAMETER Network Access Server (NAS) information in BNG, use the `show diameter nas` command in EXEC mode.

```
show diameter nas  [{checkpoint session-id|session session-id|summary}]
```

**Syntax Description**

- `checkpoint session-id` (Optional) Displays checkpoint information of specific NAS session.
- `session session-id` (Optional) Displays specific NAS session information.
- `summary` (Optional) Displays summary of NAS sessions.

**Command Default**

None

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read</td>
</tr>
</tbody>
</table>

This is a sample output for the `show diameter nas session` command:

```
RP/0/RSP0/CPU0:router# show diameter nas session 00070a6f

Nas Session status for [00070a6f]
  Session Status       : Active
  Diameter Session ID  : 1.1.1.1;4;461423;1187179

  Authentication Status : NA
  Authorization Status  : SUCCESS
  Accounting Status (Start) : NA
  Accounting Status (Stop)   : NA
  Disconnect status        : NA

Peer Information:
  Server group       : NASREQ_SG
  Server Used        : NASREQ_SERVER
```

This is a sample output for the `show diameter nas summary` command:

```
RP/0/RSP0/CPU0:router# show diameter nas summary
```
NAS Statistics:

NAS Initiated msgs:

Authentication ::

In : 0 Out : 0
Requests received : 0 Requests send : 0
Response received : 0 Result forwarded : 0
Transaction Succeeded : 0 Transactions Failed : 0

Authorization ::

In : 1 Out : 1
Requests received : 1 Requests send : 1
Response received : 1 Result forwarded : 1
Transaction Succeeded : 1 Transactions Failed : 0

Accounting (Start) ::

In : 0 Out : 0
Requests received : 0 Requests send : 0
Response received : 0 Result forwarded : 0
Transaction Succeeded : 0 Transactions Failed : 0

Accounting (Stop) ::

In : 0 Out : 0
Requests received : 0 Requests send : 0
Response received : 0 Result forwarded : 0
Transaction Succeeded : 0 Transactions Failed : 0

Accounting (Interim) ::

In : 0 Out : 0
Requests received : 0 Requests send : 0
Response received : 0 Result forwarded : 0
Transaction Succeeded : 0 Transactions Failed : 0

Disconnect ::

In : 0 Out : 0
Requests received : 0 Requests send : 0
Response received : 0 Result forwarded : 0
Transaction Succeeded : 0 Transactions Failed : 0

Server Initiated msgs:

Coa (RAR) ::

In : 0 Out : 0
Requests received : 0 Requests send : 0
Response received : 0 Result forwarded : 0
Transaction Succeeded : 0 Transactions Failed : 0

POD (ASR) ::

In : 0 Out : 0
Requests received : 0 Requests send : 0
Response received : 0 Result forwarded : 0
Transaction Succeeded : 0 Transactions Failed : 0

Diameter NAS summary
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show diameter gx, on page 257</td>
<td>Displays the status of DIAMETER Gx application in BNG.</td>
</tr>
<tr>
<td></td>
<td>show diameter gy, on page 259</td>
<td>Displays the status of DIAMETER Gy application in BNG.</td>
</tr>
</tbody>
</table>
show diameter peer

To display the DIAMETER peer information in BNG, use the `show diameter peer` command in EXEC mode.

```
show diameter peer peer-name
```

**Syntax Description**

| peer peer-name | Specifies the name of the DIAMETER peer. |

**Command Default**

None

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read</td>
</tr>
</tbody>
</table>

This is a sample output for the `show diameter peer` command:

```
RP/0/RSP0/CPU0:router# show diameter peer peer1
Origin Host : test
Origin Realm : testrealm
Source Interface :
TLS Trustpoint :
Connection timer value : 30 seconds
Watchdog timer value : 30 seconds
Transaction timer value : 30 seconds
Peer name : peer1
type : SERVER
Address/port : 01010101/3868
Transport protocol : TCP
Peer security protocol : NONE
connection timer : 30 seconds
watchdog timer value : 30 seconds
transaction timer value : 30 seconds
VRF name : default
Source-interface :
Destination realm :
Destination host name :
Peer connection status : Closed

Peer Statistics
---------------------
IN / OUT
---------------------
ASR 0 / 0
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show diameter gx, on page 257</td>
<td>Displays the status of DIAMETER Gx application in BNG.</td>
</tr>
<tr>
<td>show diameter gy, on page 259</td>
<td>Displays the status of DIAMETER Gy application in BNG.</td>
</tr>
<tr>
<td>show diameter nas, on page 261</td>
<td>Displays the DIAMETER Network Access Server (NAS) information in BNG.</td>
</tr>
</tbody>
</table>
show checkpoint dynamic process (DIAMETER)

To display the checkpoint information of DIAMETER process, use the `show checkpoint diameter process` command in the EXEC mode mode.

```
show checkpoint dynamic process process-name
```

**Syntax Description**

- `process-name` Name of the process (in this case, `diameter`) for which the checkpoint information must be displayed.

**Command Default**

None

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read</td>
</tr>
</tbody>
</table>

This is a sample output of the `show checkpoint dynamic process diameter` command:

```
RP/0/RSP0/CPU0:router# show checkpoint dynamic process diameter

Name       Version ID     Seg #Objects Length InfoLen Flags
---------------------------------------------------------------
0x00000003 0, 0, 0x400001c00 M 0 292 4 I M
0x00000004 0, 0, 0x400001d00 M 1 264 4 I M
0x00000002 0, 0, 0x400001e00 M 1 24 4 I M
0x00000001 0, 0, 0x400001f00 M 1 24 4 I M

Segment 0: Number of pages allocated: 4
Segment 0: Number of pages free: 3
Segment 1: Number of pages allocated: 9
Segment 1: Number of pages free: 3
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show diameter peer, on page 264</code></td>
<td>Displays DIAMETER peer information in BNG.</td>
</tr>
<tr>
<td><code>show diameter gx, on page 257</code></td>
<td>Displays the status of DIAMETER Gx application in BNG.</td>
</tr>
</tbody>
</table>
### DIAMETER Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show diameter gy, on page 259</code></td>
<td>Displays the status of DIAMETER Gy application in BNG.</td>
</tr>
<tr>
<td><code>show diameter nas, on page 261</code></td>
<td>Displays the DIAMETER Network Access Server (NAS) information in BNG.</td>
</tr>
</tbody>
</table>
show checkpoint dynamic process (DIAMETER)
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*.

To use commands of this module, 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 any command, contact your AAA administrator for assistance.

- dynamic-template, on page 270
- dynamic-template type ips subscriber, on page 271
- dynamic-template type ppp, on page 272
- dynamic-template type service, on page 273
- monitor-session (interface-dynamic-template-BNG), on page 274
- service-policy (BNG), on page 276
- test radius coa activate, on page 278
- timeout idle, on page 280
- vrf (dynamic-template-BNG), on page 282
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}
```

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dynamic-template type ppp, on page 272</td>
<td>Enables the <code>ppp</code> dynamic template type.</td>
</tr>
<tr>
<td>dynamic-template type ipsubscriber, on page 271</td>
<td>Enables the <code>ipsubscriber</code> dynamic template type.</td>
</tr>
<tr>
<td>dynamic-template type service, on page 273</td>
<td>Enables the <code>service</code> dynamic template type.</td>
</tr>
</tbody>
</table>
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`

**Syntax Description**

`template-name` Specifies the dynamic template name.

**Command Default**

None

**Command Modes**

Dynamic template configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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 ipsb1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dynamic-template, on page 270</td>
<td>Enables the dynamic template configuration mode.</td>
</tr>
<tr>
<td>dynamic-template type ppp, on page 272</td>
<td>Enables the ppp dynamic template type.</td>
</tr>
<tr>
<td>dynamic-template type service, on page 273</td>
<td>Enables the service dynamic template type.</td>
</tr>
</tbody>
</table>
**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.

**Syntax Description**

```
dynamic-template type ppp template-name
```

- **template-name** specifies the dynamic template name.

**Command Default**

None

**Command Modes**

Dynamic template configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dynamic-template, on page 270</td>
<td>Enables the dynamic template configuration mode.</td>
</tr>
<tr>
<td>dynamic-template type ipsubscriber, on page 271</td>
<td>Enables the ipsubscriber dynamic template type.</td>
</tr>
<tr>
<td>dynamic-template type service, on page 273</td>
<td>Enables the service dynamic template type.</td>
</tr>
</tbody>
</table>
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
```

**Syntax Description**

- `template-name` Specifies the dynamic template name.

**Command Default**

None

**Command Modes**

Dynamic template configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

- `config-services read, write`

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dynamic-template, on page 270</td>
<td>Enables the dynamic template configuration mode.</td>
</tr>
<tr>
<td>dynamic-template type ppp, on page 272</td>
<td>Enables the ppp dynamic template type.</td>
</tr>
<tr>
<td>dynamic-template type ipsubscriber, on page 271</td>
<td>Enables the ipsubscriber dynamic template type.</td>
</tr>
</tbody>
</table>
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}]  [port-level]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>session-name</code></td>
<td>Name of the monitor session to configure.</td>
</tr>
<tr>
<td><code>direction</code></td>
<td>Specifies that traffic replication is in only one direction.</td>
</tr>
<tr>
<td><code>rx-only</code></td>
<td>Specifies that only ingress traffic is replicated.</td>
</tr>
<tr>
<td><code>tx-only</code></td>
<td>Specifies that only egress traffic is replicated.</td>
</tr>
</tbody>
</table>

**Command Default**

Replicates both ingress and egress traffic.

**Command Modes**

Interface configuration
Dynamic template configuration (for BNG)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.0.0</td>
<td>The <code>acl</code> and <code>mirror first</code> keywords were added.</td>
</tr>
<tr>
<td>Release 5.1</td>
<td>The support for this command under dynamic-template configuration mode was added for BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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.

If a physical interface is configured for Layer 3, then the traffic mirroring session can be associated on physical interfaces. Example:

```
interface TenGigE0/1/0/0
ipv4 address 10.0.0.1 255.255.255.0
```
If a physical interface has sub-interfaces configured for Layer 3, then the traffic mirroring session must be associated on each sub-interface. Example:

```bash
interface TenGigE0/1/0/1.601
ipv4 address 10.0.1.1 255.255.255.0
encapsulation dot1q 601
```

For more information about monitoring a session, see Configuring Traffic Monitoring chapter in Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

This example shows how to enter monitor session configuration mode:

```bash
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
```

This example shows how to configure `monitor-session` command in the dynamic-template configuration mode for BNG:

```bash
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
```

```bash
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]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>input</td>
<td>Configures an ingress service-policy.</td>
</tr>
<tr>
<td>output</td>
<td>Configures an egress service-policy.</td>
</tr>
<tr>
<td>type</td>
<td>Creates the service policy for policy-based routing (PBR).</td>
</tr>
<tr>
<td>service-policy_name</td>
<td>Name of the service policy.</td>
</tr>
<tr>
<td>acct-stats</td>
<td>(Optional) Enables service accounting.</td>
</tr>
<tr>
<td>merge</td>
<td>(Optional) Enables the policy to be merged.</td>
</tr>
<tr>
<td>seq_num</td>
<td>Sequence number of the policy. Range is from 0 to 255.</td>
</tr>
</tbody>
</table>

### Command Default

None

### Command Modes

Dynamic template configuration mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.3.0</td>
<td>Support was added for policy based routing.</td>
</tr>
<tr>
<td>4.3.1</td>
<td><strong>acct-stats</strong> and <strong>merge</strong> keywords were added to support service accounting and policy merge features.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

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

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This is an example of configuring the **service-policy** command in the dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router# configure
```
This example shows how to enable service accounting feature in the dynamic template configuration mode using `service-policy` command:

```plaintext
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
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# 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:

```plaintext
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="#">dynamic-template, on page 270</a></td>
<td>Enables the dynamic template configuration mode.</td>
</tr>
<tr>
<td><a href="#">dynamic-template type ppp, on page 272</a></td>
<td>Enables the ppp dynamic template type.</td>
</tr>
<tr>
<td><a href="#">dynamic-template type ipsubscriber, on page 271</a></td>
<td>Enables the ipsubscriber dynamic template type.</td>
</tr>
<tr>
<td><a href="#">accounting aaa list type service, on page 28</a></td>
<td>Configures service accounting feature.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>service</td>
<td>Specifies the service to be activated or de-activated.</td>
</tr>
<tr>
<td>name</td>
<td>Name of the service, which is same as the dynamic-template name.</td>
</tr>
<tr>
<td>acct-ses-id</td>
<td>Specifies the accounting session ID of the subscriber on which the template is to be activated or de-activated.</td>
</tr>
<tr>
<td>id</td>
<td>ID of the accounting session, in hexadecimal format.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

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
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor-session</td>
<td>Defines a traffic mirroring session and enters monitor session configuration mode.</td>
</tr>
<tr>
<td>monitor-session (interface-dynamic-template-BNG)</td>
<td>Associates a traffic mirroring session with a specific interface or dynamic template.</td>
</tr>
<tr>
<td>show monitor-session status</td>
<td>Displays status information about configured traffic mirroring sessions.</td>
</tr>
<tr>
<td>show monitor-session counters</td>
<td>Displays statistics regarding traffic mirroring sessions.</td>
</tr>
<tr>
<td>clear monitor-session counters</td>
<td>Clears the traffic mirroring session statistics.</td>
</tr>
</tbody>
</table>
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}]`

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.2.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 5.1</td>
<td>The support for <code>threshold</code> and <code>traffic</code> keywords were added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show subscriber feature accounting</code>, on page 588</td>
<td>Displays the feature accounting information of the subscriber.</td>
</tr>
</tbody>
</table>
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
```

**Syntax Description**

- `vrf-name` Specifies the name of the vrf.

**Command Default**

None

**Command Modes**

Dynamic template type configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dynamic-template</code>, on page 270</td>
<td>Enables the dynamic template configuration mode.</td>
</tr>
<tr>
<td><code>dynamic-template type ppp</code>, on page 272</td>
<td>Enables the ppp dynamic template type.</td>
</tr>
<tr>
<td><code>dynamic-template type ipsubscriber</code>, on page 271</td>
<td>Enables the ipsubscriber dynamic template type.</td>
</tr>
</tbody>
</table>
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.*

To use commands of this module, 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 any command, contact your AAA administrator for assistance.

- `lpts punt excessive-flow-trap`, on page 284
- `lpts punt excessive-flow-trap dampening`, on page 285
- `lpts punt excessive-flow-trap interface-based-flow`, on page 286
- `lpts punt excessive-flow-trap non-subscriber-interfaces`, on page 287
- `lpts punt excessive-flow-trap penalty-rate`, on page 288
- `lpts punt excessive-flow-trap penalty-timeout`, on page 290
- `lpts punt excessive-flow-trap subscriber-interfaces`, on page 292
- `show lpts punt excessive-flow-trap`, on page 293
- `show lpts punt excessive-flow-trap information`, on page 296
- `show lpts punt excessive-flow-trap interface`, on page 299
- `show lpts punt excessive-flow-trap protocol`, on page 301
**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.

```plaintext
lpts punt excessive-flow-trap {subscriber-interfaces|non-subscriber-interfaces|penalty-rate|penalty-timeout}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>subscriber-interfaces</td>
<td>Enables the Excessive Punt Flow Trap for subscriber interfaces.</td>
</tr>
<tr>
<td>non-subscriber-interfaces</td>
<td>Enables the Excessive Punt Flow Trap for non-subscriber interfaces.</td>
</tr>
<tr>
<td>penalty-rate</td>
<td>Sets the penalty policing rate for a protocol.</td>
</tr>
<tr>
<td>penalty-timeout</td>
<td>Sets the penalty timeout for a protocol.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show lpts punt excessive-flow-trap</code>, on page 293</td>
<td>Displays the bad actor flows trapped by the Excessive Punt Flow Trap feature.</td>
</tr>
</tbody>
</table>
lpts punt excessive-flow-trap dampening

To enable false positive suppression through dampening, use the `lpts punt excessive-flow-trap dampening` command in Global Configuration mode. To remove this configuration, use the `no` form of this command.

```
lpts punt excessive flow trap dampening [time]
```

**Syntax Description**

- `time`  The time (in milliseconds) within which a second bad actor notification must arrive to consider the flow as a repeated offender.

  The range is from 1 to 60000; the default is 30000 milliseconds (30 seconds).

**Command Default**

By default, the dampening feature is disabled.

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.3.0</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to configure a dampening time of 40 milliseconds:

```
RP/0/RSP0/CPUD:router#configure
RP/0/RSP0/CPUD:router(config)#lpts punt excessive-flow-trap dampening 40
```
lpts punt excessive-flow-trap interface-based-flow

To enable interface-based flow (that is, considering all the packets received on a non-subscriber interface, irrespective of the source MAC address, to be a part of a single flow), use the `lpts punt excessive-flow-trap interface-based-flow` command in Global Configuration mode. To remove this interface-based flow configuration, use the `no` form of this command.

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
None

**Command Modes**
Global Configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.3.0</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Users cannot enable this command, if EPFT is turned on for the subscriber-interfaces and non-subscriber-interfaces MAC or vice versa. This is because, interface-based flow feature is mutually exclusive with MAC-based EPFT on non-subscriber interface feature.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example show how to enable interface-based flow:

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)#lpts punt excessive-flow-trap interface-based-flow
```
**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.

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mac</code></td>
<td>Enables MAC-based EPFT on non-subscriber interface.</td>
</tr>
</tbody>
</table>

### Command Default
None

### Command Modes
Global Configuration mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.3.0</td>
<td>The command was modified to add <code>mac</code> keyword to enable MAC-based EPFT on non-subscriber interfaces.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The user cannot enable `lpts punt excessive-flow-trap interface-based-flow` command, if EPFT is turned on for the subscriber-interfaces and non-subscriber interfaces `mac`.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### 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
```

This example shows how to enable EPFT on a non-subscriber VLAN sub-interface, based on the source MAC address:

```
RP/0/RSP0/CPU0:router(config)# lpts punt excessive-flow-trap non-subscriber-interfaces mac
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show lpts punt excessive-flow-trap</code>, on page 293</td>
<td>Displays the bad actor flows trapped by the Excessive Punt Flow Trap feature.</td>
</tr>
</tbody>
</table>
Ipts 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 | unclassified}
penalty_rate
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>default</code></td>
<td>Sets the default penalty policing rate for all protocols.</td>
</tr>
<tr>
<td><code>arp</code></td>
<td>Sets the penalty policing rate for the ARP protocol.</td>
</tr>
<tr>
<td><code>icmp</code></td>
<td>Sets the penalty policing rate for the ICMP protocol.</td>
</tr>
<tr>
<td><code>dhcp</code></td>
<td>Sets the penalty policing rate for the DHCP protocol.</td>
</tr>
<tr>
<td><code>pppoe</code></td>
<td>Sets the penalty policing rate for the PPPoE protocol.</td>
</tr>
<tr>
<td><code>ppp</code></td>
<td>Sets the penalty policing rate for the PPP protocol.</td>
</tr>
<tr>
<td><code>igmp</code></td>
<td>Sets the penalty policing rate for the IGMP protocol.</td>
</tr>
<tr>
<td><code>ip</code></td>
<td>Sets the penalty policing rate for the IPv4 protocol.</td>
</tr>
<tr>
<td><code>l2tp</code></td>
<td>Sets the penalty policing rate for the L2TP protocol.</td>
</tr>
<tr>
<td><code>unclassified</code></td>
<td>Sets the penalty police rates for unclassified source MAC.</td>
</tr>
</tbody>
</table>

**penalty_rate**  Penalty rate in packets per second (pps).

The range, in pps, is from 2 to 100; default is 10.

**Command Default**

None

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.3.0</td>
<td>The command was modified to add <code>unclassified</code> keyword to set the penalty police rates for unclassified source MAC.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lpts punt excessive-flow-trap, on page 284</td>
<td>Enables the Excessive Punt Flow Trap feature.</td>
</tr>
</tbody>
</table>
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
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Sets the default penalty timeout for all protocols.</td>
</tr>
<tr>
<td>arp</td>
<td>Sets the penalty timeout for the ARP protocol.</td>
</tr>
<tr>
<td>icmp</td>
<td>Sets the penalty timeout for the ICMP protocol.</td>
</tr>
<tr>
<td>dhcp</td>
<td>Sets the penalty timeout for the DHCP protocol.</td>
</tr>
<tr>
<td>pppoe</td>
<td>Sets the penalty timeout for the PPPoE protocol.</td>
</tr>
<tr>
<td>ppp</td>
<td>Sets the penalty timeout for the PPP protocol.</td>
</tr>
<tr>
<td>igmp</td>
<td>Sets the penalty timeout for the IGMP protocol.</td>
</tr>
<tr>
<td>ip</td>
<td>Sets the penalty timeout for the IPv4 protocol.</td>
</tr>
<tr>
<td>l2tp</td>
<td>Sets the penalty timeout for the L2TP protocol.</td>
</tr>
</tbody>
</table>

**Command Default**

The default value in minutes is 15.

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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)#

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>lpts punt excessive-flow-trap</code>, on page 284</td>
<td>Enables the Excessive Punt Flow Trap feature.</td>
</tr>
</tbody>
</table>
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
```

Syntax Description
- This command has no keywords or arguments.

Command Default
- None

Command Modes
- Global Configuration mode

Command History
```
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
```

Usage Guidelines
- No specific guidelines impact the use of this command.

Task ID
```
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>
```

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
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show lpts punt excessive-flow-trap, on page 293</td>
<td>Displays the bad actor flows trapped by the Excessive Punt Flow Trap feature.</td>
</tr>
</tbody>
</table>
```
To display the bad actor flows trapped by Excessive Punt Flow Trap (EPFT), use the `show lpts punt excessive-flow-trap` command in the EXEC mode.

```
show lpts punt excessive-flow-trap
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>protocol</strong></td>
<td>Enter the protocol type.</td>
</tr>
<tr>
<td>• arp</td>
<td>Displays ARP bad actors.</td>
</tr>
<tr>
<td>• icmp</td>
<td>Displays ICMP bad actors.</td>
</tr>
<tr>
<td>• dhcp</td>
<td>Displays DHCP bad actors.</td>
</tr>
<tr>
<td>• pppoe</td>
<td>Displays PPPoE bad actors.</td>
</tr>
<tr>
<td>• ppp</td>
<td>Displays PPP bad actors.</td>
</tr>
<tr>
<td>• igmp</td>
<td>Displays IGMP bad actors.</td>
</tr>
<tr>
<td>• ipv4</td>
<td>Displays IPv4 bad actors.</td>
</tr>
<tr>
<td>• l2tp</td>
<td>Displays L2TP bad actors.</td>
</tr>
<tr>
<td>• unclassified</td>
<td>Displays unclassified bad actors.</td>
</tr>
<tr>
<td>• all</td>
<td>Displays bad actors for all protocols.</td>
</tr>
<tr>
<td><strong>interface</strong></td>
<td>Displays the bad actors on an interface. For more information on the interface types, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><strong>type</strong></td>
<td>Specifies the interface type. For more information, use the question mark (?) online help function.</td>
</tr>
</tbody>
</table>
interface-path-id Either a physical interface instance or a virtual interface instance as follows:

- Physical interface instance. Naming notation is rack/slot/module/port and a slash between values is required as part of the notation.
  - rack: Chassis number of the rack.
  - slot: Physical slot number of the modular services card or line card.
  - module: Module number. A physical layer interface module (PLIM) is always 0.
  - port: Physical port number of the interface.

- Virtual interface instance. Number range varies depending on interface type.

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.

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. |
| location    | Displays bad actors on a line card. |

**Command Default**

None

**Command Modes**

EXEC mode

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Release</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td></td>
<td>4.3.0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Release</td>
<td>The command was modified to include unclassified option in the protocol list, to display unclassified bad actors.</td>
</tr>
<tr>
<td></td>
<td>5.3.0</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>lpts</td>
<td>read</td>
</tr>
<tr>
<td>basic-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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 is a sample output for `show lpts punt excessive-flow-trap unclassified` command:

Parent Interface: Bundle-Ether1.1  
Intf Handle: 0x08000260  
Protocol: UNCLASSIFIED  
RSP  
Penalty Rate: 0 pps (all packets dropped)  
Time Remaining: 13 mins 54 secs

Src MAC Addr: 0000.6416.0102  
Location: 0/0/CPU0  
Punt Reason: Unclassified packets for RSP  
Penalty Timeout: 15 mins

This table describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Penalty Rate</td>
<td>The penalty policing rate for a protocol. The range is from 2 to 100. The example shown here is for MAC-based EPFT, where all packets from the source MAC are dropped. Therefore, penalty rate is zero (0).</td>
</tr>
<tr>
<td>Penalty Timeout</td>
<td>The penalty timeout value for a protocol. A bad actor flow trapped for sending excessive protocol packets (arp, ppp or unclassified), is penalty policed for the period of penalty-timeout configured (in minutes). By default, it is 15 minutes.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>lpts punt excessive-flow-trap, on page 284</code></td>
<td>Enables the Excessive Punt Flow Trap feature.</td>
</tr>
</tbody>
</table>
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.

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

None

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>lpts</td>
<td>read</td>
</tr>
<tr>
<td>basic-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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
--------------------------------------------------------------
<table>
<thead>
<tr>
<th>Protocol</th>
<th>Police Rate (pps)</th>
<th>Penalty Timeout (mins)</th>
<th>Punt Reasons</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP</td>
<td>10</td>
<td>15</td>
<td>ARP</td>
</tr>
<tr>
<td></td>
<td>Reverse ARP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dynamic ARP Inspection (DAI)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICMP</td>
<td>10</td>
<td>-</td>
<td>ICMP</td>
</tr>
<tr>
<td></td>
<td>ICMP-local</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ICMP-app</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ICMP-control</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ICMP-default</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP</td>
<td>10</td>
<td>-</td>
<td>DHCP Snoop Request</td>
</tr>
<tr>
<td></td>
<td>DHCP Snoop Reply</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>penalty-rate</td>
<td>The penalty policing rate for a protocol. For arp the value is 15 and for pppoe the value is 25.</td>
</tr>
</tbody>
</table>
The penalty timeout value for a protocol. For arp the value is 2.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>penalty-timeout</td>
<td>The penalty timeout value for a protocol. For arp the value is 2.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>lpts punt excessive-flow-trap, on page 284</td>
<td>Enables the Excessive Punt Flow Trap feature.</td>
</tr>
</tbody>
</table>
**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 ]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>type</strong></td>
<td>Specifies the interface type. For more information, use the question mark (?) online help function.</td>
</tr>
</tbody>
</table>
| **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.  
  - 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.  
  - *dhep*: 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 mode
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>lpts</td>
<td>read</td>
</tr>
<tr>
<td>basic-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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
    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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intf Handle</td>
<td>The interface handler for the Bundle Ether interface.</td>
</tr>
<tr>
<td>location</td>
<td>The location of the interface.</td>
</tr>
<tr>
<td>protocol</td>
<td>Specifies if it uses the IPv4 or IPv6 protocol.</td>
</tr>
<tr>
<td>punt reason</td>
<td>The reason to punt the excessive flow trap.</td>
</tr>
<tr>
<td>penalty-rate</td>
<td>The penalty policing rate for a protocol in pps.</td>
</tr>
<tr>
<td>penalty-timeout</td>
<td>The penalty timeout value for a protocol in minutes.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lpts punt excessive-flow-trap, on page 284</td>
<td>Enables the Excessive Punt Flow Trap feature.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>protocol</th>
<th>Enter the protocol type.</th>
</tr>
</thead>
<tbody>
<tr>
<td>• arp</td>
<td>Displays ARP bad actors.</td>
</tr>
<tr>
<td>• icmp</td>
<td>Displays ICMP bad actors.</td>
</tr>
<tr>
<td>• dhcp</td>
<td>Displays DHCP bad actors.</td>
</tr>
<tr>
<td>• pppoe</td>
<td>Displays PPPoE bad actors.</td>
</tr>
<tr>
<td>• ppp</td>
<td>Displays PPP bad actors.</td>
</tr>
<tr>
<td>• igmp</td>
<td>Displays IGMP bad actors.</td>
</tr>
<tr>
<td>• ipv4</td>
<td>Displays IPv4 bad actors.</td>
</tr>
<tr>
<td>• l2tp</td>
<td>Displays L2TP bad actors.</td>
</tr>
<tr>
<td>• all</td>
<td>Displays bad actors for all protocols.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>lpts</td>
<td>read</td>
</tr>
<tr>
<td>basic-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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
```
**show lpts punt excessive-flow-trap protocol**

Intf Handle: 0x08000320
Location: 0/6/CPU0
Protocol: IPv4/v6
Penalty Rate: 10 pps
Punt Reason: Raw-default
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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intf Handle</td>
<td>The interface handler for the Bundle Ether interface.</td>
</tr>
<tr>
<td>location</td>
<td>The location of the interface.</td>
</tr>
<tr>
<td>protocol</td>
<td>Specifies if it uses the IPv4 or IPv6 protocol.</td>
</tr>
<tr>
<td>punt reason</td>
<td>The reason to punt the excessive flow trap.</td>
</tr>
<tr>
<td>penalty-rate</td>
<td>The penalty policing rate for a protocol in pps.</td>
</tr>
<tr>
<td>penalty-timeout</td>
<td>The penalty timeout value for a protocol in minutes.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lpts punt excessive-flow-trap, on page 284</td>
<td>Enables the Excessive Punt Flow Trap feature.</td>
</tr>
</tbody>
</table>
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*.

To use commands of this module, 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 any command, contact your AAA administrator for assistance.

- `initiator dhcp`, on page 304
- `initiator dhcp-snoop`, on page 306
- `initiator unclassified-ip`, on page 308
- `initiator unclassified-source`, on page 310
- `ips subscriber interface`, on page 311
- `ips subscriber I2-connected`, on page 312
- `ips subscriber routed`, on page 314
- `ips subscriber session-limit`, on page 316
- `ips subscriber subscriber-templates`, on page 317
- `show ips subscriber access-interface`, on page 318
- `show ips subscriber interface`, on page 321
- `show ips subscriber summary`, on page 325
- `show ips subscriber template-interface`, on page 328
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.

**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
IP subscriber IPv4 routed configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.3.0</td>
<td>Supported was added for IPv6.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
This command is not supported for IPv6 routed subscriber.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This is an example of configuring the `initiator dhcp` command in the Interface configuration mode:

```sh
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:

```sh
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipsubscriber summary, on page 325</td>
<td>Displays the ipsubscriber information.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>initiator unclassified-ip, on page 308</td>
<td>Enables packet-triggered IPv4 or IPv6 routed subscriber session in an access-interface.</td>
</tr>
</tbody>
</table>
### initiator dhcp-snoop

To configure DHCP to pass the control packets from BNG to the DHCP server to enable DHCP L3 snooping for an IP subscriber, use the `initiator dhcp-snoop` command in the IP subscriber IPv4 (or IPv6) routed configuration mode. To disable this configuration, use the `no` form of this command.

For IPv4:

```
initiator dhcp-snoop
```

For IPv6:

```
initiator dhcp-snoop [prefix-len prefix-len]
```

#### Syntax Description

- **prefix-len**
  - Configures the prefix-length for IPv6 subscriber route to determine the mask to be used for traffic classification.
  - This option is applicable only for `dhcp-snoop` IPv6 sessions; not for IPv4 sessions.

- **prefix-len**
  - Specifies the value of subscriber route prefix-length.
  - The range is from 0 to 127.

#### Command Default

None

#### Command Modes

- Interface IP subscriber IPv4 routed
- Interface IP subscriber IPv6 routed

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

This is supported only on Cisco IOS XR 64-bit operating system.

If `prefix-length` is configured, only the IAPD-based session and classification are supported. If `prefix-length` is not configured, the value is considered as 128, by default. In that case, the IANA-based session and classification are supported.

#### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to enable IPv6 subscriber session creation based on the DHCP control packets that are not destined for BNG:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitEthernet 0/0/0
RP/0/RSP0/CPU0:router(config-if)# ipv4 address 192.0.2.1 255.255.255.0
```
RP/0/RSP0/CPU0:router(config-if)# proxy-arp
RP/0/RSP0/CPU0:router(config-if)# service-policy type control subscriber policy-map-IPSUBV6
RP/0/RSP0/CPU0:router(config-if)# ipsubscriber ipv6 routed
RP/0/RSP0/CPU0:router(config-if-ipsub-ipv6-routed)# initiator dhcp-snoop
RP/0/RSP0/CPU0:router(config-if-ipsub-ipv6-routed)# commit

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>initiator dhcp, on page 304</td>
<td>Enables L2-connected IP subscriber for IPv4 or IPv6.</td>
</tr>
<tr>
<td>ipsubscriber routed, on page 314</td>
<td>Enables an access-interface to host routed subscriber sessions.</td>
</tr>
</tbody>
</table>
initiator unclassified-ip

To enable packet-triggered routed subscriber sessions (IPv4 and IPv6) on an access-interface in BNG, use the `initiator unclassified-ip` command in the appropriate configuration sub mode. To disable this feature, use the `no` form of this command.

```
initiator unclassified-ip [prefix-len prefix-len]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>prefix-len</th>
<th>Configures the prefix-length for IPv6 subscriber route.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This option is available only for packet-triggered IPv6 sessions.</td>
</tr>
<tr>
<td>prefix-len</td>
<td>Specifies the value of subscriber route prefix-length.</td>
</tr>
<tr>
<td></td>
<td>The range is from 0 to 127.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

IP subscriber IPv4 routed configuration
IP subscriber IPv6 routed configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.2.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to host packet-triggered routed IPv4 subscriber 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-subif)# ipsubscriber ipv4 routed
RP/0/RSP0/CPU0:router(config-if-ipsub-ipv4-routed)# initiator unclassified-ip
```

This example shows how to host packet-triggered routed IPv6 subscriber 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-subif)# ipsubscriber_ipv6 routed
```
RP/0/RSP0/CPU0:router(config-if-ipsub-ipv6-routed)# **initiator unclassified-ip prefix-len 56**

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>initiator dhcp, on page 304</strong></td>
<td>Enables I2-connected IP subscriber for IPv4 or IPv6.</td>
</tr>
<tr>
<td></td>
<td><strong>ipsubscriber routed, on page 314</strong></td>
<td>Enables an access-interface to host routed subscriber sessions.</td>
</tr>
</tbody>
</table>
initiator unclassified-source

To enable unclassified packets as first-sign-of-life for IPv4 subscriber, use the `initiator unclassified-source` command in the appropriate configuration submode. To disable this feature, use the `no` form of this command.

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
None

**Command Modes**
IP subscriber IPv4 L2-connected configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Note: Because packet-triggered L2 sessions are not supported for IPv6, this command is not supported for IPv6.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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
```
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**

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
None

**Command Modes**
Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>read,</td>
</tr>
<tr>
<td></td>
<td>write</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show subscriber manager sadb, on page 591</td>
<td>Displays the subscriber management feature attribute database information.</td>
</tr>
<tr>
<td>show ipsubscriber access-interface, on page 318</td>
<td>Shows the access interface information for IP subscriber.</td>
</tr>
<tr>
<td>show ipsubscriber interface, on page 321</td>
<td>Shows the interface information for IP subscriber interfaces.</td>
</tr>
</tbody>
</table>
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 [address-unique]}
```

**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.
- `address-unique`: Enables subscriber IP uniqueness check during first-sign-of-life processing.

**Command Default**

None

**Command Modes**

Interface configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.3.0</td>
<td>Supported was added for IPv6 prefixes.</td>
</tr>
<tr>
<td>5.2.2</td>
<td>This command was modified to add the <code>address-unique</code> option for <code>unclassified-source</code> initiator.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Packet-triggered L2 session (`initiator unclassified-source`) is not supported for IPv6.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>read, write</td>
</tr>
</tbody>
</table>
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
```

This example shows how to enable subscriber IP uniqueness check during first-sign-of-life processing:

```
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 unclassified-source address-unique
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ipsubscriber summary, on page 325</code></td>
<td>Displays the ipsubscriber information.</td>
</tr>
</tbody>
</table>
ipsubscriber routed

To host IPv4 or IPv6 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|ipv6} routed [initiator {dhcp|unclassified-ip} [prefix-len prefix-len]]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>Specifies IPv4 subscriber.</td>
</tr>
<tr>
<td>ipv6</td>
<td>Specifies IPv6 subscriber.</td>
</tr>
<tr>
<td>initiator</td>
<td>Specifies session initiator for routed subscriber.</td>
</tr>
<tr>
<td>dhcp</td>
<td>Configures DHCP as the session initiator for routed subscriber.</td>
</tr>
<tr>
<td>unclassified-ip</td>
<td>Configures unclassified packets as first-sign-of-life for IPv4 or IPv6 subscriber.</td>
</tr>
<tr>
<td>prefix-len</td>
<td>Configures the prefix length of IPv6 subscriber.</td>
</tr>
<tr>
<td>prefix-len</td>
<td>Specifies the prefix length of IPv6 subscriber.</td>
</tr>
<tr>
<td>prefix-len</td>
<td>The range is from 1 to 127.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.2.2</td>
<td>Initiator <code>unclassified-ip</code> was added for the support of packet-triggered IPv4 or IPv6 routed subscriber sessions.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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.
If DHCPv6 is used in standalone mode to provide IA-NA and IA-PD addresses (prefixes) to the routing gateway (RG), and if the RG is directly connected (or connected through an L2 cloud) to the BNG, then the summary route is not required.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to host DHCP-initiated IPv4 routed subscriber 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-subif)# ipsubscriber ipv4 routed initiator dhcp
```

This example shows how to host packet-triggered IPv6 routed subscriber 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-subif)# ipsubscriber ipv6 routed
RP/0/RSP0/CPU0:router(config-subif)# initiator unclassified-ip prefix-len 56
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipsubscriber interface</code> on page 311</td>
<td>Enables interface based static session in BNG.</td>
</tr>
<tr>
<td><code>show ipsubscriber access-interface</code> on page 318</td>
<td>Shows the access interface information for IP subscriber.</td>
</tr>
<tr>
<td><code>show subscriber session</code> on page 608</td>
<td>Displays the subscriber management session information.</td>
</tr>
<tr>
<td><code>initiator unclassified-ip</code> on page 308</td>
<td>Enables packet-triggered routed subscriber sessions on an access-interface.</td>
</tr>
</tbody>
</table>
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
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>total</td>
<td>Limits IP subscribers for all sources.</td>
</tr>
<tr>
<td>unclassified-source</td>
<td>Limits IP subscribers for unclassified sources.</td>
</tr>
<tr>
<td>per-vlan</td>
<td>Limits the per VLAN subscribers.</td>
</tr>
<tr>
<td>session-limit</td>
<td>Specifies the maximum number to which of the IP subscriber session can be limited.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Interface configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

- network read, write

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
```
To enable template-based session provisioning for IPoE subscribers at an access-interface level, use the `ipsubscriber subscriber-templates` command in interface configuration mode. To disable subscriber templates on an access-interface, use the `no` form of this command.

```
ipsubscriber subscriber-templates max_templates
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>max_templates</th>
<th>Specifies maximum number of templates on the specified access-interface. The range is from 1 to 10.</th>
</tr>
</thead>
</table>

**Command Default**
None

**Command Modes**
Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
You must clear all subscriber sessions on an access-interface before disabling the subscriber templates or before modifying the number of subscriber templates on that access-interface.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to enable template-based session provisioning for IPoE subscribers:

```
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 subscriber-templates 7
```
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 mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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
```

This is the sample output of the `show ipsubscriber access-interface` command:

```
RP/0/RSP0/CP00: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

<table>
<thead>
<tr>
<th>Interface</th>
<th>Proto</th>
<th>DHCP</th>
<th>Pkt Trigger DHCPv6</th>
<th>PktTrigIPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/0/0/0</td>
<td>DHCP,PKT, DHCPv6,PKTv6</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>UP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BE1.1</td>
<td>DHCP,PKT</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>UP</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Specifies the access interface type.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proto</td>
<td>Specifies the prototype, for instance, DHCP, DHCPv6, PKTv6.</td>
</tr>
<tr>
<td>DHCP</td>
<td>Specifies the DHCP initiation.</td>
</tr>
<tr>
<td>Pkt Trigger</td>
<td>Specifies the packet trigger Initiation.</td>
</tr>
<tr>
<td>DHCPv6</td>
<td>Specifies the packet trigger Initiation for IPv6.</td>
</tr>
<tr>
<td>PktTrigIPv6</td>
<td>Specifies the DHCPv6 initiation.</td>
</tr>
<tr>
<td>State</td>
<td>Specifies the various states of the access interface, for example, up, down, deleted, and unknown state.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipsubscriber l2-connected, on page 312</td>
<td>Displays the subscriber management session information.</td>
</tr>
</tbody>
</table>
show ipsubscriber interface

To display the interface information for the IP subscriber interfaces, use the `show ipsubscriber interface` command in the EXEC mode.

```plaintext
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>type</code></td>
<td>Interface type. For more information on interface types available for this command, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>interface-path-id</code></td>
<td>Physical interface or virtual interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: Use the <code>show interfaces</code> command to see a list of all interfaces currently configured on the router.</td>
</tr>
<tr>
<td><code>access-interface</code></td>
<td>Specifies the access or parent interface.</td>
</tr>
<tr>
<td><code>address-family</code></td>
<td>Specifies the address-family in which the IP subscriber interface operates.</td>
</tr>
<tr>
<td><code>brief</code></td>
<td>Displays the brief summary of IP Subscriber access interface status and configuration.</td>
</tr>
<tr>
<td><code>dynamic-routes</code></td>
<td>Specifies the dynamic routes.</td>
</tr>
<tr>
<td><code>location</code></td>
<td>Specifies the IP subscriber location.</td>
</tr>
<tr>
<td><code>node-id</code></td>
<td>Specifies the fully qualified location specification.</td>
</tr>
<tr>
<td><code>outer-vlan-id</code></td>
<td>Specifies the subscriber outer VLAN ID.</td>
</tr>
<tr>
<td><code>id</code></td>
<td>Outer VLAN ID. The range is from 1 to 4094.</td>
</tr>
<tr>
<td><code>inner-vlan-id</code></td>
<td>Specifies the subscriber inner VLAN ID.</td>
</tr>
<tr>
<td><code>id</code></td>
<td>Inner VLAN ID. The range is from 1 to 4094.</td>
</tr>
<tr>
<td><code>subscriber-ip</code></td>
<td>Specifies the subscriber IPv4 address.</td>
</tr>
<tr>
<td><code>subscriber-label</code></td>
<td>Specifies the subscriber label.</td>
</tr>
<tr>
<td><code>subscriber-mac</code></td>
<td>Specifies the subscriber MAC address.</td>
</tr>
<tr>
<td><code>vrf</code></td>
<td>Specifies the VRF in which the IP subscriber interface operates.</td>
</tr>
</tbody>
</table>
**Command Default**

None

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.2.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.3.1</td>
<td>The <code>outer-vlan-id</code> keyword along with an optional <code>inner-vlan-id</code> keyword was added.</td>
</tr>
<tr>
<td>Release 5.1</td>
<td>The <code>dynamic-routes</code> keyword was added.</td>
</tr>
<tr>
<td>Release 5.3.0</td>
<td>A new output field, Template ID, was added for <code>show ipsUBscriber interface internal</code> command.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>read</td>
</tr>
</tbody>
</table>

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

```
### Interface Proto Subscriber IP MAC Address Sublabel VRF

<table>
<thead>
<tr>
<th>State</th>
<th>Proto</th>
<th>Subscriber IP</th>
<th>MAC Address</th>
<th>Sublabel</th>
<th>VRF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/0/0/0.ip1</td>
<td>DHCP</td>
<td>1.10.10.9</td>
<td>0100.0000.0000</td>
<td>0x40</td>
<td>default</td>
</tr>
<tr>
<td>UP</td>
<td>DHCPv6</td>
<td>0100.0000.0000</td>
<td>0x40</td>
<td>default</td>
<td></td>
</tr>
<tr>
<td>Gi0/0/0/0.ip2</td>
<td>PKT</td>
<td>2.20.20.9</td>
<td>0200.0000.0000</td>
<td>0x20</td>
<td>default</td>
</tr>
<tr>
<td>UP</td>
<td>PKTv6</td>
<td>0200.0000.0000</td>
<td>0x20</td>
<td>default</td>
<td></td>
</tr>
<tr>
<td>Gi0/0/0/0.ip3</td>
<td>DHCPv6</td>
<td>5.40.20.9</td>
<td>0200.2200.0000</td>
<td>0x21</td>
<td>default</td>
</tr>
<tr>
<td>UP</td>
<td>PKTv6</td>
<td>0200.2210.0000</td>
<td>0x31</td>
<td>default</td>
<td></td>
</tr>
</tbody>
</table>

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 is a sample output of the `show ipsubscriber interface internal` command, with BNG Subscriber Templates feature enabled:

RP/0/RSP0/CPU0:router# show ipsubscriber interface internal

Tue Nov 4 12:52:33.016 EDT
Interface: Bundle-Ether601.603.ip8
Type: L2-connected
Access Interface: Bundle-Ether601.603
Ifhandle: 0x9e0
Access Ifhandle: 0x560
Subscriber MAC: 0000.6611.0103
Subscriber IPv4: 15.15.0.4
Subscriber Label: 0xc3
IPv4 Initiator: DHCP
VLAN ID: 603
Created: Nov 2 13:42:34 (age 1d23h)
VRF: default (0xe0000000), IPv4 Table: default (0xe0000000)
IPv4 State: Up (old: Adjacency added)
Last state change: Nov 2 13:42:35 (1d23h in current state)
Flags: 0x80030811 (V4_ROUTE_ADDED AFI_IPV4 ACTIVTED )
Flags2: 0x4 (V4_INIT_DONE )
AAA Transaction Id: 8589934603
Interface Number: 8
Wavl Tree Pointer: 0x10827c58
Template ID : 0x6e0

[IPv4 Event History]
Nov 2 13:42:34.368 FSOL Received
Nov 2 13:42:34.368 Session Created
Nov 2 13:42:34.880 IM Intf Created
Nov 2 13:42:35.008 VRF Received
Nov 2 13:42:35.008 VRF Conf Received
Nov 2 13:42:35.008 Feature-Conf Activated
Nov 2 13:42:35.520 EA-DPC Success
Nov 2 13:42:35.520 Subscriber Route Added
Nov 2 13:42:35.520 All RIB Route Added

This table describes the significant fields shown in the display.

### Table 17: `show ipsubscriber interface` Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Specifies the access interface type.</td>
</tr>
<tr>
<td>Proto</td>
<td>Specifies the prototype, for instance, DHCP, DHCPv6, PKTv6.</td>
</tr>
<tr>
<td>Subscriber IP</td>
<td>Specifies the IP address of the subscriber interface.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Specifies the MAC address for each interface type.</td>
</tr>
<tr>
<td>Sublabel</td>
<td>Specifies the sub label type for each interface.</td>
</tr>
<tr>
<td>VRF</td>
<td>Specifies the default VRF type.</td>
</tr>
<tr>
<td>State</td>
<td>Specifies the various states of the access interface, for example, up, down, deleted, and unknown state.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipsubscriber l2-connected</code>, on page 312</td>
<td>Displays the subscriber management session information.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>location</code></td>
<td>Specifies the IP subscriber location.</td>
</tr>
<tr>
<td><code>location</code></td>
<td>Specifies the fully qualified location specification.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>read</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th></th>
<th>DHCP</th>
<th>Pkt Trigger</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Initialized</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Session creation started</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Control-policy executing</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Control-policy executed</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Session features applied</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>VRF configured</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Adding adjacency</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Adjacency added</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Up</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Down</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Disconnecting</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Disconnected</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Unknown state</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Total: 0 0

DHCPv6 PktTrig-IPv6
```
This table describes the significant fields shown in the display.

**Table 18: show ipsubscriber summary Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid</td>
<td>Specifies the number of invalid packets for DHCP and Packet Trigger.</td>
</tr>
<tr>
<td>Initialized</td>
<td>Specifies the number of packets that were initialized for DHCP and Packet Trigger.</td>
</tr>
<tr>
<td>Session creation started</td>
<td>Specifies the total number of session initiation that was created.</td>
</tr>
<tr>
<td>Control-policy executing</td>
<td>Specifies the control policies that are executing for DHCP and Packet Trigger.</td>
</tr>
<tr>
<td>Control-policy executed</td>
<td>Specifies the control policies that were executed for DHCP and Packet Trigger.</td>
</tr>
<tr>
<td>Session features applied</td>
<td>Specifies the number of session features that were applied for DHCP and Packet Trigger.</td>
</tr>
<tr>
<td>VRF configured</td>
<td>Specifies the VRFs configured.</td>
</tr>
<tr>
<td>Up</td>
<td>Specifies the number of packets that are in the UP state.</td>
</tr>
<tr>
<td>Down</td>
<td>Specifies the number of packets that are in the DOWN state.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disconnecting</td>
<td>Specifies the number of packets that are disconnecting.</td>
</tr>
<tr>
<td>Disconnected</td>
<td>Specifies the number of packets that are disconnected.</td>
</tr>
<tr>
<td>Unknown State</td>
<td>Specifies the packets that are in the unknown state.</td>
</tr>
<tr>
<td>Error</td>
<td>Specifies the number of packets that are errored out.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipssubscriber l2-connected, on page 312</td>
<td>Displays the subscriber management session information.</td>
</tr>
</tbody>
</table>
show ipsubsriber template-interface

To display the template information for the IP subscriber interfaces, use the **show ipsubsriber template-interface** command in the EXEC mode.

**show ipsubsriber template-interface [access-interface interface-name] [internal]**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Access-Interface (Optional) Specifies the IP subscriber template interfaces for an access-interface.</th>
<th>Interface-type. For more information on interface types available for this command, use the question mark (?) online help function.</th>
<th>Access-Interface (Optional) Displays the internal information of IP subscriber template interfaces.</th>
</tr>
</thead>
</table>

**Command Default**

None

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>read</td>
</tr>
</tbody>
</table>

This is a sample output of the **show ipsubsriber template-interface** command:

```
RP/0/RSP0/CPU0:router# show ipsubsriber template-interface
Tue Nov 4 12:52:56.924 EDT
Template Subscriber Name     Template Subscriber Ifhandle
---------------------------------------------------------------|
Bundle-Ether601.603.tmpl1     0x6e0
Bundle-Ether601.603.tmpl2     0x720
Bundle-Ether601.603.tmpl3     0x760
Bundle-Ether601.603.tmpl4     0x7a0
Bundle-Ether601.603.tmpl5     0x7e0
Bundle-Ether601.604.tmpl1     0x820
Bundle-Ether601.604.tmpl2     0x860
Bundle-Ether601.604.tmpl3     0x8a0
Bundle-Ether601.604.tmpl4     0x8e0
Bundle-Ether601.604.tmpl5     0x920
```

This is a sample output of the **show ipsubsriber template-interface internal** command:

```
RP/0/RSP0/CPU0:router# show ipsubsriber template-interface internal
```
Template Subscriber Internal

Template Interface Name : Bundle-Ether601.603.tmpl1
Ifhandle : 0x6e0
Parent Interface : 0xBundle-Ether601.603 (560)
Interface Number : 1
Creation time : Nov 2 13:34:49

Template Interface Name : Bundle-Ether601.603.tmpl2
Ifhandle : 0x720
Parent Interface : 0xBundle-Ether601.603 (560)
Interface Number : 2
Creation time : Nov 2 13:34:49

Template Interface Name : Bundle-Ether601.603.tmpl3
Ifhandle : 0x760
Parent Interface : 0xBundle-Ether601.603 (560)
Interface Number : 3
Creation time : Nov 2 13:34:49

Template Interface Name : Bundle-Ether601.603.tmpl4
Ifhandle : 0x7a0
Parent Interface : 0xBundle-Ether601.603 (560)
Interface Number : 4
Creation time : Nov 2 13:34:49

Template Interface Name : Bundle-Ether601.603.tmpl5
Ifhandle : 0x7e0
Parent Interface : 0xBundle-Ether601.603 (560)
Interface Number : 5
Creation time : Nov 2 13:34:49

Template Interface Name : Bundle-Ether601.604.tmpl1
Ifhandle : 0x820
Parent Interface : 0xBundle-Ether601.604 (5a0)
Interface Number : 1
Creation time : Nov 2 13:34:51

Template Interface Name : Bundle-Ether601.604.tmpl2
Ifhandle : 0x860
Parent Interface : 0xBundle-Ether601.604 (5a0)
Interface Number : 2
Creation time : Nov 2 13:34:51

Template Interface Name : Bundle-Ether601.604.tmpl3
Ifhandle : 0x8a0
Parent Interface : 0xBundle-Ether601.604 (5a0)
Interface Number : 3
show ipsubscriber template-interface

Creation time : Nov 2 13:34:51

Template Interface Name : Bundle-Ether601.604.tmpl4
Ifhandle : 0x8e0
Parent Interface : 0xBundle-Ether601.604 (5a0)
Interface Number : 4
Creation time : Nov 2 13:34:51

Template Interface Name : Bundle-Ether601.604.tmpl5
Ifhandle : 0x920
Parent Interface : 0xBundle-Ether601.604 (5a0)
Interface Number : 5
Creation time : Nov 2 13:34:51

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show subscriber database, on page 580</td>
<td>Displays the configuration details of subscriber database.</td>
</tr>
<tr>
<td>show subscriber database template, on page 586</td>
<td>Displays the template interface handle and template session information of a subscriber session in BNG.</td>
</tr>
<tr>
<td>show ipsubscriber interface, on page 321</td>
<td>Shows the interface information for IP subscriber interfaces.</td>
</tr>
</tbody>
</table>
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.

To use commands of this module, 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 any command, contact your AAA administrator for assistance.

- ipv4 mtu (BNG), on page 332
- ipv4 unnumbered (point-to-point -BNG), on page 334
- ipv4 unreachable disable (BNG), on page 336
- ipv4 verify unicast source reachable-via (BNG), on page 338
- ipv6 enable (BNG), on page 340
- ipv6 mtu (BNG), on page 342
- ipv6 unreachable disable (BNG), on page 344
- show ipv4 interface (BNG), on page 346
- show ipv4 traffic (BNG), on page 349
- show ipv6 interface (BNG), on page 351
- show ipv6 neighbors (BNG), on page 355
- show ipv6 neighbors summary (BNG), on page 359
- show ipv6 traffic (BNG), on page 360
**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
```

**Syntax Description**

`bytes` MTU in bytes. Range is 68 to 65535 bytes for IPv4 packets. The maximum MTU size that can be set on an interface depends on the interface medium.

**Command Default**
If no MTU size is configured for IPv4 packets sent on an interface, the interface derives the MTU from the Layer 2 MTU.

**Command Modes**

- Interface configuration (for releases prior to R4.2.0)
- Dynamic template configuration (for releases R4.2.0 onward)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.2.0</td>
<td>This command was supported in the dynamic template configuration mode for BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The router punts the packets that needs fragmentation; whereas the software path drops the subscriber traffic that needs fragmentation.

The maximum MTU size that can be set on an interface depends on the interface medium. If the Layer 2 MTU is smaller than the Layer 3 MTU, the Cisco IOS XR software uses the Layer 2 MTU value for the Layer 3 MTU. Conversely, if the Layer 3 MTU is smaller than the Layer 2 MTU, the software uses Layer 3 MTU value. In other words the Cisco IOS XR software uses the lower of the two values for the MTU.

All devices on a physical medium must have the same protocol MTU to operate.

For releases R4.2.0 onward, to enter the dynamic template configuration mode, run the `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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>read, write</td>
</tr>
</tbody>
</table>
### Task ID Operations

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>read, write</td>
</tr>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

For releases prior to R4.2.0, this example shows how to set the maximum IPv4 packet size for GigabitEthernet interface 0/1/1/0 to 300 bytes:

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/1/0
RP/0/RSP0/CPU0:router(config-if)# ipv4 mtu 300
```

For releases R4.2.0 onward, 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ipv4 interface (BNG), on page 346</code></td>
<td>Displays the MTU status of interfaces configured for IPv4.</td>
</tr>
</tbody>
</table>
**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
```

### 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.
  - Virtual interface instance. Number range varies depending on interface type.
  - For more information about the syntax for the router, use the question mark (?) online help function.

### Command Default

IPv4 processing on a point-to-point interface is disabled unless an IPv4 address is assigned explicitly to that interface.

### Command Modes

- Interface configuration (for releases prior to R4.2.0)
- Dynamic template configuration (for releases R4.2.0 onward)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.2.0</td>
<td>This command was supported in the dynamic template configuration mode for BNG.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

For releases R4.2.0 onward, to enter the dynamic template configuration mode, run the `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).

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>read, write</td>
</tr>
<tr>
<td>network</td>
<td>read, write</td>
</tr>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

For releases prior to R4.2.0, this example shows how the GigabitEthernet interface 0/1/1/0 is assigned the loopback interface address 5:

```
RP/0/RSP0/CPU0:router(config)# interface loopback 5
RP/0/RSP0/CPU0:router(config-if)# ipv4 address 192.168.6.6 255.255.255.0
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0
RP/0/RSP0/CPU0:router(config-if)# ipv4 unnumbered loopback 5
```

For releases R4.2.0 onward, this example shows how 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.

### Syntax Description
This command has no keywords or arguments.

### Command Default
IPv4 ICMP unreachable messages are generated.

### Command Modes
- Interface configuration (for releases prior to R4.2.0)
- Dynamic template configuration (for releases R4.2.0 onward)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.2.0</td>
<td>This command was supported in the dynamic template configuration mode for BNG.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
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.

For releases R4.2.0 onward, to enter the dynamic template configuration mode, run the `dynamic-template` command in the Global Configuration mode.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>read, write</td>
</tr>
<tr>
<td>network</td>
<td>read, write</td>
</tr>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

For releases prior to R4.2.0, this example shows how to disable the generation of ICMP unreachable messages on GigabitEthernet interface 0/1/1/0:

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/1/0
RP/0/RSP0/CPU0:router(config-if)# ipv4 unreachables disable
```
For releases R4.2.0 onward, 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]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>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.</td>
</tr>
<tr>
<td>rx</td>
<td>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.</td>
</tr>
<tr>
<td>allow-default</td>
<td>(Optional) Enables the matching of default routes. This option applies to both loose and strict RPF.</td>
</tr>
<tr>
<td>allow-self-ping</td>
<td>(Optional) Enables the router to ping out an interface. This option applies to both loose and strict RPF.</td>
</tr>
</tbody>
</table>

**Command Default**

IPv4 unicast RPF is disabled.

**Command Modes**

Dynamic template configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.2.0</td>
<td>This command was supported in the dynamic template configuration mode for BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>read, write</td>
</tr>
<tr>
<td>network</td>
<td>read, write</td>
</tr>
<tr>
<td>Task ID</td>
<td>Operations</td>
</tr>
<tr>
<td>----------------</td>
<td>------------------</td>
</tr>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

IPv6 is disabled.

**Command Modes**

- Interface configuration (not applicable for BNG)
- Dynamic template configuration (for BNG)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.3.0</td>
<td>This command was supported in the dynamic template configuration mode for BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ipv6 enable` command automatically configures an IPv6 link-local unicast address on the interface while also enabling the interface for IPv6 processing. The `no ipv6 enable` command does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address.

For BNG, ensure you run this command in the dynamic template configuration mode. To enter the dynamic template configuration mode, run `dynamictemplate` command in the Global Configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6</td>
<td>read, write</td>
</tr>
<tr>
<td>network</td>
<td>read, write</td>
</tr>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example (not applicable for BNG) shows how to enable IPv6 processing on GigabitEthernet interface 0/1/0:

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0
RP/0/RSP0/CPU0:router(config-if)# ipv6 enable
```

For BNG, 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 interface (BNG), on page 351</td>
<td>Displays the usability status of interfaces configured for IPv6.</td>
</tr>
</tbody>
</table>
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
```

### Syntax Description

| bytes | MTU in bytes. Range is 1280 to 65535 for IPv6 packets. The maximum MTU size that can be set on an interface depends on the interface medium. |

### Command Default

If no MTU size is configured for IPv6 packets sent on an interface, the interface derives the MTU from the Layer 2 MTU.

### Command Modes

- Interface configuration (not applicable for BNG)
- Dynamic template configuration (for BNG)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Usage Guidelines

If an IPv6 packet exceeds the MTU set for the interface, only the source router of the packet can fragment it.

The maximum MTU size that can be set on an interface depends on the interface medium. If the Layer 2 MTU is smaller than the Layer 3 MTU, the Cisco IOS XR software uses the Layer 2 MTU value for the Layer 3 MTU. Conversely, If the Layer 3 MTU is smaller than the Layer 2 MTU, the software uses Layer 3 MTU value. In other words the Cisco IOS XR software uses the lower of the two values for the MTU.

All devices on a physical medium must have the same protocol MTU to operate.

For BNG, ensure you run this command in the dynamic template configuration mode. To enter the dynamic template configuration mode, run **dynamic-template** command in the 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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6</td>
<td>read, write</td>
</tr>
<tr>
<td>network</td>
<td>read, write</td>
</tr>
</tbody>
</table>
**Task ID** | **Operations**
--- | ---
config-services | read, write

**Examples**

This example (not applicable for BNG) shows how to set the maximum IPv6 packet size for GigabitEthernet interface 0/1/0/0 to 1350 bytes:

```bash
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# ipv6 mtu 1350
```

For BNG, this example shows how to set the maximum IPv6 packet size to 1350 bytes in the dynamic template configuration mode:

```bash
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 interface (BNG), on page 351</td>
<td>Displays the usability status of interfaces configured for IPv6.</td>
</tr>
</tbody>
</table>
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
```

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
IPv6 ICMP unreachable messages are generated.

**Command Modes**
Interface configuration (not applicable for BNG)
Dynamic template configuration (for BNG)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.3.0</td>
<td>This command was supported in the dynamic template configuration mode for BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
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.

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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6</td>
<td>read, write</td>
</tr>
<tr>
<td>network</td>
<td>read, write</td>
</tr>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example (not applicable for BNG) shows how to disable the generation of ICMP unreachable messages on GigabitEthernet interface 0/6/0/0:

```
RP/0/RSP0/CPU0:router (config)# interface gigabitethernet 0/6/0/0
RP/0/RSP0/CPU0:router (config-if)# ipv6 unreachables disable
```
For BNG, 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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf</td>
<td>(Optional) Displays VPN routing and forwarding (VRF) instance information.</td>
</tr>
<tr>
<td>vrf-name</td>
<td>(Optional) Name of a VRF.</td>
</tr>
<tr>
<td>type</td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Either a physical interface instance or a virtual interface instance as follows:</td>
</tr>
<tr>
<td></td>
<td>• Physical interface instance. Naming notation is rack/slot/module/port and a slash between values is required as part of the notation.</td>
</tr>
<tr>
<td></td>
<td>• rack: Chassis number of the rack.</td>
</tr>
<tr>
<td></td>
<td>• slot: Physical slot number of the modular services card or line card.</td>
</tr>
<tr>
<td></td>
<td>• module: Module number. A physical layer interface module (PLIM) is always 0.</td>
</tr>
<tr>
<td></td>
<td>• port: Physical port number of the interface.</td>
</tr>
<tr>
<td>brief</td>
<td>(Optional) Displays the primary IPv4 addresses configured on the router’s interfaces and their protocol and line states.</td>
</tr>
<tr>
<td>summary</td>
<td>(Optional) Displays the number of interfaces on the router that are assigned, unassigned, or unnumbered.</td>
</tr>
</tbody>
</table>

**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**

If VRF is not specified, the software displays the default VRF.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.2.0</td>
<td>This command was supported for BNG.</td>
</tr>
</tbody>
</table>
**Usage Guidelines**

The `show ipv4 interface` command provides output similar to the `show ipv6 interface` command, except that it is IPv4-specific.

The interface name will be displayed only if the name belongs to the VRF instance. If the `vrf-name` is not specified then the interface instance will be displayed only if the interface belongs to the default VRF.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>read</td>
</tr>
<tr>
<td>network</td>
<td>read</td>
</tr>
</tbody>
</table>

**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 unreachable is 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 unreachable is 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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loopback0 is Up</td>
<td>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.</td>
</tr>
<tr>
<td>line protocol is Up</td>
<td>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.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Internet address</td>
<td>IPv4 Internet address and subnet mask of the interface.</td>
</tr>
<tr>
<td>Secondary address</td>
<td>Displays a secondary address, if one has been set.</td>
</tr>
<tr>
<td>MTU</td>
<td>Displays the IPv4 MTU(^1) value set on the interface.</td>
</tr>
<tr>
<td>Multicast reserved groups joined</td>
<td>Indicates the multicast groups this interface belongs to.</td>
</tr>
<tr>
<td>Directed broadcast forwarding</td>
<td>Indicates whether directed broadcast forwarding is enabled or disabled.</td>
</tr>
<tr>
<td>Outgoing access list</td>
<td>Indicates whether the interface has an outgoing access list set.</td>
</tr>
<tr>
<td>Inbound access list</td>
<td>Indicates whether the interface has an incoming access list set.</td>
</tr>
<tr>
<td>Proxy ARP</td>
<td>Indicates whether proxy ARP(^2) is enabled or disabled on an interface.</td>
</tr>
<tr>
<td>ICMP redirects</td>
<td>Specifies whether ICMPv4(^3) redirects are sent on this interface.</td>
</tr>
<tr>
<td>ICMP unreachables</td>
<td>Specifies whether unreachable messages are sent on this interface.</td>
</tr>
<tr>
<td>Internet protocol processing disabled</td>
<td>Indicates an IPv4 address has not been configured on the interface.</td>
</tr>
</tbody>
</table>

\(^1\) MTU = maximum transmission unit  
\(^2\) ARP = Address Resolution Protocol  
\(^3\) ICMPv4 = Internet Control Message Protocol version 4
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 History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.2.0</td>
<td>This command was supported for BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **show ipv4 traffic** command provides output similar to the **show ipv6 traffic** command, except that it is IPv4-specific.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>read</td>
</tr>
<tr>
<td>network</td>
<td>read</td>
</tr>
</tbody>
</table>

**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
 Opt: 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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bad hop count</td>
<td>Occurs when a packet is discarded because its TTL field was decremented to zero.</td>
</tr>
<tr>
<td>encapsulation failed</td>
<td>Usually indicates that the router had no ARP request entry and therefore did not send a datagram.</td>
</tr>
<tr>
<td>format errors</td>
<td>Indicates a gross error in the packet format, such as an impossible Internet header length.</td>
</tr>
<tr>
<td>IP statistics Rcvd total</td>
<td>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.</td>
</tr>
<tr>
<td>no route</td>
<td>Counted when the Cisco IOS XR software discards a datagram it did not know how to route.</td>
</tr>
</tbody>
</table>

4 TTL = time-to-live
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 [summary [type interface-path-id] [brief [link-local global]]]
```

**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.
  - Virtual interface instance. Number range varies depending on interface type.
    For more information about the syntax for the router, use the question mark (?) online help function.
- **brief** (Optional) Displays the primary IPv6 addresses configured on the router interfaces and their protocol and line states.
- **link-local** (Optional) Displays the link local IPv6 address.
- **global** (Optional) Displays the global IPv6 address.
- **summary** (Optional) Displays the number of interfaces on the router that are assigned, unassigned, or unnumbered.

**Command Default**

None

**Command Modes**

EXEC mode
**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.3.0</td>
<td>This command was supported for BNG.</td>
</tr>
<tr>
<td>Release 5.1.2</td>
<td>The <code>link-local</code> and <code>global</code> keywords were added to the command.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show ipv6 interface` command provides output similar to the `show ipv4 interface` command, except that it is IPv6-specific.

Use the `link-local` or `global` keywords along with the `brief` keyword to view the link local or global IPv6 addresses.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

This is the sample output of the `show ipv6 interface` command:

```plaintext
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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet0/3/0 is Shutdown, line protocol is Down</td>
<td>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.</td>
</tr>
</tbody>
</table>
**Field** | **Description**
--- | ---
line protocol is Up (or down) | Indicates whether the software processes that handle the line protocol consider the line usable (that is, whether keepalives are successful). If the interface can provide two-way communication, the line protocol is marked “Up.” For an interface to be usable, both the interface hardware and line protocol must be up.

IPv6 is enabled, stalled, disabled (stalled and disabled are not shown in sample output) | Indicates that IPv6 is enabled, stalled, or disabled on the interface. If IPv6 is enabled, the interface is marked “enabled.” If duplicate address detection processing identified the link-local address of the interface as being a duplicate address, the processing of IPv6 packets is disabled on the interface and the interface is marked “stalled.” If IPv6 is not enabled, the interface is marked “disabled.”

link-local address | Displays the link-local address assigned to the interface.

TENTATIVE | The state of the address in relation to duplicate address detection. States can be any of the following:
• duplicate—The address is not unique and is not being used. If the duplicate address is the link-local address of an interface, the processing of IPv6 packets is disabled on that interface.
• tentative—Duplicate address detection is either pending or underway on this interface.

Note | If an address does not have one of these states (the state for the address is blank), the address is unique and is being used.

Global unicast addresses | Displays the global unicast addresses assigned to the interface.

ICMP redirects | State of Internet Control Message Protocol (ICMP) IPv6 redirect messages on the interface (the sending of the messages is enabled or disabled).

ND DAD | State of duplicate address detection on the interface (enabled or disabled).

number of DAD attempts | Number of consecutive neighbor solicitation messages that are sent on the interface while duplicate address detection is performed.

ND reachable time | Displays the neighbor discovery reachable time (in milliseconds) assigned to this interface.

This is the sample output of the **show ipv6 interface brief link-local** command:

```
RP/0/RSP0/CPU0:router#show ipv6 interface brief link-local

<table>
<thead>
<tr>
<th>Interface</th>
<th>IPv6-Address</th>
<th>Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet0/0/0</td>
<td>fe80::fe:8ff:fece:26c5</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>GigabitEthernet0/0/1</td>
<td>fe80::4f:88ff:fea0:8c9d</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>GigabitEthernet0/0/3</td>
<td>unassigned</td>
<td>Shutdown</td>
<td>Down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/4</td>
<td>unassigned</td>
<td>Shutdown</td>
<td>Down</td>
</tr>
</tbody>
</table>
```

This is the sample output of the **show ipv6 interface brief global** command:
show ipv6 interface brief global

<table>
<thead>
<tr>
<th>Interface</th>
<th>IPv6-Address</th>
<th>Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet0/0/0/0</td>
<td>2001:db8::1</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>GigabitEthernet0/0/0/1</td>
<td>2001:db8::2</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>GigabitEthernet0/0/0/3</td>
<td>unassigned</td>
<td>Shutdown</td>
<td>Down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/0/4</td>
<td>unassigned</td>
<td>Shutdown</td>
<td>Down</td>
</tr>
</tbody>
</table>

This is the sample output of the `show ipv6 interface type interface-path-id brief link-local` command:

show ipv6 interface gigabitEthernet 0/0/0/0 brief link-local

<table>
<thead>
<tr>
<th>Interface</th>
<th>IPv6-Address</th>
<th>Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet0/0/0/0</td>
<td>fe80::fe:8ff:fe2e:26c5</td>
<td>Up</td>
<td>Up</td>
</tr>
</tbody>
</table>

This is the sample output of the `show ipv6 vrf vrf-name interface brief link-local` command:

show ipv6 vrf vrf1 interface brief link-local

<table>
<thead>
<tr>
<th>Interface</th>
<th>IPv6-Address</th>
<th>Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet0/0/0/2</td>
<td>fe80::46:c8ff:fe2e:daae</td>
<td>Up</td>
<td>Up</td>
</tr>
</tbody>
</table>

This is the sample output of the `show ipv6 vrf vrf-name interface type interface-path-id brief link-local` command:

show ipv6 vrf vrf1 interface gigabitEthernet 0/0/0/2 brief link-local

<table>
<thead>
<tr>
<th>Interface</th>
<th>IPv6-Address</th>
<th>Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet0/0/0/2</td>
<td>fe80::46:c8ff:fe2e:daae</td>
<td>Up</td>
<td>Up</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv4 interface (BNG), on page 346</td>
<td>Displays the usability status of interfaces configured for IPv4.</td>
</tr>
</tbody>
</table>
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 History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.3.0</td>
<td>This command was supported for BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When the `interface-type` and `interface-number` arguments are not specified, cache information for all IPv6 neighbors is displayed. Specifying the `interface-type` and `interface-number` arguments displays only cache information about the specified interface.

**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::1:0:4::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:
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
2000:0:0:4::2 0 0003.a0d6.141e REACH gigabitethernet2
```

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 0013.9400.00a9 REACH BE3 0/2/CPU0
2001:3::b 90 0013.9400.00b9 REACH BE3 0/2/CPU0
2001:3::c 35 0013.9400.00c9 REACH BE3 0/2/CPU0
2001:3::d 114 0013.9400.00d9 REACH BE3 0/2/CPU0
2001:3::e 117 0013.9400.00e9 REACH BE3 0/2/CPU0
2001:3::f 157 0013.9400.00f9 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
```
This table describes significant fields shown in the display.

**Table 22: show ipv6 neighbors Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Address</td>
<td>IPv6 address of neighbor or interface.</td>
</tr>
<tr>
<td>Age</td>
<td>Time (in minutes) since the address was confirmed to be reachable. A hyphen (-) indicates a static entry.</td>
</tr>
<tr>
<td>Link-layer Addr</td>
<td>MAC address. If the address is unknown, a hyphen (-) is displayed.</td>
</tr>
<tr>
<td>State</td>
<td>The state of the neighbor cache entry. These are the states for dynamic entries in the IPv6 neighbor discovery cache:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• probe—A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer milliseconds until a reachability confirmation is received.</td>
</tr>
<tr>
<td>Note</td>
<td>Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache; therefore, the descriptions for the INCMP (incomplete) and reach (reachable) states are different for dynamic and static cache entries.</td>
</tr>
</tbody>
</table>
### Field
<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface from which the address is reachable.</td>
</tr>
</tbody>
</table>

### Related Commands
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 neighbors summary (BNG), on page 359</td>
<td>Displays summary information for the neighbor entries.</td>
</tr>
</tbody>
</table>
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 mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.3.0</td>
<td>This command was supported for BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

```
Task ID  Operations ID
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ipv6 neighbors (BNG)</code>, on page 355</td>
<td>Displays IPv6 neighbor discovery cache information.</td>
</tr>
</tbody>
</table>
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 History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.3.0</td>
<td>This command was supported for BNG.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The show ipv6 traffic command provides output similar to the show ipv4 traffic command, except that it is IPv6-specific.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6</td>
<td>read</td>
</tr>
<tr>
<td>network</td>
<td>read</td>
</tr>
</tbody>
</table>

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
```
Neighbor Discovery ICMP statistics:
Rcvd: 0 router solicit, 0 router advert, 0 redirect
Sent: 0 router solicit, 0 router advert, 0 redirect
UDP statistics:
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
0 hopcount expired, 0 reassembly timeout,
0 unknown timeout, 0 too big,
0 echo request, 0 echo reply

This table describes the significant fields shown in the display.

Table 23: show ipv6 traffic Command Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rcvd:</td>
<td>Statistics in this section refer to packets received by the router.</td>
</tr>
<tr>
<td>total</td>
<td>Total number of packets received by the software.</td>
</tr>
<tr>
<td>local destination</td>
<td>Locally destined packets received by the software.</td>
</tr>
<tr>
<td>source-routed</td>
<td>Packets seen by the software with RH.</td>
</tr>
<tr>
<td>truncated</td>
<td>Truncated packets seen by the software.</td>
</tr>
<tr>
<td>bad header</td>
<td>An error was found in generic HBH, RH, DH, or HA. Software only.</td>
</tr>
<tr>
<td>unknown option</td>
<td>Unknown option type in IPv6 header.</td>
</tr>
<tr>
<td>unknown protocol</td>
<td>Protocol specified in the IP header of the received packet is unreachable.</td>
</tr>
<tr>
<td>Sent:</td>
<td>Statistics in this section refer to packets sent by the router.</td>
</tr>
<tr>
<td>forwarded</td>
<td>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.</td>
</tr>
<tr>
<td>Mcast:</td>
<td>Multicast packets.</td>
</tr>
</tbody>
</table>
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ipv4 traffic (BNG)</code> on page 349</td>
<td>Displays statistics about IPv4 traffic.</td>
</tr>
</tbody>
</table>
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.

To use commands of this module, 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 any command, contact your AAA administrator for assistance.

- router igmp vrf, on page 364
- igmp accounting, on page 365
- igmp explicit-tracking, on page 366
- igmp query-interval, on page 368
- igmp query-max-response-time, on page 370
- multicast (BNG), on page 372
- unicast-qos-adjust, on page 374
- show igmp unicast-qos-adjust statistics, on page 376
- show igmp vrf (BNG), on page 378
- clear igmp unicast-qos-adjust, on page 380
**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
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>vrf_name</th>
<th>Specifies the VRF name.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>traffic</td>
<td>Configures IGMP traffic variables.</td>
</tr>
<tr>
<td></td>
<td>profile</td>
<td>Configures route-policy to be used to map the bandwidth profile.</td>
</tr>
<tr>
<td></td>
<td>profile_name</td>
<td>Specifies the profile name.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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 }
```

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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**

---

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access_list_name</td>
<td>Specifies the access list tracking group range.</td>
</tr>
</tbody>
</table>

---

**Command Default**

None

**Command Modes**

Dynamic template configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>igmp query-interval</strong>, on page 368</td>
<td>Configures the frequency at which the Cisco IOS XR Software sends Internet Group Management Protocol (IGMP) host-query messages.</td>
</tr>
<tr>
<td><strong>unicast-qos-adjust</strong>, on page 374</td>
<td>Configures the IGMP QOS Shaper for subscriber unicast traffic.</td>
</tr>
<tr>
<td><strong>show igmp unicast-qos-adjust statistics</strong>, on page 376</td>
<td>Displays the internal statistics of the unicast-qos-adjusted feature.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>igmp query-max-response-time, on page 370</code></td>
<td>Configures the maximum response time advertised in Internet Group Management Protocol (IGMP) queries</td>
</tr>
<tr>
<td><code>multicast (BNG), on page 372</code></td>
<td>Configures the mode in which the multicast components will work for subscriber sessions associated with a dynamic template.</td>
</tr>
</tbody>
</table>
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*

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `dynamic-template type ppp` command to enter dynamic template type ppp configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>unicast-qos-adjust, on page 374</code></td>
<td>Configures the IGMP QOS Shaper for subscriber unicast traffic.</td>
</tr>
<tr>
<td><code>igmp explicit-tracking, on page 366</code></td>
<td>Configures explicit host tracking under Internet Group Management Protocol (IGMP) Version 3</td>
</tr>
<tr>
<td><code>igmp query-max-response-time, on page 370</code></td>
<td>Configures the maximum response time advertised in Internet Group Management Protocol (IGMP) queries</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>multicast (BNG), on page 372</td>
<td>Configures the mode in which the multicast components will work for subscriber sessions associated with a dynamic template.</td>
</tr>
<tr>
<td>show igmp unicast-qos-adjust statistics, on page 376</td>
<td>Displays the internal statistics of the unicast-qos-adjusted feature.</td>
</tr>
</tbody>
</table>
**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
```

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `dynamic-template type ppp` command to enter dynamic template type ppp configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>igmp query-interval</code>, on page 368</td>
<td>Configures the frequency at which the Cisco IOS XR Software sends Internet Group Management Protocol (IGMP) host-query messages.</td>
</tr>
<tr>
<td><code>igmp explicit-tracking</code>, on page 366</td>
<td>Configures explicit host tracking under Internet Group Management Protocol (IGMP) Version 3</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>show igmp unicast-qos-adjust statistics, on page 376</td>
<td>Displays the internal statistics of the unicast-qos-adjusted feature.</td>
</tr>
<tr>
<td>unicast-qos-adjust, on page 374</td>
<td>Configures the IGMP QOS Shaper for subscriber unicast traffic.</td>
</tr>
<tr>
<td>multicast (BNG), on page 372</td>
<td>Configures the mode in which the multicast components will work for subscriber sessions associated with a dynamic template.</td>
</tr>
</tbody>
</table>
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}
```

<table>
<thead>
<tr>
<th>qos-correlation</th>
<th>Configures multicast in a IGMP-HQOS correlation mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>passive</td>
<td>Configures multicast is an passive mode.</td>
</tr>
<tr>
<td>ipv4</td>
<td>Optional. Specifies configuration for IPv4 address family.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Dynamic template configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>The command was extended to IPoE subscribers as well.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `dynamic-template type ppp` command to enter dynamic template type ppp configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This is an example of configuring the `multicast` command in the dynamic-template configuration mode for type PPP:

```
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
```

This is an example of enabling IGMP QoS correlation for IPoE subscribers:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template
RP/0/RSP0/CPU0:router(config-dynamic-template)# type ipsSubscriber foo
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# multicast ipv4 qos-correlation
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>igmp query-interval, on page 368</code></td>
<td>Configures the frequency at which the Cisco IOS XR Software sends Internet Group Management Protocol (IGMP) host-query messages.</td>
</tr>
<tr>
<td><code>unicast-qos-adjust, on page 374</code></td>
<td>Configures the IGMP QOS Shaper for subscriber unicast traffic.</td>
</tr>
<tr>
<td><code>igmp explicit-tracking, on page 366</code></td>
<td>Configures explicit host tracking under Internet Group Management Protocol (IGMP) Version 3</td>
</tr>
<tr>
<td><code>igmp query-max-response-time, on page 370</code></td>
<td>Configures the maximum response time advertised in Internet Group Management Protocol (IGMP) queries</td>
</tr>
<tr>
<td><code>show igmp unicast-qos-adjust statistics, on page 376</code></td>
<td>Displays the internal statistics of the unicast-qos-adjusted feature.</td>
</tr>
</tbody>
</table>
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}
```

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `dynamic-template type ppp` command to enter dynamic template type ppp configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp query-interval, on page 368</td>
<td>Configures the frequency at which the Cisco IOS XR Software sends Internet Group Management Protocol (IGMP) host-query messages.</td>
</tr>
<tr>
<td>igmp explicit-tracking, on page 366</td>
<td>Configures explicit host tracking under Internet Group Management Protocol (IGMP) Version 3.</td>
</tr>
<tr>
<td>show igmp unicast-qos-adjust statistics, on page 376</td>
<td>Displays the internal statistics of the unicast-qos-adjusted feature.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>igmp query-max-response-time, on page 370</code></td>
<td>Configures the maximum response time advertised in Internet Group Management Protocol (IGMP) queries.</td>
</tr>
<tr>
<td><code>multicast (BNG), on page 372</code></td>
<td>Configures the mode in which the multicast components will work for subscriber sessions associated with a dynamic template.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>(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.</td>
</tr>
<tr>
<td></td>
<td>Specifies the output modifiers.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>multicast read</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP to QoS Batch stats</td>
<td>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.</td>
</tr>
<tr>
<td>IGMP to QoS message send stats</td>
<td>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.</td>
</tr>
<tr>
<td>Resync stats</td>
<td>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.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp query-interval, on page 368</td>
<td>Configures the frequency at which the Cisco IOS XR Software sends Internet Group Management Protocol (IGMP) host-query messages.</td>
</tr>
<tr>
<td>unicast-qos-adjust, on page 374</td>
<td>Configures the IGMP QOS Shaper for subscriber unicast traffic.</td>
</tr>
<tr>
<td>igmp explicit-tracking, on page 366</td>
<td>Configures explicit host tracking under Internet Group Management Protocol (IGMP) Version 3</td>
</tr>
<tr>
<td>igmp query-max-response-time, on page 370</td>
<td>Configures the maximum response time advertised in Internet Group Management Protocol (IGMP) queries</td>
</tr>
<tr>
<td>multicast (BNG), on page 372</td>
<td>Configures the mode in which the multicast components will work for subscriber sessions associated with a dynamic template.</td>
</tr>
</tbody>
</table>
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 mode

Command History

```
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
```

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

```
Task ID     Operation
multicast  read
```

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

<table>
<thead>
<tr>
<th>Interface</th>
<th>Number</th>
<th>Max #</th>
</tr>
</thead>
<tbody>
<tr>
<td>BV1</td>
<td>7</td>
<td>10</td>
</tr>
<tr>
<td>Loopback1001</td>
<td>3</td>
<td>25000</td>
</tr>
</tbody>
</table>

RP/0/RSP0/CPU0:router#show igmp vrf vrf1 interface bvi1

Thu Feb 7 10:02:48.231 GMT

BV1 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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported Interfaces</td>
<td>Specifies the number of supported interfaces.</td>
</tr>
<tr>
<td>Unsupported Interfaces</td>
<td>Specifies the number of unsupported interfaces.</td>
</tr>
<tr>
<td>Enabled Interfaces</td>
<td>Specifies the number of interfaces that are enabled.</td>
</tr>
<tr>
<td>Disabled Interfaces</td>
<td>Specifies the number of interfaces that are disabled.</td>
</tr>
</tbody>
</table>
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 }

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rate</td>
<td>Specifies the rate programmed in QoS.</td>
</tr>
<tr>
<td>statistics</td>
<td>Specifies the unicast rate adjustment statistics.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies the interface specific rate.</td>
</tr>
<tr>
<td>type</td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
</tbody>
</table>

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 mode |
| Command History | Release 4.2.0 This command was introduced. |
| Usage Guidelines | No specific guidelines impact the use of this command. |
| Task ID | Task ID Operation |
| | multicast exec |
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
```
clear igmp unicast-qos-adjust
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*.

To use commands of this module, 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 any command, contact your AAA administrator for assistance.

- ipv6 nd dad attempts (BNG), on page 384
- ipv6 nd framed-prefix-pool, on page 387
- ipv6 nd managed-config-flag (BNG), on page 388
- ipv6 nd ns-interval (BNG), on page 390
- ipv6 nd nud-enable, on page 392
- ipv6 nd other-config-flag (BNG), on page 393
- ipv6 nd ra-initial, on page 395
- ipv6 nd ra-interval (BNG), on page 396
- ipv6 nd ra-lifetime (BNG), on page 398
- ipv6 nd ra-unicast, on page 400
- ipv6 nd reachable-time (BNG), on page 401
- ipv6 nd start-ra-on-ipv6-enable, on page 403
- ipv6 nd suppress-cache-learning, on page 404
- ipv6 nd suppress-ra (BNG), on page 405
**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.

```plaintext
ipv6 nd dad attempts value
```

**Syntax Description**

- **value** Number of neighbor solicitation messages. Range is 0 to 600. Configuring a value of 0 disables duplicate address detection processing on the specified interface; a value of 1 configures a single transmission without follow-up transmissions.

**Command Default**

Duplicate address detection on unicast IPv6 addresses with the sending of one neighbor solicitation message is enabled. The default is one message.

**Command Modes**

- Interface configuration (not applicable for BNG)
- Dynamic template configuration (for BNG)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.3.0</td>
<td>This command was supported in the dynamic template configuration mode for BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Duplicate address detection verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces (the new addresses remain in a tentative state while duplicate address detection is performed). Duplicate address detection uses neighbor solicitation messages to verify the uniqueness of unicast IPv6 addresses.

The DupAddrDetectTransmits node configuration variable (as specified in RFC 2462, *IPv6 Stateless Address Autoconfiguration*) is used to automatically determine the number of consecutive neighbor solicitation messages that are sent on an interface while duplicate address detection is performed on a tentative unicast IPv6 address.

The interval between the sending of duplicate address detection neighbor solicitation messages (the duplicate address detection timeout interval) is specified by the neighbor discovery-related variable RetransTimer (as specified in RFC 2461, *Neighbor Discovery for IP Version 6 (IPv6)*), which is used to determine the time between retransmissions of neighbor solicitation messages to a neighbor when the address is being resolved or when the reachability of a neighbor is being probed. This is the same management variable used to specify the interval for neighbor solicitation messages during address resolution and neighbor unreachability detection. Use the `ipv6 nd ns-interval` command to configure the interval between neighbor solicitation messages that are sent during duplicate address detection.

Duplicate address detection is suspended on interfaces that are administratively down. While an interface is administratively down, the unicast IPv6 addresses assigned to the interface are set to a pending state. Duplicate address detection is automatically restarted on an interface when the interface returns to being administratively up.

For BNG, ensure you run this command in the dynamic template configuration mode. To enter the dynamic template configuration mode, run `dynamic-template` command in the Global Configuration mode.
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 GigabitEthernet
```

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).

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6</td>
<td>read,</td>
<td>write</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>config-services</td>
<td>read,</td>
<td>write</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Examples

This example (not applicable for BNG) shows how to set the number of consecutive neighbor solicitation messages for interface 0/2/0/1 to 1 and then display the state (tentative or duplicate) of the unicast IPv6 address configured for an interface:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/1
RP/0/RSP0/CPU0:router(config-if)# ipv6 nd dad attempts 1
RP/0/RSP0/CPU0:router(config-if)# Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]: y

RP/0/RSP0/CPU0:router# show ipv6 interface
gigabitethernet2/2/0/0 is Up, line protocol is Up
IPv6 is disabled, link-local address unassigned
No global unicast address is configured
```

```
gigabitethernet2/2/0/1 is Up, line protocol is Up
IPv6 is enabled, link-local address is fe80::203:fdff:fe1b:4501
Global unicast address(es):
  1::1, subnet is 1::/64 [DUPPLICATE]
MTU is 1514 (1500 is available to IPv6)
```
ICMP redirects are disabled
ND DAD is enabled, number of DAD attempts 1
ND reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
Hosts use stateless autoconfig for addresses.
gigabitethernet2/2/0/2 is Shutdown, line protocol is Down
IPv6 is enabled, link-local address is fe80::200:11ff:fe11:1111 [TENTATIVE]
Global unicast address(es):
    111::2, subnet is 111::/64 [TENTATIVE]
MTU is 1514 (1500 is available to IPv6)
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts 1
ND reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
Hosts use stateless autoconfig for addresses.

For BNG, this example shows how to display the state (tentative or duplicate) of the unicast IPv6 address on the dynamic template configuration mode:

```
RP/0/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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 nd ns-interval (BNG), on page 390</td>
<td>Configures the interval between IPv6 neighbor solicitation transmissions on an interface.</td>
</tr>
<tr>
<td>show ipv6 interface (BNG), on page 351</td>
<td>(Not applicable for BNG) Displays the usability status of interfaces configured for IPv6.</td>
</tr>
</tbody>
</table>
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
```

**Syntax Description**

| `pool_name` | Specifies the framed address pool name. |

**Command Default**

None

**Command Modes**

Dynamic template configuration

**Command History**

```
Release          Modification
4.3.0             This command was introduced.
```

**Usage Guidelines**

This value is included in all IPv6 router advertisements sent out from this interface. Very short intervals are not recommended in normal IPv6 operation. When a nondefault value is configured, the configured time is both advertised and used by the router itself.

To enter the dynamic template configuration mode, run `dynamic-template` command in the Global Configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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 pl
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`

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
The managed address configuration flag is not set in IPv6 router advertisements.

**Command Modes**
Interface configuration (not applicable for BNG)
Dynamic template configuration (for BNG)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.3.0</td>
<td>This command was supported in the dynamic template configuration mode for BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Setting the managed address configuration flag in IPv6 router advertisements indicates to attached hosts whether they should use stateful autoconfiguration to obtain addresses. If the flag is set, the attached hosts should use stateful autoconfiguration to obtain addresses. If the flag is not set, the attached hosts should not use stateful autoconfiguration to obtain addresses.

Hosts may use stateful and stateless address autoconfiguration simultaneously.

For BNG, ensure you run this command in the dynamic template configuration mode. To enter the dynamic template configuration mode, run `dynamic-template` command in the Global Configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6</td>
<td>read, write</td>
</tr>
<tr>
<td>network</td>
<td>read, write</td>
</tr>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
This example (not applicable for BNG) shows how to configure the managed address configuration flag in IPv6 router advertisements on GigabitEthernet interface 0/1/1/0:

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/1/0
RP/0/RSP0/CPU0:router(config-if)# ipv6 nd managed-config-flag
```
For BNG, this example shows how to configure the managed address configuration flag in IPv6 router advertisements on dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp pl
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv6 nd managed-config-flag
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show ipv6 interface (BNG), on page 351</td>
<td>Displays the usability status of interfaces configured for IPv6.</td>
</tr>
</tbody>
</table>
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
```

**Syntax Description**

| milliseconds | Interval (in milliseconds) between IPv6 neighbor solicit transmissions. Range is 1000 to 3600000. |

**Command Default**

0 milliseconds (unspecified) is advertised in router advertisements, and the value 1000 is used for the neighbor discovery activity of the router itself.

**Command Modes**

- Interface configuration (not applicable for BNG)
- Dynamic template configuration (for BNG)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.3.0</td>
<td>This command was supported in the dynamic template configuration mode for BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This value is included in all IPv6 router advertisements sent out from this interface. Very short intervals are not recommended in normal IPv6 operation. When a nondefault value is configured, the configured time is both advertised and used by the router itself.

For BNG, ensure you run this command in the dynamic template configuration mode. To enter the dynamic template configuration mode, run `dynamic-template` command in the Global Configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6</td>
<td>read, write</td>
</tr>
<tr>
<td>network</td>
<td>read, write</td>
</tr>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example (not applicable for BNG) configures an IPv6 neighbor solicit transmission interval of 9000 milliseconds for GigabitEthernet interface 0/1/1/0:

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/1/0
RP/0/RSP0/CPU0:router(config-if)# ipv6 nd ns-interval 9000
```
For BNG, this example configures an IPv6 neighbor solicit transmission interval of 9000 milliseconds in the dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp pl
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv6 nd ns-interval 9000
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ipv6 interface (BNG), on page 351</code></td>
<td>Displays the usability status of interfaces configured for IPv6.</td>
</tr>
</tbody>
</table>
**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**

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

None

**Command Modes**

Dynamic template configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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 pl
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
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

The other stateful configuration flag is not set in IPv6 router advertisements.

**Command Modes**

- Interface configuration (not applicable for BNG)
- Dynamic template configuration (for BNG)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.3.0</td>
<td>This command was supported in the dynamic template configuration mode for BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The setting of the other stateful configuration flag in IPv6 router advertisements indicates to attached hosts how they can obtain autoconfiguration information other than addresses. If the flag is set, the attached hosts should use stateful autoconfiguration to obtain the other (nonaddress) information.

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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6</td>
<td>read, write</td>
</tr>
<tr>
<td>network</td>
<td>read, write</td>
</tr>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example (not applicable for BNG) configures the “other stateful configuration” flag in IPv6 router advertisements on GigabitEthernet interface 0/1/0:
For BNG, this example configures the “other stateful configuration” flag for IPv6 router advertisements in the dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/1/0
RP/0/RSP0/CPU0:router(config-if)# ipv6 nd other-config-flag
```

```
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp pl
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv6 nd other-config-flag
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 nd managed-config-flag (BNG), on page 388</code></td>
<td>Sets the managed address configuration flag in IPv6 router advertisements.</td>
</tr>
<tr>
<td><code>show ipv6 interface (BNG), on page 351</code></td>
<td>Displays the usability status of interfaces configured for IPv6.</td>
</tr>
</tbody>
</table>
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
```

### 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
4.3.0           This command was supported in the dynamic template configuration mode for BNG.
```

### Usage Guidelines

To enter the dynamic template configuration mode, run `dynamic-template` command in the Global Configuration mode.

### 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 pl
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv6 nd ra-initial 5 201
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 nd ra-interval (BNG)</code>, on page 396</td>
<td>Configures the interval between IPv6 router advertisement transmissions on an interface.</td>
</tr>
</tbody>
</table>
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
```

**Syntax Description**

`seconds` The interval (in seconds) between IPv6 router advertisement transmissions.

**Command Default**

`seconds`: 200 seconds

**Command Modes**

- Interface configuration (not applicable for BNG)
- Dynamic template configuration (for BNG)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.3.0</td>
<td>This command was supported in the dynamic template configuration mode for BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The interval between transmissions should be less than or equal to the IPv6 router advertisement lifetime if the router is configured as a default router by using the `ipv6 nd ra-lifetime` command. To prevent synchronization with other IPv6 nodes, randomly adjust the actual value used to within 20 percent of the specified value.

For BNG, ensure you run this command in the dynamic template configuration mode. To enter the dynamic template configuration mode, run `dynamic-template` command in the Global Configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6</td>
<td>read, write</td>
</tr>
<tr>
<td>network</td>
<td>read, write</td>
</tr>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example (not applicable for BNG) configures an IPv6 router advertisement interval of 201 seconds on GigabitEthernet interface 0/1/1/0:

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/1/0
RP/0/RSP0/CPU0:router(config-if)# ipv6 nd ra-interval 201
```

For BNG, this example configures an IPv6 router advertisement interval of 201 seconds in the dynamic template configuration mode:
## Neighbor Discovery Commands

```plaintext
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 nd ra-lifetime (BNG), on page 398</code></td>
<td>Configures the lifetime of an IPv6 router advertisement.</td>
</tr>
<tr>
<td><code>show ipv6 interface (BNG), on page 351</code></td>
<td>Displays the usability status of interfaces configured for IPv6.</td>
</tr>
</tbody>
</table>
**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
```

**Syntax Description**

- `seconds`: The validity (in seconds) of this router as a default router on this interface.

**Command Default**

- `seconds`: 1800 seconds

**Command Modes**

- Interface configuration (not applicable for BNG)
- Dynamic template configuration (for BNG)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.3.0</td>
<td>This command was supported in the dynamic template configuration mode for BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The router lifetime value is included in all IPv6 router advertisements sent out the interface. The value indicates the usefulness of the router as a default router on this interface. Setting the value to 0 indicates that the router should not be considered a default router on this interface. The router lifetime value can be set to a nonzero value to indicate that it should be considered a default router on this interface. The nonzero value for the router lifetime value should not be less than the router advertisement interval.

For BNG, ensure you run this command in the dynamic template configuration mode. To enter the dynamic template configuration mode, run `dynamic-template` command in the Global Configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6</td>
<td>read, write</td>
</tr>
<tr>
<td>network</td>
<td>read, write</td>
</tr>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example (not applicable for BNG) configures an IPv6 router advertisement lifetime of 1801 seconds on GigabitEthernet interface 0/1/1/0:

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/1/0
RP/0/RSP0/CPU0:router(config-if)# ipv6 nd ra-lifetime 1801
```
For BNG, this example configures an IPv6 router advertisement lifetime of 1801 seconds in the dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv6 nd ra-lifetime 1801
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ipv6 nd ra-interval (BNG), on page 396</td>
<td>Configures the interval between IPv6 router advertisement transmissions on an interface.</td>
</tr>
<tr>
<td></td>
<td>show ipv6 interface (BNG), on page 351</td>
<td>Displays the usability status of interfaces configured for IPv6.</td>
</tr>
</tbody>
</table>
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
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

None

**Command Modes**

Dynamic template configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dynamic-template, on page 270</td>
<td>Groups a set of configuration items that can be applied to a group of subscribers.</td>
</tr>
</tbody>
</table>
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
```

**Syntax Description**

- `milliseconds`: The amount of time (in milliseconds) that a remote IPv6 node is considered reachable. The range is from 0 to 3600000.

**Command Default**

0 milliseconds (unspecified) is advertised in router advertisements and 30000 (30 seconds) is used for the neighbor discovery activity of the router itself.

**Command Modes**

- Interface configuration (not applicable for BNG)
- Dynamic template configuration (for BNG)

**Command History**

- **Release 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**

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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6</td>
<td>read, write</td>
</tr>
<tr>
<td>network</td>
<td>read, write</td>
</tr>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example (not applicable for BNG) shows how to configure an IPv6 reachable time of 1,700,000 milliseconds for GigabitEthernet interface 0/1/1/0:
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/1/0
RP/0/RSP0/CPU0:router(config-if)# ipv6 nd reachable-time 1700000

For BNG, this example shows how to configure an IPv6 reachable time of 1,700,000 milliseconds in the dynamic template configuration mode:

RP/0/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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 interface (BNG), on page 351</td>
<td>Displays the usability status of interfaces configured for IPv6.</td>
</tr>
</tbody>
</table>
ipv6 nd start-ra-on-ipv6-enable

To automatically send IPv6 router advertisements to a subscriber interface after configuring IPv6 (by using `ipv6 enable` command), use the `ipv6 nd start-ra-on-ipv6` command in the dynamic template configuration mode. To disable the IPv6 router advertisements, use the `no` form of this command.

```
ipv6 nd [start-ra-on-ipv6-enable]
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

On a dual stack environment, the IPv6 router advertisements are supported by default. The default behavior is that IPv6 neighbor discovery (ND) waits for the IPv6 stack to boot up before triggering a router advertisement.

**Command Modes**

Dynamic template configuration mode

**Command History**

- **Release 6.0**
  - This command was introduced.

**Usage Guidelines**

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.

This command can be used only for IPoE subscriber sessions

**Example**

This example shows how to enable IPv6 router advertisements on an IPv4 subscriber interface:

```
RP/0/RSP0/CPU0:router(config)# dynamic-template type ipsubscriber ipv6ra
RP/0/RSP0/CPU0:router(config)# dynamic-template type ipsubscriber ipv6ra
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 nd idb interface &lt;subscriber-interface&gt; detail location &lt;member-location&gt;</td>
<td>Displays the usability status of interfaces configured for IPv6.</td>
</tr>
</tbody>
</table>
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**

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

None

**Command Modes**

Dynamic template configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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 pl
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 re-enable the sending of IPv6 router advertisement transmissions on a LAN interface, use the `no` form of this command.

```
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 interfaces if IPv6 unicast routing is enabled on the interfaces. IPv6 router advertisements are not sent on other types of interfaces.

**Command Modes**
- Interface configuration (not applicable for BNG)
- Dynamic template configuration (for BNG)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.3.0</td>
<td>This command was supported in the dynamic template configuration mode for BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `no ipv6 nd suppress-ra` command to enable the sending of IPv6 router advertisement transmissions on non-LAN interface types (for example, serial or tunnel interfaces).

For BNG, ensure you run this command in the dynamic template configuration mode. To enter the dynamic template configuration mode, run `dynamic-template` command in the Global Configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6</td>
<td>read, write</td>
</tr>
<tr>
<td>network</td>
<td>read, write</td>
</tr>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example (not applicable for BNG) shows how to suppress IPv6 router advertisements on Gigabit Ethernet interface 0/1/1/0:

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/1/0
RP/0/RSP0/CPU0:router(config-if)# ipv6 nd suppress-ra
```

For BNG, this example shows how to suppress IPv6 router advertisements in the dynamic template configuration mode:
RP/0/RSP0/CPU0:router(config)# **dynamic-template type ppp p1**
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# **ipv6 nd suppress-ra**

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 interface (BNG), on page 351</td>
<td>Displays the usability status of interfaces configured for IPv6.</td>
</tr>
</tbody>
</table>
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*.

To use commands of this module, 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 any command, contact your AAA administrator for assistance.

- ppp authentication (BNG), on page 408
- ppp chap, on page 411
- ppp ipcp, on page 412
- ppp lcp, on page 414
- ppp max-bad-auth (BNG), on page 415
- ppp max-configure (BNG), on page 417
- ppp max-failure (BNG), on page 419
- ppp ms-chap, on page 421
- ppp timeout, on page 422
- show ppp interfaces (BNG), on page 424
- show ppp statistics, on page 430
- show ppp summary, on page 433
**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 in an appropriate configuration mode. To disable PPP authentication, use the `no` form of this command.

```
ppp authentication protocol [protocol [protocol]] {list-name|default}
```

**Syntax Description**

- `protocol` Name of the authentication protocol used for PPP authentication. See Table 26: PPP Authentication Protocols for Negotiation, on page 409 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**

- Interface configuration
- Dynamic template configuration

**Command History**

- **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**

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.
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.

**Note**

Table 26: PPP Authentication Protocols for Negotiation, on page 409 lists the protocols used to negotiate PPP authentication.

Table 26: PPP Authentication Protocols for Negotiation

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>chap</td>
<td>Enables CHAP on an interface.</td>
</tr>
<tr>
<td>ms-chap</td>
<td>Enables Microsoft’s version of CHAP (MS-CHAP) on an interface.</td>
</tr>
<tr>
<td>pap</td>
<td>Enables PAP on an interface.</td>
</tr>
</tbody>
</table>

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.

---

**Examples**

In this example, CHAP is enabled on POS 0/4/0/1 and uses the authentication list MIS-access:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface POS 0/4/0/1
RP/0/RSP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RSP0/CPU0:router(config-if)# ppp authentication chap MIS-access
```

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
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa authentication</td>
<td>Specifies one or more AAA authentication methods for use on serial interfaces running PPP.</td>
</tr>
<tr>
<td>encapsulation</td>
<td>Sets the encapsulation method used by the interface.</td>
</tr>
<tr>
<td>username</td>
<td>Configures a new user with a username, establishes a password, and grants permissions for the user.</td>
</tr>
</tbody>
</table>
**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
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>hostname</code></td>
<td>Sets the CHAP hostname.</td>
</tr>
<tr>
<td><code>chap_hostname</code></td>
<td>Specifies the CHAP hostname.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Dynamic template configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `dynamic-template type ppp` command to enter the ppp dynamic template type configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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 pl
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ppp chap hostname host1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ppp authentication (BNG), on page 408</code></td>
<td>Sets PPP link authentication method.</td>
</tr>
</tbody>
</table>
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_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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use the `dynamic-template type ppp` command to enter the ppp dynamic template type configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
</tbody>
</table>
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 pl
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ppp ipcp
```
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.

```plaintext
ppp lcp [ delay delay_seconds delay_milliseconds | renegotiation ignore ]
```

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This is an example of configuring the **ppp lcp** command in the dynamic template configuration mode:

```plaintext
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp pl
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ppp lcp delay 45 890
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp authentication (BNG), on page 408</td>
<td>Sets PPP link authentication method.</td>
</tr>
</tbody>
</table>
**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
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>retries</code></td>
<td>Number of retries after which the interface is to reset itself. Range is from 0 to 10. Default is 0 retries.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>retries</code></td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface configuration</td>
<td></td>
</tr>
<tr>
<td>Dynamic template configuration</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Release</strong></td>
<td><strong>Modification</strong></td>
</tr>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.2.0</td>
<td>This command was supported in the dynamic template configuration mode for BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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.

**Examples**

In this example, POS interface 0/3/0/1 is set to allow two additional retries after an initial authentication failure (for a total of three failed authentication attempts):

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RSP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RSP0/CPU0:router(config-if)# ppp authentication chap
RP/0/RSP0/CPU0:router(config-if)# ppp max-bad-auth 3
```

This example shows how to allow two additional retries after an initial authentication failure in the dynamic template configuration mode:
ppp max-bad-auth (BNG)

```
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
```

**Syntax Description**

- `retries` Maximum number of retries. Range is 4 through 20. Default is 10.

**Command Default**

- `retries`: 10

**Command Modes**

- Interface configuration
- Dynamic template configuration

**Command History**

- **Release** | **Modification**
  - 3.9.0 This command was introduced.
  - 4.2.0 This command was supported in the dynamic template configuration mode for BNG.

**Usage Guidelines**

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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example shows a limit of four configure requests:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RSP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RSP0/CPU0:router(config-if)# ppp max-configure 4
```

This example shows how a limit of four configure requests is specified in the dynamic template configuration mode:
configure

RP/0/RSP0/CPU0:router(config) dynamic-template type ppp p1

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp max-failure (BNG), on page 419</td>
<td>Configures the maximum number of consecutive CONFNAKs to permit before terminating a negotiation.</td>
</tr>
</tbody>
</table>
**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
```

**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**

- Interface configuration
- Dynamic template configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.2.0</td>
<td>This command was supported in the dynamic template configuration mode for BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To enter the dynamic template configuration mode, run `dynamic-template` command in the Global Configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The `ppp max-failure` command specifies that no more than three CONFNAKs are permitted before terminating the negotiation:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RSP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RSP0/CPU0:router(config-if)# ppp max-failure 3
```

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp max-configure (BNG), on page 417</td>
<td>Specifies the maximum number of configure requests to attempt (without response) before stopping the requests.</td>
</tr>
</tbody>
</table>
**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
```

**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 4.2.0**: This command was introduced.

**Usage Guidelines**

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

**Task ID**

- **ppp**: read, write
- **aaa**: read, write

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 pl
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ppp ms-chap hostname host1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp authentication (BNG), on page 408</td>
<td>Sets PPP link authentication method.</td>
</tr>
</tbody>
</table>
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 ]
```

**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 wait 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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
```
## BNG PPP Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ppp authentication (BNG), on page 408</strong></td>
<td>Sets PPP link authentication method.</td>
</tr>
</tbody>
</table>
**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 mode

### Command History

- **Release 3.9.0** This command was introduced.
- **Release 4.2.0** This command was supported in the dynamic template configuration mode for BNG.
- **Release 5.3.2** The command was modified to include a new output display field, **SRG-state**, as part of geo redundancy support for PPPoE sessions in BNG router.

### Usage Guidelines

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.

Multilink PPP and POS are not supported for BNG Geo Redundancy.

---

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read</td>
</tr>
</tbody>
</table>

---

**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:
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:

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 MRRU: 1500 bytes
  Peer MRRU: 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

This is a sample output of the show ppp interfaces command in the BNG router, having subscriber redundancy group (SRG) in geo redundancy enabled for PPPoE sessions:

show ppp interfaces

Bundle-Ether2.1.pppoe16534 is down, line protocol is up
  SRG Role: Slave
  LCP: Open
Keepalives enabled (60 sec, retry count 5)
Local MRU: 1492 bytes
Peer MRU: 65531 bytes
Authentication
  Of Peer: PAP (Completed as user1@domain.com)
  Of Us: <None>
IPCP: Open
  Local IPv4 address: 12.16.0.1
  Peer IPv4 address: 12.0.250.23
IPV6CP: Initial
  Local IPv6 address: fe80::<n>
  Peer IPv6 address: fe80::<n>

Table 27: show ppp interfaces Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ack-Rcvd</td>
<td>Configuration acknowledgement was received; waiting for peer to send configuration request.</td>
</tr>
<tr>
<td>Ack-Sent</td>
<td>Configuration acknowledgement was sent; waiting for peer to respond to configuration request.</td>
</tr>
<tr>
<td>Authentication</td>
<td>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).</td>
</tr>
<tr>
<td>Closed</td>
<td>Lower layer is up, but this layer is not required.</td>
</tr>
<tr>
<td>Closing</td>
<td>Shutting down due to local change.</td>
</tr>
<tr>
<td>Initial</td>
<td>Connection is idle.</td>
</tr>
<tr>
<td>IPCP</td>
<td>IP Control Protocol (IPCP) state. The seven possible states that may be displayed are as follows:</td>
</tr>
</tbody>
</table>
  - 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. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keepalive</td>
<td>Keepalive setting and interval in seconds for echo request packets.</td>
</tr>
</tbody>
</table>
| 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 |
<p>| 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. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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.             |
| 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|interface|interface-type|interface-path-id|summary|location} [location]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>extended</code></td>
<td>Displays the extended PPP statistics across all interfaces.</td>
</tr>
<tr>
<td><code>interface</code></td>
<td>Displays the PPP statistics for a single interface.</td>
</tr>
<tr>
<td><code>summary</code></td>
<td>Displays aggregated PPP statistics across all interfaces.</td>
</tr>
<tr>
<td><code>location</code></td>
<td>Displays the PPP statistics for interfaces at a location.</td>
</tr>
<tr>
<td><code>location</code></td>
<td>Specifies the location details.</td>
</tr>
<tr>
<td><code>type</code></td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>interface-path-id</code></td>
<td>Physical interface or virtual interface.</td>
</tr>
</tbody>
</table>

**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 mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read</td>
</tr>
</tbody>
</table>

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
(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
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
### Proto-Rej 0 0
### MPLSCP

<table>
<thead>
<tr>
<th></th>
<th>Sent</th>
<th>Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conf-Req</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Conf-Ack</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Conf-Nak</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Conf-Rej</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Term-Req</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Term-Ack</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Proto-Rej</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

### OSICP

<table>
<thead>
<tr>
<th></th>
<th>Sent</th>
<th>Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conf-Req</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Conf-Ack</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Conf-Nak</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Conf-Rej</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Term-Req</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Term-Ack</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Proto-Rej</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ppp interfaces (BNG), on page 424</code></td>
<td>Displays the PPP interfaces.</td>
</tr>
<tr>
<td><code>show ppp summary, on page 433</code></td>
<td>Displays the PPP summary.</td>
</tr>
</tbody>
</table>
**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 mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read</td>
</tr>
</tbody>
</table>

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
------------------------------------
Name  Total Open ACK sent ACK rcvd REQ sent Stop- ping Stop- ing Clos- ing Clos- ing Starting- ing Initial
------ ------ ----- ------ ------ ------ ------ ------ ------ ------ ------ ------ -----
LCP    10300 10300 0 0 0 0 0 0 0 0 0 0 0
CDPCP  100 0 0 100 0 0 0 0 0 0 0 0
IPCP   10000 10000 0 0 0 0 0 0 0 0 0 0
IPv6CP 0 0 0 0 0 0 0 0 0 0 0 0
MPLSCP 0 0 0 0 0 0 0 0 0 0 0 0
OSICP  0 0 0 0 0 0 0 0 0 0 0 0
```
### LCP/Authentication Phases

<table>
<thead>
<tr>
<th>Phase</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LCP Not Negotiated</td>
<td>100</td>
</tr>
<tr>
<td>Authenticating</td>
<td>0</td>
</tr>
<tr>
<td>Line held down</td>
<td>0</td>
</tr>
<tr>
<td>Line Up (Local Termination)</td>
<td>10200</td>
</tr>
<tr>
<td>Line Up (L2 Forwarded)</td>
<td>0</td>
</tr>
<tr>
<td>Line UP (VPDN Tunneled)</td>
<td>100</td>
</tr>
</tbody>
</table>

#### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ppp statistics, on page 430</td>
<td>Displays the PPP statistics.</td>
</tr>
<tr>
<td>show ppp interfaces (BNG), on page 424</td>
<td>Displays the PPP interfaces.</td>
</tr>
</tbody>
</table>
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.

To use commands of this module, 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 any command, contact your AAA administrator for assistance.

- l2tp-class, on page 436
- l2tp-source-ip, on page 438
- l2tp reassembly, on page 439
- process-failures switchover, on page 440
- redundancy (BNG), on page 441
- session-limit (BNG), on page 442
- template (BNG), on page 443
- tunnel, on page 444
- vpdn, on page 445
- vpn, on page 446
- show l2tpv2, on page 447
- show l2tpv2 redundancy, on page 449
- show l2tpv2 redundancy mirroring, on page 451
- show vpdn, on page 453
- show vpdn redundancy, on page 456
- show vpdn redundancy mirroring, on page 457
**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 ]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>c1</td>
<td>Specifies the l2tp class name.</td>
</tr>
<tr>
<td>l1</td>
<td>Specifies the l2tp class name.</td>
</tr>
<tr>
<td>l2tp_class_name</td>
<td>Specifies the l2tp class name.</td>
</tr>
<tr>
<td>authentication</td>
<td>Authenticates the L2TP control connection.</td>
</tr>
<tr>
<td>congestion-control</td>
<td>Enables L2TP congestion control.</td>
</tr>
<tr>
<td>digest</td>
<td>Specifies message digest configuration for L2TPv3 control connection.</td>
</tr>
<tr>
<td>hello-interval</td>
<td>Hides AVPs in outgoing control messages.</td>
</tr>
<tr>
<td>hidden</td>
<td>Sets HELLO message interval.</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies the local hostname for control connection authentication.</td>
</tr>
<tr>
<td>ip</td>
<td>Specifies the settings for tunnel.</td>
</tr>
<tr>
<td>password</td>
<td>Specifies the password for control connection authentication.</td>
</tr>
<tr>
<td>receive-window</td>
<td>Receives the window size for control connection.</td>
</tr>
<tr>
<td>retransmit</td>
<td>Specifies the control message retransmission parameters.</td>
</tr>
<tr>
<td>security</td>
<td>Specifies the L2TP security command.</td>
</tr>
<tr>
<td>timeout</td>
<td>Specifies the control connection timeout parameters.</td>
</tr>
<tr>
<td>tunnel</td>
<td>Specifies the tunnel settings.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

Global Configuration mode
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel, on page 444</td>
<td>Configures L2TP tunnel.</td>
</tr>
</tbody>
</table>
l2tp-source-ip

To configure the tunnel source IP address for the subscriber redundancy group, use the `l2tp-source-ip` command in subscriber redundancy group configuration mode. To remove the tunnel source IP address configuration, use the `no` form of this command.

```
l2tp-source-ip  ip-address
```

**Syntax Description**

| **ip-address** | Source IP address of the L2TP tunnel. |

**Command Default**

None

**Command Modes**

Subscriber redundancy group configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.3.2</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to configure the L2TP tunnel source IP address for the subscriber redundancy group:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# subscriber redundancy group 1
RP/0/RSP0/CPU0:router(config-subscr-red-group)# l2tp-source-ip 10.10.10.1
```
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.

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
None

**Command Modes**
VPDN configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpdn, on page 445</td>
<td>Configures VPDN and enters the VPDN sub-configuration mode.</td>
</tr>
<tr>
<td>redundancy (BNG), on page 441</td>
<td>Enables VPDN redundancy and enters the VPDN redundancy configuration mode.</td>
</tr>
</tbody>
</table>
**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.

### Syntax Description

This command has no keywords or arguments.

### Command Default

None

### Command Modes

VPDN configuration mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

No specific guidelines impact the use of this command.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpdn, on page 445</td>
<td>Configures VPDN and enters the VPDN sub-configuration mode.</td>
</tr>
</tbody>
</table>
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
```

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpdn-template_name</td>
<td>Specifies the vpdn template name.</td>
</tr>
<tr>
<td>description</td>
<td>Specifies the description of the vpdn template.</td>
</tr>
<tr>
<td>caller-id</td>
<td>Specifies the options to apply on calling station id.</td>
</tr>
<tr>
<td>ip</td>
<td>Specifies the tos ip value.</td>
</tr>
<tr>
<td>dsl-line-forwarding</td>
<td>Enables dsl line information forwarding.</td>
</tr>
<tr>
<td>ipv4</td>
<td>Specifies the ipv4 settings for tunnel.</td>
</tr>
<tr>
<td>l2tp-class</td>
<td>Specifies the l2tp class name.</td>
</tr>
<tr>
<td>tunnel</td>
<td>Specifies the l2tp tunnel commands.</td>
</tr>
<tr>
<td>vpn</td>
<td>Specifies the vpn id/vrf name.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

VPDN configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the vpdn command, to enter vpdn configuration submode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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`

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `vpdn template` command to enter vpdn template configuration submode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vpdn, on page 445</code></td>
<td>Configures VPDN and to enter the VPDN sub-configuration mode.</td>
</tr>
</tbody>
</table>
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}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>caller-id</td>
<td>Specifies the options to apply on calling station id.</td>
</tr>
<tr>
<td>history</td>
<td>Enables VPDN history logging.</td>
</tr>
<tr>
<td>l2tp</td>
<td>Specifies the l2tpv2 protocol commands.</td>
</tr>
<tr>
<td>logging</td>
<td>Enables logging for VPDN.</td>
</tr>
<tr>
<td>session-limit</td>
<td>Allows to configure maximum simultaneous VPDN sessions.</td>
</tr>
<tr>
<td>softshut</td>
<td>Specifies that a new session is no longer allowed.</td>
</tr>
<tr>
<td>template</td>
<td>Specifies the VPDN template configuration.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `vpdn` command in Global Configuration mode to enter vpdn sub-configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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
```
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 }
```

**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 4.2.0**
  - This command was introduced.

**Usage Guidelines**
Use the `vpdn template` command to enter vpdn template configuration submode.

**Task ID**
- `tunnel` read, write

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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>class</td>
<td>Displays the L2TP class details.</td>
</tr>
<tr>
<td>counters</td>
<td>Displays the L2TP counter information.</td>
</tr>
<tr>
<td>session</td>
<td>Displays the L2TP session information.</td>
</tr>
<tr>
<td>statistics</td>
<td>Displays the L2TP protocol statistics.</td>
</tr>
<tr>
<td>tunnel</td>
<td>Displays the L2TP tunnel information.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>read</td>
</tr>
<tr>
<td>network</td>
<td>read</td>
</tr>
</tbody>
</table>

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 Na 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
Resend queue size 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2tp-class, on page 436</td>
<td>Configures the l2tp class.</td>
</tr>
</tbody>
</table>
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 mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.3.1</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel</td>
<td>read</td>
</tr>
</tbody>
</table>

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
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>l2tp-class, on page 436</code></td>
<td>Configures the L2TP class.</td>
</tr>
</tbody>
</table>
show l2tpv2 redundancy mirroring

To display the L2TP related mirroring statistics, use the `show l2tpv2 redundancy mirroring` command in the EXEC mode.

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
None

**Command Modes**
EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.1</td>
<td>This command was</td>
</tr>
<tr>
<td></td>
<td>introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>tunnel</td>
</tr>
<tr>
<td></td>
<td>read</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th></th>
<th>Send/Receive/Drop</th>
<th>Since Last Clear</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Send/Receive/Drop</td>
<td></td>
</tr>
<tr>
<td>CCSync</td>
<td>0/0/0</td>
<td>0/0/0</td>
</tr>
<tr>
<td>CCPProtoSync</td>
<td>0/0/0</td>
<td>0/0/0</td>
</tr>
<tr>
<td>CCUnSync</td>
<td>0/0/0</td>
<td>0/0/0</td>
</tr>
<tr>
<td>CCSynAck</td>
<td>0/0/0</td>
<td>0/0/0</td>
</tr>
<tr>
<td>CCIAck</td>
<td>0/0/0</td>
<td>0/0/0</td>
</tr>
<tr>
<td>CCSessionSyncDone</td>
<td>0/0/0</td>
<td>0/0/0</td>
</tr>
<tr>
<td>SessionSync</td>
<td>0/0/0</td>
<td>0/0/0</td>
</tr>
<tr>
<td>AppStatus</td>
<td>0/1/1</td>
<td>0/1/1</td>
</tr>
<tr>
<td>AddCCSteadyState</td>
<td>0/1/0</td>
<td>0/1/0</td>
</tr>
<tr>
<td>DelCCSteadyState</td>
<td>0/0/0</td>
<td>0/0/0</td>
</tr>
<tr>
<td>ADDSessionSteadyState</td>
<td>0/5/3</td>
<td>0/5/3</td>
</tr>
<tr>
<td>DelSessionSteadyState</td>
<td>0/0/0</td>
<td>0/0/0</td>
</tr>
<tr>
<td>CCCotherPackets</td>
<td>0/0/0</td>
<td>0/0/0</td>
</tr>
<tr>
<td>ZLB ACK</td>
<td>0/0/0</td>
<td>0/0/0</td>
</tr>
<tr>
<td>SCCRQ</td>
<td>0/0/0</td>
<td>0/0/0</td>
</tr>
<tr>
<td>SCCRP</td>
<td>0/0/0</td>
<td>0/0/0</td>
</tr>
<tr>
<td>SCCCN</td>
<td>0/1/0</td>
<td>0/1/0</td>
</tr>
<tr>
<td>StopCCN</td>
<td>0/0/0</td>
<td>0/0/0</td>
</tr>
<tr>
<td>Hello</td>
<td>0/0/0</td>
<td>0/0/0</td>
</tr>
<tr>
<td>OCRQ</td>
<td>0/0/0</td>
<td>0/0/0</td>
</tr>
<tr>
<td>OCRP</td>
<td>0/0/0</td>
<td>0/0/0</td>
</tr>
</tbody>
</table>
show l2tpv2 redundancy mirroring

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2tp-class, on page 436</td>
<td>Configures the L2TP class.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>client</code></td>
<td>Displays VPDN client information.</td>
</tr>
<tr>
<td><code>config</code></td>
<td>Displays VPDN configuration information.</td>
</tr>
<tr>
<td><code>history</code></td>
<td>Displays the vpdn session history information.</td>
</tr>
<tr>
<td><code>tunnel destination</code></td>
<td>Displays the vpdn tunnel destination information.</td>
</tr>
<tr>
<td><code>session</code></td>
<td>Displays the vpdn session information.</td>
</tr>
</tbody>
</table>

### Command Default

None

### Command Modes

EXEC mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.2.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 5.3.2</td>
<td>The command was modified to include a new output display field, <strong>SRG-state</strong>, as part of geo redundancy support for PPPoE sessions.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

No specific guidelines impact the use of this command.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>read</td>
</tr>
<tr>
<td>network</td>
<td>read</td>
</tr>
</tbody>
</table>

These are some of the options to use 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: 58795 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, 12tp 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

This is a sample output of the `show vpdn session` command, with geo redundancy enabled for PPPoE sessions:

RP/0/RSP0/CPU0:router# show vpdn session

SRG Role: Master
Subscriber label: 0x42, interface name: Bundle-Ether1.10.pppoe3
    user name: user1@lns2.com
    parent interface: Bundle-Ether1.10
    state: est last change: 00:01:01
time to setup session: 0:2 (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: 58795 remote tunnel id: 54970
    local session id: 46362 remote session id: 16 remote port: 1701
tunnel assigned id:
tunnel client authentication id: LAC
tunnel server authentication id: LNS
tunnel authentication: disabled
class attribute mask:
Subscriber data
    NAS port id: 0/0/1/10
    NAS port type: Virtual PPPoE over VLAN
    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, 12tp busy timeout: 60
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpdn, on page 445</td>
<td>Configures VPDN and enters the VPDN sub-configuration mode.</td>
</tr>
</tbody>
</table>

TOS mode: default
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 mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>read</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpdn, on page 445</td>
<td>Configures VPDN and enters the VPDN sub-configuration mode.</td>
</tr>
<tr>
<td>redundancy (BNG), on page 441</td>
<td>Enables VPDN redundancy and enters the VPDN redundancy configuration mode.</td>
</tr>
</tbody>
</table>
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 mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>read</td>
</tr>
</tbody>
</table>

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 Received:                     2      2
Acks Received:                         0      0
Acks Failed:                           0      0
Timeouts:                              0      0
```
show vpdn redundancy mirroring

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpdn, on page 445</td>
<td>Configures VPDN and enters the VPDN sub-configuration mode.</td>
</tr>
<tr>
<td>redundancy (BNG), on page 441</td>
<td>Enables VPDN redundancy and enters the VPDN redundancy configuration mode.</td>
</tr>
</tbody>
</table>

Messages Processed: 2 2
Message Drops: 0 0
Stale Messages: 0 0
Unknown Ack received: 0 0
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*.

To use commands of this module, 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 any command, contact your AAA administrator for assistance.

- pado delay, on page 460
- pado delay circuit-id, on page 461
- pado delay remote-id, on page 463
- pado delay service-name, on page 465
- pppoe bba-group, on page 467
- pppoe enable bba-group, on page 470
- pppoe in-flight-window, on page 471
- pppoe sessions limit, on page 472
- pppoe sessions throttle, on page 475
- clear pppoe statistics, on page 477
- show pppoe interfaces, on page 479
- show pppoe limits, on page 481
- show pppoe statistics, on page 485
- show pppoe summary, on page 488
- show pppoe throttles, on page 490
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
```

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

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 bb1
RP/0/RSP0/CPU0:router(config-bbagroup)# pado delay 1000
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>pado delay circuit-id, on page 461</strong></td>
<td>Configures a delay for PPPoE PADO message for a PPPoE BBA-Group in BNG, based on the Circuit-ID received in PADI message.</td>
</tr>
<tr>
<td><strong>pado delay remote-id, on page 463</strong></td>
<td>Configures a delay for PPPoE PADO message for a PPPoE BBA-Group in BNG, based on the Remote-ID received in PADI message.</td>
</tr>
<tr>
<td><strong>pado delay service-name, on page 465</strong></td>
<td>Configures a delay for PPPoE PADO message for a PPPoE BBA-Group in BNG, based on the Service-Name received in PADI message.</td>
</tr>
</tbody>
</table>
**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}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>delay</strong></td>
<td>Delay value for PADO message, in milliseconds, based on the Circuit-ID. The range is from 0 to 10000.</td>
</tr>
<tr>
<td><strong>string</strong></td>
<td>Delays the PADO message, when the Circuit-ID string received in PADI message matches the configured string.</td>
</tr>
<tr>
<td><strong>contains</strong></td>
<td>Delays the PADO message, when the Circuit-ID received in PADI message contains the configured string.</td>
</tr>
<tr>
<td><strong>string</strong></td>
<td>String received in PADI message, that needs to be exactly matching the Circuit-ID (when used along with <strong>string</strong> keyword) or the string received in PADI message, that needs to be contained within the Circuit-ID (when used along with the <strong>contains</strong> keyword).</td>
</tr>
</tbody>
</table>

| Command Default | None |
| Command Modes | PPPoE BBA-Group configuration |

<table>
<thead>
<tr>
<th>Command History</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Release</strong></td>
<td><strong>Modification</strong></td>
</tr>
<tr>
<td>4.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Usage Guidelines</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting a value of 0 for <strong>delay</strong> 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.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>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).</td>
<td></td>
</tr>
<tr>
<td>If there are no matches, the configured pado delay is used for PADO message.</td>
<td></td>
</tr>
</tbody>
</table>
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 bbal
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 bbal
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 bbal
RP/0/RSP0/CPU0:router(config-bbagroup)# pado delay circuit-id contains circuit2 5000
```
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.

**Syntax**

```
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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.
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 bb1
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 bb1
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 bb1
RP/0/RSP0/CPU0:router(config-bbagroup)# pado delay remote-id contains remote2 5000
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>pado delay</code>, on page 460</td>
<td>Configures a specific delay for PPPoE PADO message for a PPPoE BBA-Group in BNG.</td>
</tr>
<tr>
<td><code>pado delay circuit-id</code>, on page 461</td>
<td>Configures a delay for PPPoE PADO message for a PPPoE BBA-Group in BNG, based on the Circuit-ID received in PADI message.</td>
</tr>
<tr>
<td><code>pado delay service-name</code>, on page 465</td>
<td>Configures a delay for PPPoE PADO message for a PPPoE BBA-Group in BNG, based on the Service-Name received in PADI message.</td>
</tr>
</tbody>
</table>
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
```

### 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

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.
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>pado delay</code>, on page 460</td>
<td>Configures a specific delay for PPPoE PADO message for a PPPoE BBA-Group in BNG.</td>
</tr>
<tr>
<td><code>pado delay circuit-id</code>, on page 461</td>
<td>Configures a delay for PPPoE PADO message for a PPPoE BBA-Group in BNG, based on the Circuit-ID received in PADI message.</td>
</tr>
<tr>
<td><code>pado delay remote-id</code>, on page 463</td>
<td>Configures a delay for PPPoE PADO message for a PPPoE BBA-Group in BNG, based on the Remote-ID received in PADI message.</td>
</tr>
</tbody>
</table>
**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 | global }
```

**Syntax Description**

- **bba-group-name**: Specifies the bba group name.
- **global**: Specifies the global bba-group.

**Notes**

- **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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>6.2.1</td>
<td>Modified the command to include global BBA-Group.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

BBA-Groups are configured globally (these are essentially configuration templates), containing the PPPoE configuration settings.

When this configuration changes to use a different BBA-Group, then all existing PPPoE sessions running under the interface are terminated.

Among the various BBA-Groups that can be configured on a router, one BBA-Group can be configured as a global BBA-Group. If the maximum limit for PPPoE sessions is set under **pppoe bba-group global** configuration, it indicates the limit for the total number of sessions on the entire router. Currently, **global** BBA-Group supports only configurations related to session limit, except AAA override configuration. For more details, see usage guidelines section of **pppoe sessions limit** command.

Global BBA-Group support in BNG is subjected to these restrictions:

- Currently global BBA-Group supports only configurations related to session limit, except AAA override configuration.
- You cannot change the configuration at run time for global BBA-Group.
• The **global** BBA-Group is not valid for subscriber redundancy group (SRG) in BNG, and hence the **pppoe bba-group global** command must not be used in BNG geo redundancy scenarios.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read,</td>
<td>write</td>
</tr>
</tbody>
</table>

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 global
RP/0/RSP0/CPU0:router(config-bbagroup)# sessions max limit 250
```

This is an example of configuring maximum PPPoE sessions limit for the entire router, under global PPPoE BBA-Group:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pppoe bba-group global
RP/0/RSP0/CPU0:router(config-bbagroup)# sessions max limit 250
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pppoe enable bba-group, on page 470</td>
<td>Enables PPPoE on an interface.</td>
</tr>
</tbody>
</table>
**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
```

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When this configuration changes to use a different BBAGroup, then all existing PPPoE sessions running under the interface are terminated.

**Task ID**

```
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
</tbody>
</table>
```

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pppoe bba-group, on page 467</td>
<td>Enables you to add configuration for a particular bba-group.</td>
</tr>
</tbody>
</table>
pppoe in-flight-window

To configure a limit for the number of PPPoE sessions that are in progression towards established state in BNG, use the `pppoe in-flight-window` command in Global Configuration mode. To remove this limit, use the `no` form of this command.

```
pppoe in-flight-window size
```

**Syntax Description**

<table>
<thead>
<tr>
<th><code>size</code></th>
</tr>
</thead>
</table>

Specifies the window-size for the number of PPPoE sessions that are in progression towards established state in BNG.

**Command Default**

None

**Command Modes**

Global Configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The recommended in-flight-window size for RP-based subscribers is 200, and that for LC-based subscribers is 50. Values higher than these are not recommended for production deployment, as it can lead to system instability.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to configure the in-flight-window size for PPPoE sessions in BNG:

```
RP/0/RSP0/CPU0:router(config)# pppoe in-flight-window 200
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pppoe sessions limit, on page 472</td>
<td>Configures a limit for PPPoE sessions for a PPPoE BBA-Group in BNG.</td>
</tr>
<tr>
<td>pppoe sessions throttle, on page 475</td>
<td>Configures a throttle value for PPPoE sessions for a PPPoE BBA-Group in BNG.</td>
</tr>
</tbody>
</table>
**pppoe sessions limit**

To set the PPPoE sessions limit for a particular PPPoE BBA-Group or for the entire router, 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]
```

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
Modification

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.

Release 6.2.1
Functionality was included to set a global PPPoE session limit, that is, a session limit for the entire router.

Usage Guidelines

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.

The `sessions outer-vlan limit` command limits the sessions only in single VLAN tag scenarios. You must use the `sessions vlan limit` command, to limit the sessions in double VLAN tag scenarios; this limits the maximum number of sessions allowed for each inner VLAN and outer VLAN, for each access-interface.

In order to set a global PPPoE session limit, use the `sessions max limit` command under `pppoe bba-group global` configuration mode. The combined number of sessions on all individual BBA-Groups cannot exceed this global limit. For example, consider a configuration where the global limit is set as 250, the limit of BBA-Group 1 (say, `bba1`) is set as 100, and the limit of BBA-Group 2 (say, `bba2`) is set as 200. If 100 sessions are already created with `bba1`, then only 150 sessions (that is, 250 - 100) can be created with `bba2`, even though `bba2` has a session limit of 200. Similarly there can be different combinations of sessions with local BBA-Groups as long as the global session limit is not exceeded. For more details, see `pppoe bba-group` command.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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
```
This example shows how to set the global PPPoE session limit for a router as 250:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# pppoe bba-group global
RP/0/RSP0/CPU0:router(config-bbagroup)# sessions max limit 250
```
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.

```
pppoe 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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-interface</td>
<td>Throttles PPPoE sessions based on any one access interface</td>
</tr>
<tr>
<td>circuit-id</td>
<td>Throttles PPPoE sessions with any one circuit-id.</td>
</tr>
<tr>
<td>circuit-id-and-remote-id</td>
<td>Throttles PPPoE sessions by circuit-id and remote-id.</td>
</tr>
<tr>
<td>inner-vlan</td>
<td>Throttles PPPoE sessions with any one inner-vlan id.</td>
</tr>
<tr>
<td>mac</td>
<td>Throttles PPPoE sessions from any one mac address.</td>
</tr>
<tr>
<td>mac-iwf</td>
<td>Throttles Inter-Working Function (IWF) sessions from any one mac address.</td>
</tr>
<tr>
<td>outer-vlan</td>
<td>Throttles PPPoE sessions with any one outer-vlan id.</td>
</tr>
<tr>
<td>remote-id</td>
<td>Throttles PPPoE sessions with any one remote-id.</td>
</tr>
<tr>
<td>vlan</td>
<td>Throttles PPPoE sessions with matching vlan ids.</td>
</tr>
<tr>
<td>throttle</td>
<td>Specifies the action of throttling the PPPoE sessions for various attributes.</td>
</tr>
<tr>
<td>request-count</td>
<td>Specifies the number of session requests allowed before throttling.</td>
</tr>
<tr>
<td>request-period</td>
<td>Specifies the time interval during which the session requests are counted.</td>
</tr>
<tr>
<td>blocking-period</td>
<td>Specifies the time interval during which no more requests from the subscriber are accepted, when the subscriber has already been throttled.</td>
</tr>
</tbody>
</table>

**Command Default**

Sessions throttle is disabled by default.

**Command Modes**

PPPoE BBA-Group configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
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

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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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 bbal
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 bbal
RP/0/RSP0/CPU0:router(config-bbagroup)# sessions mac-iwf access-interface throttle 5000 100 50
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pppoe sessions limit, on page 472</td>
<td>Configures a limit for PPPoE sessions for a PPPoE BBA-Group in BNG.</td>
</tr>
<tr>
<td>show pppoe throttles, on page 490</td>
<td>Shows the throttle information for the PPPoE sessions.</td>
</tr>
</tbody>
</table>
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 the EXEC mode.

**clear pppoe statistics [internal] location node-id**

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>internal</code></td>
<td>Clears internal PPPoE statistics.</td>
</tr>
<tr>
<td><code>location</code></td>
<td>Clears PPPoE statistics for a given node.</td>
</tr>
<tr>
<td><code>node-id</code></td>
<td>Specifies the node ID. The node-id argument is entered in the rack/slot/module notation.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows the sample output before and after clearing the PPPoE statistics:

```shell
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

<table>
<thead>
<tr>
<th>Description</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session-stage packet for unknown session</td>
<td>4097</td>
</tr>
<tr>
<td>Session-stage packet with no error</td>
<td>6</td>
</tr>
<tr>
<td>TOTAL</td>
<td>4103</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Packets</th>
<th>Sent</th>
<th>Received</th>
<th>Dropped</th>
</tr>
</thead>
<tbody>
<tr>
<td>PADI</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PADO</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PADR</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PADS (success)</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PADS (error)</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PADT</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Session-stage</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Other</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

TOTAL

<table>
<thead>
<tr>
<th>Packet Error Count</th>
<th>------</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOTAL</td>
<td>0</td>
</tr>
</tbody>
</table>

RP/0/RSP0/CPU0:router#

## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show pppoe statistics, on page 485</td>
<td>Shows the counters for packets received and sent by the PPPoE sessions.</td>
</tr>
</tbody>
</table>
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 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 mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.3.2</td>
<td>The command was modified to include a new output display field, <strong>SRG-state</strong>, as part of geo redundancy support for PPPoE sessions.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.
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
```

This is a sample output of the `show pppoe interfaces` command, with geo redundancy enabled for PPPoE sessions:

```
RP/0/RSP0/CPU0:router# show pppoe interfaces
Bundle-Ether2.1.pppoe16534 is Complete
  Session id: 16534
  Parent interface: Bundle-Ether2.1
  BBA-Group: BBA1
  Local MAC address: 0002.0003.0004
  Remote MAC address: 0000.6201.0103
  Outer VLAN ID: 10
  Tags:
    Service name: AGILENT
    Host-Uniq: 4 bytes, (000e0000)
    SRG-state: SRG-Standby
```
show pppoe limits

To show the PPPoE session limit information, use the `show pppoe limits` command in the EXEC mode mode.

```plaintext
show pppoe limits [active] [{access-interface type interface-path-id | bba-group bba-group-name | location node}]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Active</th>
<th>Shows only those throttles that are currently blocking packets.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>access-interface</td>
<td>Shows PPPoE status for all sessions on a single access interface.</td>
</tr>
<tr>
<td></td>
<td>type</td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td></td>
<td>interface-path-id</td>
<td>Physical interface or virtual interface.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
<td>Use the <code>show interfaces</code> command to see a list of all interfaces currently configured on the router.</td>
</tr>
</tbody>
</table>

For more information about the syntax for the router, use the question mark (?) online help function.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>bba-group</th>
<th>Shows throttles for all interfaces with a given bba-group.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>bba_group_name</td>
<td>Specifies the bba-group to show throttle for.</td>
</tr>
<tr>
<td></td>
<td>location</td>
<td>Shows PPPoE status for all sessions at a location.</td>
</tr>
<tr>
<td></td>
<td>node</td>
<td>Specifies the fully qualified location specification.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>EXEC mode</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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 | No specific guidelines impact the use of this command. |

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read</td>
</tr>
</tbody>
</table>

This is a sample output of the `show pppoe limits` command:
show pppoe limits

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
GE0/1/0/0/12 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:

show pppoe limits

RP/0/RSP0/CPU0:router# show pppoe limits

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: 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

<table>
<thead>
<tr>
<th>Access-Int</th>
<th>Inner VLAN ID</th>
<th>State</th>
<th>#Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>BE2.10</td>
<td>10</td>
<td>Block</td>
<td>10</td>
</tr>
</tbody>
</table>

MAC-IWF-Access-Interface session limits not configured.

Inner-VLAN-ID session limit information:
Maximum session limit: 10 sessions
Warning threshold: 8 sessions

<table>
<thead>
<tr>
<th>Access-Int</th>
<th>Inner VLAN ID</th>
<th>State</th>
<th>#Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>BE2.10</td>
<td>10</td>
<td>Block</td>
<td>10</td>
</tr>
</tbody>
</table>

MAC-IWF-Access-Interface session limits not configured.

Outer-VLAN-ID session limit information:
Maximum session limit: 10 sessions
Warning threshold: 8 sessions

<table>
<thead>
<tr>
<th>Access-Int</th>
<th>Outer VLAN ID</th>
<th>State</th>
<th>#Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>BE2.10</td>
<td>10</td>
<td>Block</td>
<td>10</td>
</tr>
</tbody>
</table>

MAC-IWF-Access-Interface session limits not configured.

Outer-VLAN-ID session limit information:
Maximum session limit: 10 sessions
Warning threshold: 8 sessions

<table>
<thead>
<tr>
<th>Access-Int</th>
<th>Outer VLAN ID</th>
<th>State</th>
<th>#Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>BE2.10</td>
<td>10</td>
<td>Block</td>
<td>10</td>
</tr>
</tbody>
</table>

MAC-IWF-Access-Interface session limits not configured.

VLAN-ID session limit information:
Maximum session limit: 10 sessions
Warning threshold: 8 sessions

<table>
<thead>
<tr>
<th>Access-Int</th>
<th>Outer, Inner VLAN ID</th>
<th>State</th>
<th>#Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>BE2.10</td>
<td>10, 10</td>
<td>Block</td>
<td>10</td>
</tr>
</tbody>
</table>

MAC-IWF-Access-Interface session limits not configured.

Circuit-ID-and-Remote-ID session limit information:
Maximum session limit: 10 sessions
Warning threshold: 8 sessions

<table>
<thead>
<tr>
<th>Circuit-ID</th>
<th>State</th>
<th>#Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>circuit0</td>
<td>Block</td>
<td>10</td>
</tr>
<tr>
<td>remote10</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This table describes the significant fields displayed in the `show pppoe limits` command output:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block</td>
<td>Specifies that the number of sessions is at the maximum limit.</td>
</tr>
<tr>
<td>OK</td>
<td>Specifies that the number of sessions is below the maximum limit and the warning threshold (if configured).</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warn</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pppoe sessions limit, on page 472</td>
<td>Configures a limit for PPPoE sessions for a PPPoE BBA-Group in BNG.</td>
</tr>
<tr>
<td>show pppoe throttles, on page 490</td>
<td>Shows the throttle information for the PPPoE sessions.</td>
</tr>
<tr>
<td>show pppoe interfaces, on page 479</td>
<td>Shows a summary of the protocol state for the specified PPPoE interface filtered by circuit-id, remote-id, interface, or location.</td>
</tr>
<tr>
<td>show pppoe statistics, on page 485</td>
<td>Shows the counters for packets received and sent by the PPPoE sessions.</td>
</tr>
<tr>
<td>show pppoe summary, on page 488</td>
<td>Shows summary information of the PPPoE sessions.</td>
</tr>
</tbody>
</table>
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 mode.

```
show pppoe statistics \{access-interface\}\{typeinterface-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 mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

```
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read</td>
</tr>
</tbody>
</table>
```

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
```
show pppoe statistics

Packets Sent Received Dropped

<table>
<thead>
<tr>
<th></th>
<th>Sent</th>
<th>Received</th>
<th>Dropped</th>
</tr>
</thead>
<tbody>
<tr>
<td>PADI</td>
<td>0</td>
<td>3723</td>
<td>18</td>
</tr>
<tr>
<td>PADO</td>
<td>3182</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PADS</td>
<td>0</td>
<td>1732</td>
<td>93</td>
</tr>
<tr>
<td>PADS (success)</td>
<td>1601</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PADS (error)</td>
<td>38</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PADT</td>
<td>158</td>
<td>552</td>
<td>9</td>
</tr>
<tr>
<td>Session-stage</td>
<td>0</td>
<td>18</td>
<td>17</td>
</tr>
<tr>
<td>Other</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

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 received: 1
- PADS received: 1
- Unknown packet type received: 1
- Unexpected Session-ID in packet: 1
- No Service-Name Tag: 1
- PADT for unknown session: 1
- 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: 1
- 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 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 mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read</td>
</tr>
</tbody>
</table>

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 mode.

```
show pppoe throttles [active] [access-interface type interface-path-id | bba-group bba-group-name | location node]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>active</td>
<td>Shows only those throttles that are currently blocking packets.</td>
</tr>
<tr>
<td>access-interface</td>
<td>Shows PPPoE status for all sessions on a single access interface.</td>
</tr>
<tr>
<td>type</td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or virtual interface.</td>
</tr>
<tr>
<td>bba-group</td>
<td>Shows throttles for all interfaces with a given bba-group.</td>
</tr>
<tr>
<td>bba_group_name</td>
<td>Specifies the bba-group name.</td>
</tr>
<tr>
<td>location</td>
<td>Shows PPPoE status for all sessions at a location.</td>
</tr>
<tr>
<td>node</td>
<td>Specifies the fully qualified location specification.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.3.1</td>
<td>The command output was extended for the throttle for circuit-id, remote-id, inner-vlan, outer-vlan, vlan and circuit-id-and-remote-id.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

```
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read</td>
</tr>
</tbody>
</table>
```

This is the sample output of the `show pppoe throttles` command:
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 Monitor 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

<table>
<thead>
<tr>
<th>Circuit-ID</th>
<th>State</th>
<th>Time Since</th>
</tr>
</thead>
<tbody>
<tr>
<td>circuit0</td>
<td>Block</td>
<td>91s 8s 10 10</td>
</tr>
</tbody>
</table>

Remote-ID throttle information:
Max packets per request period: 10
Request period duration: 10s
Blocking period duration: 100s

<table>
<thead>
<tr>
<th>Time Since</th>
<th>Remote-ID</th>
<th>State</th>
<th>left</th>
<th>reset</th>
<th>PADI</th>
<th>PADR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>remote10</td>
<td>Block</td>
<td>91s</td>
<td>8s</td>
<td>10</td>
<td>10</td>
</tr>
</tbody>
</table>

Inner-VLAN-ID throttle information:
Max packets per request period: 10
Request period duration: 10s
Blocking period duration: 100s

<table>
<thead>
<tr>
<th>Time Since</th>
<th>Access-Int</th>
<th>Inner VLAN ID</th>
<th>State</th>
<th>left</th>
<th>reset</th>
<th>PADI</th>
<th>PADR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>BE2.10</td>
<td>10</td>
<td>Block</td>
<td>91s</td>
<td>8s</td>
<td>10</td>
<td>10</td>
</tr>
</tbody>
</table>

Outer-VLAN-ID throttle information:
Max packets per request period: 10
Request period duration: 10s
Blocking period duration: 100s

<table>
<thead>
<tr>
<th>Time Since</th>
<th>Access-Int</th>
<th>Outer VLAN ID</th>
<th>State</th>
<th>left</th>
<th>reset</th>
<th>PADI</th>
<th>PADR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>BE2.10</td>
<td>10</td>
<td>Block</td>
<td>91s</td>
<td>8s</td>
<td>10</td>
<td>10</td>
</tr>
</tbody>
</table>

VLAN-ID throttle information:
Max packets per request period: 10
Request period duration: 10s
Blocking period duration: 100s

<table>
<thead>
<tr>
<th>Time Since</th>
<th>Access-Int</th>
<th>Outer, Inner VLAN ID</th>
<th>State</th>
<th>left</th>
<th>reset</th>
<th>PADI</th>
<th>PADR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>BE2.10</td>
<td>10, 10</td>
<td>Block</td>
<td>91s</td>
<td>8s</td>
<td>10</td>
<td>10</td>
</tr>
</tbody>
</table>

Circuit-ID-and-Remote-ID throttle information:
Max packets per request period: 0
Request period duration: 0s
Blocking period duration: 0s

<table>
<thead>
<tr>
<th>Time Since</th>
<th>Circuit-ID</th>
<th>Remote-ID</th>
<th>State</th>
<th>left</th>
<th>reset</th>
<th>PADI</th>
<th>PADR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>circuit0</td>
<td>remote10</td>
<td>Block</td>
<td>91s</td>
<td>8s</td>
<td>10</td>
<td>10</td>
</tr>
</tbody>
</table>

This table describes the significant fields displayed in the `show pppoe throttles` command output:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block</td>
<td>Specifies that the throttle is active and that packets are dropped.</td>
</tr>
<tr>
<td>Idle</td>
<td>Specifies that the packets relevant to the throttle are not yet received.</td>
</tr>
<tr>
<td>Monitor</td>
<td>Specifies that the packets are counted, but the throttle is not yet active.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>pppoe sessions throttle, on page 475</strong></td>
<td>Configures a throttle value for PPPoE sessions for a PPPoE BBA-Group in BNG.</td>
</tr>
<tr>
<td><strong>show pppoe limits, on page 481</strong></td>
<td>Shows the PPPoE session limit information.</td>
</tr>
<tr>
<td><strong>show pppoe interfaces, on page 479</strong></td>
<td>Shows a summary of the protocol state for the specified PPPoE interface filtered by circuit-id, remote-id, interface, or location.</td>
</tr>
<tr>
<td><strong>show pppoe statistics, on page 485</strong></td>
<td>Shows the counters for packets received and sent by the PPPoE sessions.</td>
</tr>
<tr>
<td><strong>show pppoe summary, on page 488</strong></td>
<td>Shows summary information of the PPPoE sessions.</td>
</tr>
</tbody>
</table>
show pppoe throttles
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.

To use commands of this module, 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 any command, contact your AAA administrator for assistance.

- qos account, on page 496
- qos output minimum-bandwidth, on page 498
- service-policy (QoS-BNG), on page 499
- service-policy (interface BNG), on page 502
- shape average (BNG), on page 505
- show qos inconsistency (BNG), on page 507
- show qos interface (BNG), on page 509
- show qos shared-policy-instance (BNG), on page 520
- show qos summary BNG, on page 522
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 ]
```

### 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command is available only in the dynamic template type ppp submode.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos</td>
<td>read, write</td>
</tr>
</tbody>
</table>
This is an example of configuring the `qos account` command in dynamic template configuration mode:

```plaintext
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>qos output minimum-bandwidth, on page 498</code></td>
<td>Sets the minimum guaranteed output bandwidth for a subscriber.</td>
</tr>
</tbody>
</table>
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 kbps).

**Command Default**

None

**Command Modes**

Dynamic template configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrrp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos account, on page 496</td>
<td>Enables QoS Layer 2 overhead accounting.</td>
</tr>
</tbody>
</table>
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 [subscriber-group |group-name|resourceid0|resourceid1|resourceid2|resourceid3] | resource-id value
```

**Ingress and Egress VLAN Policies:**

```
service-policy {input |output} service_policy_name
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>input</code></td>
<td>Attaches the specified service-policy to the ingress direction.</td>
</tr>
<tr>
<td><code>output</code></td>
<td>Attaches the specified service-policy to the egress direction.</td>
</tr>
<tr>
<td><code>service_policy_name</code></td>
<td>Name of the input or output service-policy.</td>
</tr>
<tr>
<td><code>subscriber-parent</code></td>
<td>Groups subscribers and attaches them to an aggregate shaper based on a logical Group-ID.</td>
</tr>
<tr>
<td><code>subscriber-group</code></td>
<td>Groups subscribers and attaches them to an aggregate shaper based on a logical Group-ID.</td>
</tr>
<tr>
<td><code>group-name</code></td>
<td>Name of the logical group for the subscribers.</td>
</tr>
<tr>
<td><code>resource-id0</code>, <code>resource-id1</code>, <code>resource-id2</code>, <code>resource-id3</code></td>
<td>Specifies reserved group-ID values to achieve increased scale support on physical LC-based interfaces.</td>
</tr>
<tr>
<td><code>resource-id</code></td>
<td>Specifies a resource-ID that allows to map the desired chunk to be used for this particular S-VLAN and all the subscribers under it.</td>
</tr>
<tr>
<td><code>value</code></td>
<td>The resource-ID value that ranges from 0-3.</td>
</tr>
</tbody>
</table>

**Note**

- This keyword applies only to the egress direction.
- Policies with `subscriber-group` do not support `resource-id`.

### Command Default

None

### Command Modes

Interface configuration
**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.2.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.3.0</td>
<td>Support for the resource-id keyword was added.</td>
</tr>
<tr>
<td>Release 4.3.1</td>
<td>Support for the ingress and egress VLAN policies on an access interface was added.</td>
</tr>
<tr>
<td>Release 6.2.1</td>
<td>Support was added for subscriber-group keyword.</td>
</tr>
<tr>
<td>Release 6.3.2</td>
<td>Specifies reserved group-ID values to achieve increased scale support on physical LC-based interfaces.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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 to which its parent interface is associated with.

The system default does not offer larger scale configuration for subscriber sessions. So, in order to achieve a larger scale for each TM over physical LC-based interfaces, use the group-ID feature configuration along with reserved keywords such as resourceid0, resourceid1, resourceid2 and resourceid3 that act as the group-IDs of the subscriber. This functionality is available in Cisco ASR 9000 High Density 100GE Ethernet line cards, and is supported only on Cisco IOS XR 64-bit operating system.

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.

For restrictions on the usage of group-based grand parent shaping feature (using subscriber-group), see Cisco ASR 9000 Series Aggregation Services Router Broadband Network Gateway Configuration Guide.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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:

```plaintext
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:

```plaintext
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
```

This example shows how to enable group-based grand parent shaping feature by grouping subscribers and attaching them to an aggregate shaper based on a logical Group-ID:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether1.1234
RP/0/RSP0/CPU0:router(config-if)# encapsulation ambiguous dot1q 1-4
RP/0/RSP0/CPU0:router(config-if)# service-policy output P0 subscriber-parent subscriber-group G0
RP/0/RSP0/CPU0:router(config-if)# service-policy output P1 subscriber-parent subscriber-group G1
RP/0/RSP0/CPU0:router(config-if)# service-policy output P2 subscriber-parent subscriber-group G2
RP/0/RSP0/CPU0:router(config-if)# service-policy output P3 subscriber-parent subscriber-group G3
```

This example shows how to enable subscriber QoS on main interface, and to achieve higher subscriber scale configuration on physical line card-based interfaces:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet 0/1/0/10
RP/0/RSP0/CPU0:router(config-if)# service-policy output parent_policy subscriber-parent subscriber-group resourceid0
RP/0/RSP0/CPU0:router(config-if)# service-policy output parent_policy subscriber-parent subscriber-group resourceid1
RP/0/RSP0/CPU0:router(config-if)# service-policy output parent_policy subscriber-parent subscriber-group resourceid2
RP/0/RSP0/CPU0:router(config-if)# service-policy output parent_policy subscriber-parent subscriber-group resourceid3
```
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]
```

**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**

- Interface configuration. This does not apply to BNG.
- Layer 2 transport configuration. This does not apply to BNG.
- Subinterface configuration. This does not apply to BNG.
- Dynamic template configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>3.9.0</td>
<td>This command was updated to support shared policy instance over bundle interfaces.</td>
</tr>
<tr>
<td>4.3.0</td>
<td>The command was supported in dynamic template configuration mode in BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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.
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

This example shows policy map policy1 applied to Packet-over-SONET/SDH (POS) interface 0/2/0/0:

```bash
RP/0/RSP0/CPU0:router(config)# class-map class1
RP/0/RSP0/CPU0:router(config-cmap)# match precedence ipv4 1
RP/0/RSP0/CPU0:router(config-cmap)# exit
RP/0/RSP0/CPU0:router(config)# policy-map policy1
RP/0/RSP0/CPU0:router(config-pmap)# class class1
RP/0/RSP0/CPU0:router(config-pmap-c)# set precedence 2
RP/0/RSP0/CPU0:router(config-pmap)# exit
RP/0/RSP0/CPU0:router(config)# interface POS 0/2/0/0
RP/0/RSP0/CPU0:router(config-if)# service-policy output policy1
```

This example shows policy map policy2 applied to GigabitEthernet subinterface 0/1/0/0.1:

```bash
RP/0/RSP0/CPU0:router(config)# class-map class2
RP/0/RSP0/CPU0:router(config-cmap)# exit
RP/0/RSP0/CPU0:router(config)# policy-map policy2
RP/0/RSP0/CPU0:router(config-pmap)# class-map class2
RP/0/RSP0/CPU0:router(config-pmap-c)# set precedence 3
RP/0/RSP0/CPU0:router(config-pmap)# exit
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0.1
RP/0/RSP0/CPU0:router(config-subif)# service-policy input policy2 shared-policy-instance ethernet101
```

This example does not apply to BNG.

This example shows policy map policy 1 applied to Bundle-Ether interfaces 100.1 and 100.2:

```bash
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether 100.1
RP/0/RSP0/CPU0:router(config-if)# service-policy policy1 shared-policy-instance subscriber1
RP/0/RSP0/CPU0:router(config-if)# exit
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether 100.2
RP/0/RSP0/CPU0:router(config-if)# service-policy output policy1 shared-policy-instance subscriber1
```

This example does not apply to BNG.
This example is specific to BNG. It shows policy map policy1 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
```
shape average (BNG)

To shape traffic to the indicated bit rate according to the algorithm specified, use the `shape average` command in policy map class configuration mode. To remove traffic shaping, use the `no` form of this command.

```
shape average {percent {percentage | $shape-rate = percentage} | rate [units] | per-thousand value | per-million value [$shape-rate = rate [units]]}
```

**Syntax Description**

- **percent** `percentage` Specifies the interface bandwidth in percentage. Values can be from 1 to 100.

- **rate** `rate` (Optional) Indicates the shaping rate in the specified units. Values can be from 1 to 4294967295.

- **units** `units` (Optional) Specifies the units for the bandwidth. Values can be:
  - **Excess burst size**—values can be from 1 to 4294967295
  - **bps**—bits per second (default)
  - **gbps**—gigabits per second
  - **kbps**—kilobits per second
  - **mbps**—megabits per second

- **per-thousand** `value` Specifies shape rate as parts per thousand of the available bandwidth.

- **per-million** `value` Specifies shape rate as parts per million of the available bandwidth.

- `$` `value` Specifies that a QoS shaper variable is configured.

- **shape-rate** `QoS shaper variable name that can be parameterized`.

**Command Default**

- `units`: `bps`

**Command Modes**

Policy map class configuration

**Command History**

```
Release 3.7.2  This command was introduced.

Release 5.2.0  $shape-rate =rate option was added to support QoS shaper parameterization in BNG.
```

**Usage Guidelines**

For `shape average` commands in the child policy, the reference used for percentage parameters is relative to the maximum rate of the parent. If shaping or policing is not configured on the parent, then the parent inherits the interface rate.

If you have both shape and bandwidth configured for a class, ensure that the shape percent value is always greater than the percent value for bandwidth.

The shaper parameters, used to override the locally-configured values in BNG, can either be sent to BNG by the RADIUS server during connection establishment, as CISCO VSAs in an Access Accept message, or can be sent to BNG as part of the CoA messages.
This example sets traffic shaping to 50 percent of the parent shaper rate:

```
RP/0/RSP0/CPU0:router(config)# policy-map policy1
RP/0/RSP0/CPU0:router(config-pmap)# class class1
RP/0/RSP0/CPU0:router(config-pmap-c)# shape average percent 50
```

This example shows how to set traffic shaping to 100000 kbps:

```
RP/0/RSP0/CPU0:router(config)# policy-map policy1
RP/0/RSP0/CPU0:router(config-pmap)# class class1
RP/0/RSP0/CPU0:router(config-pmap-c)# shape average 100000 kbps
```

This example shows how to set the default value of QoS shape-rate variable (shaper4) as 100000 kbps, in BNG:

```
RP/0/RSP0/CPU0:router(config)# policy-map policy1
RP/0/RSP0/CPU0:router(config-pmap)# class class1
RP/0/RSP0/CPU0:router(config-pmap-c)# shape average $shaper4 = 100000 kbps
```
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 mode

**Command History**

- **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 enter the dynamic template configuration mode, run `dynamic-template` command in the Global Configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos</td>
<td>read</td>
</tr>
</tbody>
</table>
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:

==========================================================================
Interface Direction Policy Name SPI Name
==========================================================================
GigabitEthernet0/7/0/1.5 output parent-none

This example displays summary counts of inconsistency warnings:

RP/0/RSP0/CPU0:router# show qos inconsistency summary location 0/7/CPU0

Summary Counts of QoS Inconsistency Warnings:

<table>
<thead>
<tr>
<th>Inconsistency Warning Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANCP - No Shaper at top policymap</td>
<td>1</td>
</tr>
<tr>
<td>ANCP - Downstream Rate less than Shaper Rate</td>
<td>4</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show qos interface (BNG), on page 509</td>
<td>Displays QoS information for a specific interface.</td>
</tr>
</tbody>
</table>
# show qos interface (BNG)

To display QoS information for a specific interface, use the `show qos interface` command in the EXEC mode.

```plaintext
show qos interface type interface-path-id {input|output} {member type interface-path-id} [host-link interface-path-id | location node-id]
```

## Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>type</code></td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>interface-path-id</code></td>
<td>Either a physical interface instance or a virtual interface instance as follows:</td>
</tr>
<tr>
<td></td>
<td>• Physical interface instance. Naming notation is <code>rack/slot/module/port</code> and a slash between values is required as part of the notation.</td>
</tr>
<tr>
<td></td>
<td>• <code>rack</code>: Chassis number of the rack.</td>
</tr>
<tr>
<td></td>
<td>• <code>slot</code>: Physical slot number of the modular services card or line card.</td>
</tr>
<tr>
<td></td>
<td>• <code>module</code>: Module number. A physical layer interface module (PLIM) is always 0.</td>
</tr>
<tr>
<td></td>
<td>• <code>port</code>: Physical port number of the interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>• Virtual interface instance. Number range varies depending on interface type.</td>
</tr>
<tr>
<td><code>input</code></td>
<td>Attaches the specified policy map to the input interface.</td>
</tr>
<tr>
<td><code>output</code></td>
<td>Attaches the specified policy map to the output interface.</td>
</tr>
<tr>
<td><code>member</code></td>
<td>Specifies member of bundle interface or pin-down (generic list) interface of PWHE interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This keyword is applicable only for bundle and PWHE interface.</td>
</tr>
</tbody>
</table>

For more information about the syntax for the router, use the question mark (?) online help function.
**show qos interface (BNG)**

<table>
<thead>
<tr>
<th>host-link</th>
<th>(Optional) Specifies the host-link.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Note</strong> This keyword is applicable only for satellite information.</td>
</tr>
</tbody>
</table>

| 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 mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.3.0</td>
<td>The command was supported in dynamic template configuration mode in BNG.</td>
</tr>
<tr>
<td>Release 5.1.1</td>
<td>The show qos interface command output was updated to display Flow Aware call admission control (CAC) and user based rate limiting (UBRL) information.</td>
</tr>
</tbody>
</table>

The show qos interface command output was updated to display QoS Offload on satellite information.

PWHE interface type **PW-Ether** and **PW-IW** were added.

The show output was updated for PWHE interface details.

**Usage Guidelines**
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.

(Only BNG) To enter the dynamic template configuration mode, run **dynamic-template** command in the Global Configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**
This is the sample output which shows the QoS information on a Ten Gigabit Ethernet interface, applicable for the releases 5.3.2 onwards:

```
RP/0/RSP0/CPU0: tardis1-pwhe-spe#show qos interface tenGigE 0/0/0/0/0 output
Interface: TenGigE0_0_0_0_0 output
Bandwidth configured: 10000000 kbps Bandwidth programed: 10000000 kbps
ANCP user configured: 0 kbps ANCP programed in HW: 0 kbps
Port Shaper programed in HW: 0 kbps
Policy: EGRESS_CHILD_POLICY Total number of classes: 8
----------------------------------------------------------------------
Level: 0 Policy: EGRESS_CHILD_POLICY Class: cp1
QueueID: 525248 (Priority 1)
```
Queue Limit: 126976 kbytes Abs-Index: 179 Template: 0 Curve: 7
Shape CIR Profile: INVALID

Level: 0 Policy: EGRESS_CHILD_POLICY Class: cp2
QueueID: 525249 (Priority 2)
Queue Limit: 13824 kbytes (54443 packets) Abs-Index: 129 Template: 0 Curve: 6
Shape CIR Profile: INVALID

Level: 0 Policy: EGRESS_CHILD_POLICY Class: cp3
QueueID: 525251 (Priority 3)
Queue Limit: 13824 kbytes (54443 packets) Abs-Index: 129 Template: 0 Curve: 5
Shape CIR Profile: INVALID

Level: 0 Policy: EGRESS_CHILD_POLICY Class: cp4
QueueID: 525252 (Priority 4)
Queue Limit: 13824 kbytes (54443 packets) Abs-Index: 129 Template: 0 Curve: 0
Shape CIR Profile: INVALID

Level: 0 Policy: EGRESS_CHILD_POLICY Class: cp5
QueueID: 525253 (Priority 5)
Queue Limit: 13824 kbytes (54443 packets) Abs-Index: 129 Template: 0 Curve: 0
Shape CIR Profile: INVALID

Level: 0 Policy: EGRESS_CHILD_POLICY Class: cp6
QueueID: 525254 (Priority 6)
Queue Limit: 13824 kbytes (54443 packets) Abs-Index: 129 Template: 0 Curve: 0
Shape CIR Profile: INVALID

Level: 0 Policy: EGRESS_CHILD_POLICY Class: cp7
QueueID: 525255 (Priority 7)
Queue Limit: 13824 kbytes (54443 packets) Abs-Index: 129 Template: 0 Curve: 0
Shape CIR Profile: INVALID

Level: 0 Policy: EGRESS_CHILD_POLICY Class: class-default
QueueID: 525250 (Priority Normal)
Queue Limit: 13824 kbytes (54443 packets) Abs-Index: 129 Template: 0 Curve: 0
Shape CIR Profile: INVALID
WFQ Profile: 0/206 Committed Weight: 906 Excess Weight: 906
Bandwidth: 0 kbps, BW sum for Level 0: 0 kbps, Excess Ratio: 900

This is the sample output shows the QoS information on a GigabitEthernet interface:

RP/0/RSP0/CPU0:router# 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

---------------------------------------------------------------------

This is the sample output shows the QoS information on a GigabitEthernet interface:
This example shows the L2VPN QoS information on TenGigE 0/4/0/0/7 interface:

```
RP/0/RSP0/CPU0:router# show qos interface TenGigE 0/4/0/0/7 output
Thu Sep 5 10:02:14.217 UTC
NOTE:- Configured values are displayed within parentheses
Interface TenGigE0/4/0/0/7 ifh 0x2000048 -- output policy
NPU Id: 0
Total number of classes: 8
Interface Bandwidth: 10000000 kbps
Accounting Type: Layer2 (Include Layer 2 encapsulation and above)

Level1 Class = prec-1
Schedule entry ID = 0x32 (0x10001)
Egressq Queue ID = 50 (LP queue)
Queue Max. BW. = 100000 kbps (1 %)
Queue Min. BW. = 0 kbps (default)
Weight = 25 (BWR not configured)
Guaranteed service rate = 100000 kbps
TailDrop Threshold = 1250000 bytes / 100 ms (default)
Policer not configured for this class
WRED not configured for this class

Level1 Class (HP2) = prec-2
Schedule entry ID = 0x33 (0x10002)
Egressq Queue ID = 51 (HP2 queue)
Guaranteed service rate = 10000000 kbps
TailDrop Threshold = 12500000 bytes / 10 ms (default)
Policer Bucket Id = 0x9000100095103
Policer committed rate = 99968 kbps (1 %)
Policer conform burst = 124928 bytes (default)
Policer conform action = Just TX
```
Policer exceed action = DROP PKT
WRED not configured for this class

Level1 Class = prec-3
Schedule entry ID = 0x36 (0x10003)
Egressq Queue ID = 54 (LP queue)
Queue Max. BW. = 100000 kbps (1 %)
Queue Min. BW. = 100000 kbps (1 %)
Weight = 25 (BWR not configured)
Guaranteed service rate = 100000 kbps
TailDrop Threshold = 13750 bytes / 1 ms (1100 us)
Policer not configured for this class
WRED not configured for this class

Level1 Class = prec-5
Schedule entry ID = 0x37 (0x10004)
Egressq Queue ID = 55 (LP queue)
Queue Max. BW. = 100000 kbps (1 %)
Queue Min. BW. = 0 kbps (default)
Weight = 25 (BWR not configured)
Guaranteed service rate = 100000 kbps
TailDrop Threshold = 1250000 bytes / 100 ms (default)
Policer not configured for this class

WRED table handle = 0x0

RED profile
WRED Min. Threshold = 249856 bytes (20 ms)
WRED Max. Threshold = 374784 bytes (30 ms)
WRED First Segment = 1334
WRED Segment Size = 11

Level1 Class (HP1) = prec-6
Schedule entry ID = 0x3a (0x10005)
Egressq Queue ID = 58 (HP1 queue)
Guaranteed service rate = 10000000 kbps
TailDrop Threshold = 12500000 bytes / 10 ms (default)
Policer Bucket Id = 0x90001000a5103
Policer committed rate = 99968 kbps (1 %)
Policer conform burst = 124928 bytes (default)
Policer conform action = Just TX
Policer exceed action = DROP PKT
WRED not configured for this class

Level1 Class (HP1) = prec-7
Schedule entry ID = 0x3b (0x10006)
Egressq Queue ID = 59 (HP1 queue)
Guaranteed service rate = 10000000 kbps
TailDrop Threshold = 12500000 bytes / 10 ms (default)
Policer Bucket Id = 0x90001000b5103
Policer committed rate = 99968 kbps (1 %)
Policer conform burst = 124928 bytes (default)
Policer conform action = Just TX
Policer exceed action = DROP PKT
WRED not configured for this class

Level1 Class = prec-0
Egressq Queue ID = 62 (Default LP queue)
Policer Bucket Id = 0x90001000c5103
Policer committed rate = 99968 kbps (1 %)
Policer conform burst = 1245184 bytes (default)
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: 131265 (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: 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
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
WFQ Profile: 2/9 Committed Weight: 10 Excess Weight: 10
Bandwidth: 0 kbps, BW sum for Level 2: 0 kbps, Excess Ratio: 1
This is the sample output of the `show qos interface` command for CAC:

```
RP/0/RSP0/CPU0# show qos interface gigabitEthernet 0/1/0/0 input

Interface: GigabitEthernet0_1_0_0 input
Bandwidth configured: 1000000 kbps Bandwidth programed: 1000000 kbps
ANCP user configured: 0 kbps ANCP programed in HW: 0 kbps
Port Shaper programed in HW: 0 kbps
Policy: premium_services (Flow Aware Policy) Total number of classes: 5
```

This is the sample output of the `show qos interface` command for CAC:
This is the sample output of the `show qos interface` command for UBRL:

```
RP/0/RSP0/CPU0:router# show qos interface gigabitEthernet 0/1/0/0 input

Interface: GigabitEthernet0_1_0_0 input
Bandwidth configured: 1000000 kbps Bandwidth programed: 1000000 kbps
ANCP user configured: 0 kbps ANCP programmed in HW: 0 kbps
Port Shaper programmed in HW: 0 kbps
Policy: voice_flow (Flow Aware Policy) Total number of classes: 3

Level: 0 Policy: voice_flow Class: voice_prec6
QueueID: 98 (Port Default)
Policer Profile: 56 (Single)
Conform: 50000 kbps (5 mbps) Burst: 62500 bytes (0 Default)
Child Policier Conform: set dscp 34
Child Policier Exceed: DROP
Child Policier Violate: DROP

Level: 0 Policy: voice_flow Class: ubrl1
Flow QoS Info: UBRL
```
This is the sample output of the `show qos interface` command for PW-HE subinterfaces.

```
RP/0/RSP0/CPU0:router#  show qos interface  pw-ether1.1 input member tengige0/2/0/5
Interface: TenGigE0_2_0_5 input  Bandwidth configured: 10000000 kbps  Bandwidth programed: 10000000 kbps
ANCP user configured: 0 kbps  ANCP programed in HW: 0 kbps
Port Shaper programed in HW: 0 kbps
Policy: PW-HE-Ingress Total number of classes: 9

Level: 0 Policy: PW-HE-Ingress Class: class-default
QueueID: N/A  Policer Profile: 55 (Single)
Conform: 2000000 kbps (2 gbps) Burst: 25000000 bytes (0 Default)

Level: 1 Policy: DSCP_CE-PE_ETM Class: multicast_limit
Parent Policy: PW-HE-Ingress Class: class-default
QueueID: 161 (Port Priority 2)
Policer Profile: 57 (SrTCM)
Conform: 40000 kbps (2 percent) Burst: 128000 bytes (128000 bytes)
Peak Burst: 128000 bytes (256000 bytes)
Child Policer Conform: set prec 5
Child Policer Exceed: set prec 4
Child Policer Violate: set prec 4

Level: 1 Policy: DSCP_CE-PE_ETM Class: dscp_AF4x_ipprec_4
Parent Policy: PW-HE-Ingress Class: class-default
QueueID: 162 (Port Default)
Policer Profile: 58 (Single)
Conform: 10000000 kbps (5 percent) Burst: 256000 bytes (256000 bytes)
Child Policer Conform: set exp-imp 5
Child Policer Exceed: DROP
Child Policer Violate: DROP

Level: 1 Policy: DSCP_CE-PE_ETM Class: dscp_EF_ipprec_5
Parent Policy: PW-HE-Ingress Class: class-default
QueueID: 160 (Port Priority 1)
Policer Profile: 56 (Single)
Conform: 20000 kbps (1 percent) Burst: 125000 bytes (50 ms)
Child Policer Conform: TX
Child Policer Exceed: DROP
Child Policer Violate: DROP

Level: 0 Policy: voice_flow Class: class-default
QueueID: 98 (Port Default)
Policer Profile: 58 (Single)
Conform: 10000 kbps (10 mbps) Burst: 125000 bytes (0 Default)

Level: 0 Policy: voice_flow Class: class-default
QueueID: 98 (Port Default)
Policer Profile: 57 (Single)
Conform: 100000000 kbps (100000000 kbps) Burst: 12500000 bytes (12500000 bytes)
Child Policer Conform: set dscp 34
Child Policer Exceed: DROP
Child Policer Violate: DROP
```

UBRL Flow Mask Mode: src-ip (0x80)
UBRL Flow Age: 200 Seconds
Number of UBRL flows learnt: 0
QueueID: 98 (Port Default)
Flow Policer Profile: 58 (Single)
Conform: 10000 kbps (10 mbps) Burst: 125000 bytes (0 Default)
Catch-all Policer Profile: 57 (Single)
Conform: 100000000 kbps (100000000 kbps) Burst: 12500000 bytes (12500000 bytes)
Child Policer Conform: set dscp 34
Child Policer Exceed: DROP
Child Policer Violate: DROP

---------------------------------------------------------------
Level: 0 Policy: voice_flow Class: class-default
QueueID: 98 (Port Default)
Policer Profile: 57 (Single)
Conform: 100000000 kbps (100000000 kbps) Burst: 12500000 bytes (12500000 bytes)
Child Policer Conform: set dscp 34
Child Policer Exceed: DROP
Child Policer Violate: DROP

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 0 class</td>
<td>Level 0 class identifier in hexadecimal format.</td>
</tr>
<tr>
<td>Level 1 class</td>
<td>Level 1 class identifier in hexadecimal format.</td>
</tr>
<tr>
<td>class name</td>
<td>Name that was assigned to this class with the <code>class</code> command.</td>
</tr>
<tr>
<td>Conform</td>
<td>Number of conform packets transmitted.</td>
</tr>
<tr>
<td>Burst</td>
<td>Configured burst size, expressed in bytes, gigabytes (GB), kilobytes (KB), megabytes (MB), milliseconds (ms), or microseconds (us).</td>
</tr>
<tr>
<td>Queue ID</td>
<td>Queue identifier.</td>
</tr>
</tbody>
</table>
### QOS Commands

#### show qos interface (BNG)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Child Policer Conform</td>
<td>Child Policer conform action (transmitted or dropped).</td>
</tr>
<tr>
<td>Child Policer Exceed</td>
<td>Child Policer exceed action (transmitted or dropped).</td>
</tr>
<tr>
<td>Child Policer Violate</td>
<td>Child Policer violate action (transmitted or dropped).</td>
</tr>
<tr>
<td>Flow QoS Info</td>
<td>Information pertaining to CAC actions, and UBRL.</td>
</tr>
<tr>
<td>CAC Flow Mask Mode</td>
<td>Configured flow mask for CAC actions.</td>
</tr>
<tr>
<td>CAC Flow Rate</td>
<td>Configured rate for CAC actions.</td>
</tr>
<tr>
<td>CAC Rate</td>
<td>Configured total bandwidth for CAC admitted flows.</td>
</tr>
<tr>
<td>UBRL Flow Mask Mode</td>
<td>Configured flow mask for UBRL.</td>
</tr>
<tr>
<td>Flow Age</td>
<td>Configured expiry time to purge out stale flow records set in the flow cache.</td>
</tr>
</tbody>
</table>

#### Related Commands

(Not applicable for BNG)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show qos inconsistency (BNG), on page 507</td>
<td>Displays inconsistency information for the QoS policy on an interface.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>instance-name</td>
<td>String of up to 32 characters to identify the shared policy instance.</td>
</tr>
<tr>
<td>input</td>
<td>Displays details for the shared policy instance attached to the input interface.</td>
</tr>
<tr>
<td>output</td>
<td>Displays details for the shared policy instance attached to the output interface.</td>
</tr>
<tr>
<td>location node-id</td>
<td>Location of node. The node-id argument is entered in rack/slot/module notation.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 3.9.0</td>
<td>This command was updated to support shared policy instance over bundle interfaces.</td>
</tr>
<tr>
<td>Release 4.3.0</td>
<td>The command was supported in BNG.</td>
</tr>
<tr>
<td>Release 5.1.1</td>
<td>This command was updated to support SPI over PW-Ether subinterface.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To enter the dynamic template configuration mode, run `dynamic-template` command in the Global Configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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# 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 WFO Profile: 1 Committed Weight: 1 Excess Weight: 1
```
show qos shared-policy-instance spi5 output location 0/1/cPU0

Interface: GigabitEthernet0_1_1_5

shared-policy-instance: spi5 output
Bandwidth configured: 1000000 kbps Bandwidth programed: 1000000 kbps
ANCP user configured: 0 kbps ANCP programed in HW: 0 kbps
Port Shaper programed in HW: 0 kbps
Policy: parent Total number of classes: 3

Level: 0 Policy: parent Class: class-default
QueueID: N/A
Shape CIR Profile : NONE
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: child Class: prec1
Parent Policy: parent Class: class-default
QueueID: 131112 (Priority 1)
Queue Limit: 318 kbytes Abs-Index: 46 Template: 0 Curve: 6
Shape CIR Profile: INVALID
Policer Profile: 56 (Single)
Conform: 25000 kbps (5 percent) Burst: 312500 bytes (0 Default)
Child Policer Conform: TX
Child Policer Exceed: DROP
Child Policer Violate: DROP

Level: 1 Policy: child Class: class-default
Parent Policy: parent Class: class-default
QueueID: 131114 (Priority Normal)
Queue Limit: 5888 kbytes Abs-Index: 109 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 1: 0 kbps, Excess Ratio: 1
show qos summary BNG

To view the QoS summary, use the `show qos summary` command in EXEC mode.

```
show qos summary {shared-policy-instance instance-name location node-id/policer {interface type instance|location node-location] policy policy-name {interface type instance|location node-location] queue {interface type instance|location node-location] policy-name} {input|output} [member type instance] [host-link type instance] [location node-location] [np np-location]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>shared-policy-instance instance-name</td>
<td>String of up to 32 characters to identify the shared policy instance.</td>
</tr>
<tr>
<td>police</td>
<td>Show policer interface statistics.</td>
</tr>
<tr>
<td>policy policy-name</td>
<td>String to identify the policy.</td>
</tr>
<tr>
<td>queue</td>
<td>Show queue statistics.</td>
</tr>
<tr>
<td>interface type instance</td>
<td>Interface type and instance. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>location node-location</td>
<td>Identifies fully qualified location specification.</td>
</tr>
<tr>
<td>input</td>
<td>Shows the specified policy map to the input interface.</td>
</tr>
<tr>
<td>output</td>
<td>Shows the specified policy map to the output interface.</td>
</tr>
<tr>
<td>np np-location</td>
<td>(Optional) Node processor location. The node processor location is np0, np1, np2, or np3.</td>
</tr>
<tr>
<td></td>
<td>The <code>np</code> keyword is available only for BVI interface type.</td>
</tr>
<tr>
<td>member</td>
<td>Specifies member's interface name.</td>
</tr>
<tr>
<td></td>
<td>The <code>member</code> keyword is available only for bundle-ether, PW-Ether and PW-IW interface types.</td>
</tr>
<tr>
<td>host-link</td>
<td>(Optional) Specifies the host-link.</td>
</tr>
<tr>
<td></td>
<td>This keyword is applicable only for satellite interfaces.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.3.0</td>
<td>The command was supported in dynamic template configuration mode in BNG.</td>
</tr>
<tr>
<td></td>
<td>The <code>np</code> keyword was introduced.</td>
</tr>
</tbody>
</table>
Release Modification

Release 5.1.1 PWHE interface type PW-Ether and PW-IW were added.

Usage Guidelines

To enter the dynamic template configuration mode, run dynamic-template command in the Global Configuration mode.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

This example shows the results of the command to show interfaces at location 0/1/CPU0 for a shared-policy-instance:

```
RP/0/RSP0/CPU0:router# show qos summary shared-policy-instance bundlespi location 0/1/CPU0 output
List of interfaces/NPs retrieved
GigabitEthernet0/1/1/1 (member of Bundle-Ether1.1)
GigabitEthernet0/1/1/2 (member of Bundle-Ether1.1)
```

This example shows policer interface statistics of BVI interface at location 0/5/cpu0:

```
RP/0/RSP0/CPU0:router# show qos summary police interface bvi 1 output location 0/5/cpu0 np np1
Legend:
-------
1. Policer ID is displayed in HEX.
2. A '*' against the counter means the action is drop.
3. Conform displays match counter for non-policer leaf.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Class</th>
<th>PoliceID</th>
<th>Conform</th>
<th>Exceed</th>
<th>Violate</th>
</tr>
</thead>
<tbody>
<tr>
<td>BVI1</td>
<td>NP1</td>
<td>foo</td>
<td>6145</td>
<td>0</td>
<td>0*</td>
</tr>
<tr>
<td></td>
<td></td>
<td>:dscp48</td>
<td>6146</td>
<td>0</td>
<td>0*</td>
</tr>
<tr>
<td></td>
<td></td>
<td>:class-default</td>
<td>6146</td>
<td>0</td>
<td>0*</td>
</tr>
</tbody>
</table>
show qos summary BNG
Subscriber and Session Redundancy Commands

This module describes the Cisco IOS XR software commands used to configure the subscriber and session redundancy 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*.

To use commands of this module, 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 any command, contact your AAA administrator for assistance.

- access-tracking (BNG), on page 527
- accounting interim variation, on page 529
- bng-interface (subscriber), on page 530
- clear session-redundancy, on page 531
- clear subscriber session, on page 532
- core-tracking, on page 534
- disable (BNG), on page 535
- enable-fast-switchover, on page 537
- hold-timer (BNG), on page 538
- http-enrichment parameter-list, on page 540
- http-enrichment parameter-list (subscriber), on page 542
- interface-list (BNG), on page 544
- peer (BNG), on page 547
- preferred-role (BNG), on page 549
- peer route-disable, on page 551
- revertive-timer (BNG), on page 552
- source-interface (BNG), on page 554
- session redundancy, on page 556
- session redundancy group, on page 557
- session redundancy switchover, on page 558
- session redundancy synchronize, on page 560
- state-control-route, on page 561
- subscriber arp scale-mode-enable, on page 563
- subscriber arp uncond-proxy-arp-enable, on page 564
- subscriber featurette dhcp-renew-author, on page 565
- subscriber featurette identity-change, on page 566
• subscriber redundancy, on page 567
• subscriber redundancy group, on page 568
• subscriber redundancy switchover, on page 569
• subscriber redundancy synchronize, on page 571
• subscriber session limit, on page 573
• tracking-disable (BNG), on page 574
• virtual-mac, on page 575
• virtual-mac-disable, on page 576
• virtual-mac-prefix, on page 577
• show sessionmon license, on page 578
• show subscriber database, on page 580
• show subscriber database template, on page 586
• show subscriber feature accounting, on page 588
• show subscriber manager sadb, on page 591
• show subscriber manager statistics, on page 592
• show subscriber redundancy group, on page 600
• show subscriber redundancy summary, on page 604
• show subscriber running-config, on page 606
• show subscriber session, on page 608
• show subscriber session filter, on page 617
• show subscriber session history, on page 619
To configure object tracking for detecting access connectivity for the specific Subscriber Redundancy Group (SRG) or Session Redundancy Group (SERG), use the **access-tracking** command in the respective group configuration mode.

To remove the object tracking configuration, use the **no** form of this command.

**access-tracking  access-tracking-obj**

**Syntax Description**

*access-tracking-obj*  Access tracking object for the specific SRG.

**Command Default**

None

**Command Modes**

Subscriber redundancy group configuration.

Session redundancy group configuration.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.2.2</td>
<td>This command was introduced for SRG.</td>
</tr>
<tr>
<td>Release 6.2.1</td>
<td>This command was introduced for SERG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Object tracking feature allows correlation of the role of BNG SRG/SERG with the role or status of the underlying access-interface, and it is the key for automatic switchovers and for handling failure scenarios.

You must configure the track object first and then configure that track object under the SRG/SERG which holds that particular interface. This ensures that SRG/SERG master or slave role follows the underlying access role.

Advertisement of the summary route for the subscriber address/subnet pool can be also controlled through the same access-tracking object (See example section). This ensures that the subscriber summary route (or routes) is activated only when the underlying access is up or active and only then it is re-distributed into core routing. The slave does not advertise the route into the core.

For details on configuring track object, see *System Management Configuration Guide for Cisco ASR 9000 Series Routers*.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to configure object tracking for detecting access connectivity for the specific SRG in MC-LAG scenario:

Configuring the track object:
Configuring that track object under the SRG which holds that particular interface:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# subscriber redundancy
RP/0/RSP0/CPU0:router(config-subscr-red)# group 1
RP/0/RSP0/CPU0:router(config-subscr-red-group)# access-tracking mclag-be1
```

Configuring access-tracking - Routing:

```
routing static
  address-family ipv4 unicast
    200.0.0.0/16 Null0 track mclag-be1
  address-family ipv6 unicast
    20::/64 Null0 track mclag-be1

router isis 1
  address-family ipv4 unicast
    redistribute static
  address-family ipv6 unicast
    redistribute static
```
accounting interim variation

To introduce a random delay between successive interim accounting messages of sessions or services in BNG, use the `accounting interim variation` command in subscriber manager configuration mode. To remove this random delay, use the `no` form of this command.

```
accounting interim variation value
```

**Syntax Description**

`value` Interim timeout randomization value, in percentage.

The range is from 0 to 50. By default, this value is zero (0), which means there is no interim timeout randomization.

**Command Default**

By default, randomization is disabled.

**Command Modes**

Subscriber manager configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Follow these usage guidelines while applying randomization:

- Randomization cannot be applied for too small interim timeouts (that is, for timeouts less than 2 minutes).

- If interim timeout is T seconds, the value x is selected from an interval [L, T]. By default, L is 100 percent of T (that is, 0% variance from T).

- The maximum value of T-L is 900 seconds (that is, 15 minutes).

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to configure a random delay of 50% variance between successive interim accounting messages of sessions or services:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# subscriber manager
RP/0/RSP0/CPU0:router(config-subscriber-manager)# accounting interim variation 50
```
bng-interface (subscriber)

To set the interface that need to be used as bng identifier, use the `bng-interface` command in the subscriber configuration mode.

```
bng-interface interface-name
```

**Syntax Description**

- `interface-name` Specifies the interface that will be set as the bng-identifier. The IPv4/IPv6 address of this interface is used as the bng IP address.

**Command Default**

None

**Command Modes**

Subscriber configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.5.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

None

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to set the bng-identifier interface.

```
RP/0/RSP0/CPU0:router(configure)# subscriber
RP/0/RSP0/CPU0:router(config-subscriber)# bng-interface Loopback8
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>http-enrichment parameter-list</code>, on page 540</td>
<td>Enables http header enrichment feature for BNG subscribers.</td>
</tr>
<tr>
<td><code>http-enrichment parameter-list (subscriber)</code>, on page 542</td>
<td>Configures the master list of all the parameters for http-enrichment.</td>
</tr>
</tbody>
</table>
clear session-redundancy

To clear the sessions for an SERG use the `clear session-redundancy` command in EXEC mode mode.

```
clear session-redundancy [ group name [ interface interface-type interface-name interface-id ] ]
```

**Syntax Description**

```
interface-id   Identifier value for the access interface mapped to the slave SERG.
```

**Command Default**

None

**Command Modes**

Privileged Executive mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

```
Task ID   Operation
network   execute
```

This example shows how to clear the subscriber sessions for an SERG.

```
RP/0/RSP0/CPUD0:router# clear session-redundancy group 1
```
clear subscriber session

To clear the subscriber sessions in BNG, use the `clear subscriber session` command in EXEC mode mode.

clear subscriber session {all | debug { subscriber-label } | identifier { access-interface interface-type interface-instance ipv4 | ipv6 IANA} ip-address | interface interface-type interface-instance} [location node-id]

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Clears all subscriber sessions.</td>
</tr>
<tr>
<td>debug subscriber-label</td>
<td>Clears debug tracking of unique subscriber session.</td>
</tr>
<tr>
<td>identifier</td>
<td>Clears the subscriber session information based on the identifier(s) you select.</td>
</tr>
<tr>
<td>access-interface</td>
<td>Clears the subscriber session based on the access interface name.</td>
</tr>
<tr>
<td>interface-type</td>
<td>Specifies the interface type whose subscriber sessions you want to delete.</td>
</tr>
<tr>
<td>interface-instance</td>
<td>Specifies either a physical interface instance or a virtual interface instance that you want to delete.</td>
</tr>
</tbody>
</table>

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.

ipv4                  | Clears the DHCP IPv4 subscriber session information specific to an interface and IPv4 network-address/prefix. |
### clear subscriber session

**ipv6 IANA**
- Clears the DHCP IPv6 subscriber session information specific to an interface and IPv6 address/prefix.

**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 mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.4.1</td>
<td>This command was modified to include the option to clear DHCP IPv6 IANA subscriber sessions on an access-interface.</td>
</tr>
<tr>
<td>Release 4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
No specific guidelines impact the use of this command.

### Task ID
**Task ID**
- Operation: execute

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
```

This example shows how to clear DHCP IPv6 subscriber sessions on a particular access-interface:

```
RP/0/RSP0/CPU0:router# clear subscriber session identifier access-interface bundle-ether 1.1 ipv6 IANA 2001:DB8:1::1
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show subscriber session, on page 608</td>
<td>Displays the subscriber management session information.</td>
</tr>
</tbody>
</table>
core-tracking

To configure an additional object for track connectivity to the core network (such as RADIUS or DHCP servers), and to initiate automatic switchover in the event of a BNG connectivity loss even while access is up or active, use the core-tracking command in subscriber redundancy group configuration mode. To remove the object tracking configuration, use the no form of this command.

```
core-tracking  core-tracking-obj
```

Syntax Description

- `core-tracking-obj` Core tracking object for the specific SRG.

Command Default

None

Command Modes

Subscriber redundancy group configuration.

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.2.2</td>
<td></td>
</tr>
</tbody>
</table>

Usage Guidelines

This is an optional command.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to configure object tracking for detecting core connectivity for the specific SRG:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# subscriber redundancy
RP/0/RSP0/CPU0:router(config-subscr-red)# group 1
RP/0/RSP0/CPU0:router(config-subscr-red-group)# core-tracking route-to-radius
```
disable (BNG)

To disable BNG geo redundancy feature across all subscriber redundancy groups (SRGs) or session redundancy groups (SERG), use the disable command in the respective group configuration mode.

To disable a specific SRG/SERG, use the disable command in the respective group configuration mode. To remove the disable configuration, use the no prefix for this command.

disable

This command has no keywords or arguments.

Command Default
None

Command Modes
subscriber redundancy
subscriber redundancy group
session redundancy
session redundancy group

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.2.2</td>
<td>This command was introduced for SRG.</td>
</tr>
<tr>
<td>Release 6.2.1</td>
<td>This command was introduced for SERG.</td>
</tr>
</tbody>
</table>

Usage Guidelines
No specific guidelines impact the use of this command.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Subscriber Redundancy Group

This example shows how to disable geo redundancy feature for all SRGs:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# subscriber redundancy
RP/0/RSP0/CPU0:router(config-subscr-red)# disable
```

This example shows how to disable a specific SRG:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# subscriber redundancy
RP/0/RSP0/CPU0:router(config-subscr-red)# group 1
RP/0/RSP0/CPU0:router(config-subscr-red-group)# disable
```
Session Redundancy Group

This example shows how to disable geo redundancy feature for all SERGs:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# session redundancy
RP/0/RSP0/CPU0:router(config-session-red)# disable
```

This example shows how to disable a specific SERG:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# session redundancy
RP/0/RSP0/CPU0:router(config-session-red)# group 1
RP/0/RSP0/CPU0:router(config-session-red-group)# disable
```
enable-fast-switchover

To enable traffic between peer-to-peer subscriber redundancy groups in BNG, use the `enable-fast-switchover` command in subscriber redundancy group configuration mode. To disable this feature, use the `no` form of this command.

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
None

**Command Modes**
Subscriber redundancy group configuration.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The `enable-fast-switchover` command must be configured prior to configuring `state-control-route`. If `state-control-route` is already configured, you must remove that configuration and re-configure it after `enable-fast-switchover` is configured.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to enable traffic between peer-to-peer subscriber redundancy groups in BNG:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# subscriber redundancy group 110
RP/0/RSP0/CPU0:router(config-subscr-red-group)# enable-fast-switchover
```
hold-timer (BNG)

To configure the duration for which the dynamic switchover is suspended after a role change in BNG geo redundancy feature scenario, use the `hold-timer` command in subscriber/session redundancy configuration mode. To configure hold timer for a specific subscriber redundancy group (SRG) or a session redundancy group (SERG), use this command in the respective group configuration mode.

To remove the hold timer configuration, use the `no` prefix for this command.

```
hold-timer hold-timer
```

**Syntax Description**

- `hold-timer` Hold timer value, in minutes.
  The range is from 1 to 65535.

**Command Default**

By default, the hold-time is zero. That is, back to back switchovers are allowed.

**Command Modes**

- Subscriber redundancy
- Subscriber redundancy group
- Session redundancy
- Session redundancy group

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.2.2</td>
<td>This command was introduced for SRG.</td>
</tr>
<tr>
<td>Release 6.2.1</td>
<td>This command was introduced for SERG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This is an optional command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Session Redundancy Group**

This example shows how to configure hold-timer across all SERGs, in BNG geo redundancy feature scenario:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# session redundancy
RP/0/RSP0/CPU0:router(config-session-red)# hold-timer 15
```
This example shows how to configure hold-timer for a specific SERG, in BNG geo redundancy feature scenario:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# session redundancy
RP/0/RSP0/CPU0:router(config-session-red)# group 1
RP/0/RSP0/CPU0:router(config-session-red-group)# hold-timer 20
```
http-enrichment parameter-list

To enable the enrichment of the HTTP GET request header with the parameters specified and proxying of the enriched HTTP request, use the `http-enrichment parameter-list` action under the respective class-map in the policy-map configuration mode.

```
http-enrichment parameter-list { bng-interface | hostname | subscriber-ip | subscriber-mac }
```

**Syntax Description**

- **bng-interface**
  Specifies that the IPv4/IPv6 address of the interface that is configured as the BNG interface will be added as part of the enrichment header. If IPv4 address is not configured for the BNG interface it will be set as 0.0.0.0 and if IPv6 address is not configured it will be set as 0::0.

- **hostname**
  Specifies that the hostname of the router will be added as enrichment header.

- **subscriber-ip**
  Specifies that the subscriber's IPv4 and IPv6 address will be added as enrichment header.

- **subscriber-mac**
  Specifies that the subscriber's MAC address will be added as enrichment header.

**Command Default**

None

**Command Modes**

Policy-map configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.5.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command supports the setting of all possible combinations of the defined parameters, that is, 15 combinations with 4 parameters. For any changes required in the parameter list, the user will have to configure a new parameter-list. This will override the previously configured parameter-list.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to configure a PBR based policy-map with http-enrichment enabled on one of the classes.

```
RP/0/RSP0/CPU0:router (configure)# policy-map type pbr http-enrichment-policy
RP/0/RSP0/CPU0:router (config-pmap)# class type traffic open-garden-class
RP/0/RSP0/CPU0:router (config-pmap-c)# transmit
RP/0/RSP0/CPU0:router (config-pmap-c)# exit
```
RP/0/RSP0/CPU0:router(config-pmap)# class type traffic http-enrich-class1
RP/0/RSP0/CPU0:router(config-pmap-c)# http-enrichment parameter-list subscriber-mac hostname bng-interface
RP/0/RSP0/CPU0:router(config-pmap-c)# exit
RP/0/RSP0/CPU0:router(config-pmap-c)# class class-default
RP/0/RSP0/CPU0:router(config-pmap-c)# drop

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>http-enrichment parameter-list (subscriber), on page 542</td>
<td>Configures the master list of all the parameters for http-enrichment.</td>
</tr>
<tr>
<td>bng-interface (subscriber), on page 530</td>
<td>Specifies the interface that is the bng identifier.</td>
</tr>
</tbody>
</table>
http-enrichment parameter-list (subscriber)

To configure the master list of all the parameters that are needed for http enrichment across all class-map http-enrichment actions, use the `http-enrichment parameter-list` command in the subscriber configuration mode.

```
http-enrichment parameter-list { bng-interface | hostname | subscriber-ip | subscriber-mac }
```

**Syntax Description**

- **bng-interface**: Specifies that the IPv4/IPv6 address of the interface that is configured as the BNG interface will be added as part of the enrichment header. If IPv4 address is not configured for the BNG interface it will be set as 0.0.0.0 and if IPv6 address is not configured it will be set as 0::0.

- **hostname**: Specifies that the hostname of the router will be added as enrichment header.

- **subscriber-ip**: Specifies that the subscriber's IPv4 and IPv6 address will be added as enrichment header.

- **subscriber-mac**: Specifies that the subscriber's MAC address will be added as enrichment header.

**Command Default**

None

**Command Modes**

Subscriber configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.5.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command supports the setting of all possible combinations of the defined parameters, that is, 15 combinations with 4 parameters. For any changes required in the parameter list, the user will have to configure a new parameter-list. This will override the previously configured parameter-list.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to configure the master-list of http-enrichment parameters that are used in http-enrichment actions configured across all class-maps.

```
RP/0/RSP0/CPU0:router(configure)# subscriber
```
RP/0/RSP0/CPU0:router(config-subscriber)# http-enrichment parameter-list subscriber-mac
hostname bng-interface

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>http-enrichment parameter-list</strong>, on page 540</td>
<td>Enables http header enrichment feature for BNG subscribers.</td>
</tr>
<tr>
<td></td>
<td><strong>bng-interface (subscriber)</strong>, on page 530</td>
<td>Specifies the interface that is the bng identifier.</td>
</tr>
</tbody>
</table>
interface-list (BNG)

To configure the interface list (mapping list of all access ports) that are part of a specific subscriber redundancy group (SRG) or a session redundancy group (SERG), use the `interface-list` command in the respective group configuration mode. To remove the interface list configuration, use the `no` form of this command.

```
interface-list [interface interface-type interface-name {id interface-id|sub-if-range sub-if-start-range sub-if-end-range id-range id-start-range id-end-range}]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>id</code></td>
<td>Specifies the mapping identifier of the interface-list. The identifier for particular interface must be same on both master and slave nodes.</td>
</tr>
<tr>
<td><code>interface-id</code></td>
<td>Identifier value for the interface to be mapped on to the slave SRG/SERG.</td>
</tr>
<tr>
<td><code>sub-if-range</code></td>
<td>Specifies the range of sub-interfaces to be added for the given interface.</td>
</tr>
<tr>
<td><code>sub-if-start-range</code></td>
<td>Start value of sub-interface range. The range is from 0 to 2147483647.</td>
</tr>
<tr>
<td><code>sub-if-end-range</code></td>
<td>End value of sub-interface range. The range is from 0 to 2147483647.</td>
</tr>
<tr>
<td><code>id-range</code></td>
<td>Specifies the range of interface-list identifiers.</td>
</tr>
<tr>
<td><code>id-start-range</code></td>
<td>Start ID of the interface to be mapped on to the SRG/SERG peer. The range is from 1 to 65535.</td>
</tr>
<tr>
<td><code>id-end-range</code></td>
<td>End ID of the interface to be mapped on to the SRG/SERG peer. The range is from 1 to 65535.</td>
</tr>
</tbody>
</table>

### Command Default

None

### Command Modes

Subscriber redundancy group configuration.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.2</td>
<td>This command was introduced for SRG.</td>
</tr>
<tr>
<td>6.2.1</td>
<td>This command was introduced for SERG.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Because BNG works only on sub-interfaces, it is required to configure sub-interfaces under SRG/SERG; not the entire bundle or port.

Sub-interfaces on physical ports spanning different line cards (LC), or mix of physical port sub-interfaces and bundle (or other virtual interfaces like Pseudowire Headend) sub-interfaces is not allowed.

One access sub-interface can belong to only one SRG/SERG.
Because the scope of mapping ID is only within a particular SRG/SERG, same ID can be used in a different SRG/SERG.

The ID assigned to sub-interfaces within an SRG/SERG is used for correlation or mapping of sub-interface pairings across the peer routers. This allows for pairing of different interface or port numbers or types across routers.

Access interfaces can also be explicitly configured even if those sub-interfaces are not existing. Those interfaces become operational under the SRG/SERG when they are actually created.

Removal or modification (for example, change of mapping ID) of sub-interfaces in SRG/SERG during runtime has the same effect of disabling redundancy on them. This results in corresponding sessions getting cleared on the slave side.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Subscriber Redundancy Group

This example shows how to assign one or more access sub-interface under a subscriber redundancy group (SRG) in BNG:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# subscriber redundancy
RP/0/RSP0/CPU0:router(config-subscr-red)# group 1
RP/0/RSP0/CPU0:router(config-subscr-red-group)# interface-list
RP/0/RSP0/CPU0:router(config-subscr-red-grp-intf)# interface Bundle-Ether1.10 id 210
RP/0/RSP0/CPU0:router(config-subscr-red-grp-intf)# interface Bundle-Ether1.11 id 211
```

This example shows how to assign one or more access sub-interface (as a range) under a SRG in BNG:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# subscriber redundancy
RP/0/RSP0/CPU0:router(config-subscr-red)# group 1
RP/0/RSP0/CPU0:router(config-subscr-red-group)# interface-list
RP/0/RSP0/CPU0:router(config-subscr-red-grp-intf)# interface Bundle-Ether1 sub-if-range 1 9 id-range 201 209
```

### Session Redundancy Group

This example shows how to assign one or more access sub-interface under a session redundancy group (SERG) in BNG:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# session redundancy
RP/0/RSP0/CPU0:router(config-session-red)# group 1
RP/0/RSP0/CPU0:router(config-session-red-group)# interface-list
RP/0/RSP0/CPU0:router(config-session-red-grp-intf)# interface Bundle-Ether1.10 id 210
RP/0/RSP0/CPU0:router(config-session-red-grp-intf)# interface Bundle-Ether1.11 id 211
```
This example shows how to assign one or more access sub-interface (as a range) under an SERG in BNG:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router (config)# session redundancy
RP/0/RSP0/CPU0:router (config-session-red)# group 1
RP/0/RSP0/CPU0:router (config-session-red-group)# interface-list
RP/0/RSP0/CPU0:router (config-session-red-grp-intf)# interface Bundle-Ether1 sub-if-range 1 9 id-range 201 209
```
**peer (BNG)**

To configure the peer router for a subscriber redundancy group (SRG) or session redundancy group (SERG) in BNG, use the `peer` command in the respective group configuration mode.

To remove the peer router configuration, use the `no` prefix for this command.

```
peer peer-ip
```

**Syntax Description**

`peer-ip` The peer IPv4 or IPv6 address that is used to establish channel to the peering router in the SRG/SERG.

**Command Default**

None

**Command Modes**

Subscriber redundancy group configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.2.2</td>
<td>This command was introduced for SRG.</td>
</tr>
<tr>
<td>Release 6.2.1</td>
<td>This command was introduced for SERG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The IPv4 or global IPv6 address of the source-interface configured on the peer router must be configured using this command. You must ensure that the configured addresses are reachable from the respective peer routers.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Subscriber Redundancy Group

This example shows how to configure a peer router for a subscriber redundancy group (SRG) in BNG:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# subscriber redundancy
RP/0/RSP0/CPU0:router(config-subscr-red)# group 1
RP/0/RSP0/CPU0:router(config-subscr-red-group)# peer 1.1.1.2
```

### Session Redundancy Group

This example shows how to configure a peer router for a session redundancy group (SERG) in BNG:

```
RP/0/RSP0/CPU0:router# configure
```
rp/0/rsp0/cpu0:router(config)# session redundancy
rp/0/rsp0/cpu0:router(config-session-red)# group 1
rp/0/rsp0/cpu0:router(config-session-red-group)# peer 1.1.1.2
preferred-role (BNG)

To configure the initial role preference as master or slave, in a BNG geo redundancy feature scenario, use the **preferred-role** command in subscriber redundancy group (SRG) or a session redundancy group (SERG). To configure the initial role for a specific group, use this command in the respective group configuration mode.

To remove the preferred role configuration, use the no prefix for this command.

```
preferred-role {master|slave}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>master</td>
<td>Specifies the preferred role as master.</td>
</tr>
<tr>
<td>slave</td>
<td>Specifies the preferred role as slave.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Subscriber redundancy

Subscriber redundancy group

Session redundancy

Session redundancy group

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.2</td>
<td>This command was introduced for SRG.</td>
</tr>
<tr>
<td>6.2.1</td>
<td>This command was introduced for SERG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This is an optional command.

**Task ID**

```
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>
```

**Subscriber Redundancy Group**

This example shows how to configure preferred role across all SRGs as master in BNG geo redundancy feature scenario:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# subscriber redundancy
RP/0/RSP0/CPU0:router(config-subscr-red)# preferred-role master
```

This example shows how to configure preferred role for a specific SRG as slave, in BNG geo redundancy feature scenario:
Session Redundancy Group

This example shows how to configure preferred role across all SERGs as master, in BNG geo redundancy feature scenario:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# session redundancy
RP/0/RSP0/CPU0:router(config-session-red)# preferred-role master
```

This example shows how to configure preferred role for a specific SERG as slave, in BNG geo redundancy feature scenario:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# session redundancy
RP/0/RSP0/CPU0:router(config-session-red)# group 1
RP/0/RSP0/CPU0:router(config-session-red-group)# preferred-role slave
```
**peer route-disable**

To disable the route on geo redundancy hot-standby peer, so that the subscriber routes are not installed in the RIB even when the subscriber sessions are brought up on the standby peer, use the **peer route-disable** command in subscriber redundancy group configuration mode. To disable this feature, use the **no** form of this command.

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

None

**Command Modes**

Subscriber redundancy group configuration.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to disable the route on geo redundancy hot-standby peer in BNG:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# subscriber redundancy group 110
RP/0/RSP0/CPU0:router(config-subscr-red-group)# peer route-disable
```
revertive-timer (BNG)

To set the auto-revertive timer in BNG to regain the master role after a failover, use the revertive-timer in subscriber redundancy or subscriber redundancy group configuration mode. To disable the timer, use the no form of this command.

```
revertive-timer  timer-value  maximum  max-value
```

**Syntax Description**

- **timer-value**: Specifies the timer value in minutes. The range is from 1 to 65535.
  
  This value is doubled every time access tracking goes down after the first instance of auto-revert to the master role. When the timer-value exceeds the max-value limit, it is reset to the originally configured value.

- **max-value**: Specifies the maximum value until which the timer-value doubles for each instance of access down.

**Command Default**

None

**Command Modes**

- Subscriber redundancy
- Subscriber redundancy group
- Session redundancy
- Session redundancy group

**Command History**

- **Release 6.1.2**: This command was introduced for SRG.
- **Release 6.2.1**: This command was introduced for SERG.

**Usage Guidelines**

The recommended value of max-value is 4 x timer-value.

If auto-revertive timer is configured at both subscriber redundancy level and at subscriber redundancy group level, the group level configuration takes precedence over the other.

Revertive-timer should not be running in a master node. If it does, it is an error condition.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Subscriber Redundancy Group**

This example shows how to set the auto-revertive timer in BNG to 20 minutes. In this example, if the access goes down again after the first switch back to master role, the timer runs for 40 minutes.
(that is, double the previous value). This repeats until it exceeds the max-value of 80 minutes. Once it exceeds 80 minutes, the timer value is reset to 20 minutes.

RP/0/RSP0/CPU0:router(config-subscr-red)#auto-revertive 20 max-value 80

**Session Redundancy Group**

This example shows how to set the auto-revertive timer in BNG to 20 minutes. In this example, if the access goes down again after the first switch back to master role, the timer runs for 40 minutes (that is, double the previous value). This repeats until it exceeds the max-value of 80 minutes. Once it exceeds 80 minutes, the timer value is reset to 20 minutes.

RP/0/RSP0/CPU0:router(config-session-red)#auto-revertive 20 max-value 80
source-interface (BNG)

To configure the interface whose IP address must be used for peering with other routers in BNG geo redundancy scenario, use the `source-interface` command in subscriber redundancy group (SRG) or session redundancy group (SERG) configuration mode.

To remove this configuration, use the `no` prefix for this command.

```
source-interface  interface-type  interface-name
```

**Syntax Description**

- `interface-type`: Type of the source interface.
- `interface-name`: Name of the source interface.

**Command Default**

None

**Command Modes**

- Subscriber redundancy group configuration.
- Session redundancy group configuration.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.2</td>
<td>This command was introduced for SRG.</td>
</tr>
<tr>
<td>6.2.1</td>
<td>This command was introduced for SERG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

It is recommended to use a loopback address that is advertised from the router for peer and the interface must have IPv4 or IPv6 (or both) global address depending on which one is to be used for peering.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Subscriber Redundancy Group**

This example shows how to configure source interface in subscriber redundancy sub-mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# subscriber redundancy
RP/0/RSP0/CPU0:router(config-subscr-red)# source-interface loopback0
```

**Session Redundancy Group**

This example shows how to configure source interface in session redundancy sub-mode:
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# session redundancy
RP/0/RSP0/CPU0:router(config-session-red)# source-interface loopback0
**session redundancy**

To enable session redundancy feature globally in BNG and to enter the session redundancy configuration submode, use the `session redundancy` command in Global Configuration mode. To remove the configurations for session redundancy feature in BNG, use the `no` form of this command.

```
Command redundancy
```

This command has no keywords or arguments.

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Global configuration.</td>
</tr>
<tr>
<td>Command History</td>
<td>Release</td>
</tr>
<tr>
<td></td>
<td>Release</td>
</tr>
<tr>
<td></td>
<td>6.2.1</td>
</tr>
<tr>
<td>Usage Guidelines</td>
<td>The option <code>slave-mode</code> is not supported in BNG geo redundancy. The default redundancy mode is hot-standby.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to enter session redundancy submode to configure session redundancy options:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# session redundancy
RP/0/RSP0/CPU0:router(config-session-red)#
```
To configure session redundancy group (SERG) in BNG, use the `session redundancy group` command in Global Configuration mode. To remove the session redundancy group configuration, use the `no` form of this command.

```
session redundancy group group-id [description line]
```

### Syntax Description
- **group-id**: Group identifier name that needs to be configured on the BNG pair routers.
- **description**: Specifies the description for the specific SERG.
- **line**: Description for the specific SERG, in words.

### Command Default
None

### Command Modes
Global configuration.

### Command History
```
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
```

### Usage Guidelines
For successful peering between the BNG pair routers, the same `group-id` must be configured on both the routers.

You can configure multiple groups (with unique IDs) for peering with the same peer router or across different peer routers.

The SERG does not get activated until the first access-interface is assigned under it.

### Task ID
- **Task ID**: `config-services`
- **Operation**: `read, write`

This example shows how to configure a session redundancy group (SERG) in BNG:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# session redundancy group 1
RP/0/RSP0/CPU0:router(config-session-red-group)#
```
session redundancy switchover

To execute session redundancy switchover in BNG, use the session redundancy switchover command in EXEC mode.

```
session redundancy switchover [{group group-num|location node-id}] [force]
```

**Syntax Description**

- `group` Specifies the session redundancy group (SERG) number to be switched over.
- `group-num` The SERG number. The range is from 1 to 999.
- `location` Specifies a particular location to be switched over.
- `force` Specifies a forced switchover.

**Command Default**

None

**Command Modes**

Exec.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The session redundancy activate command is currently not supported.

In most cases, the switchovers are triggered automatically by changes in the underlying access interfaces or due to other failures. This command is used for planned maintenance events or for exceptional cases where implementation of access-tracking is not possible or desired. It can be used to initiate switchover for all groups on the router, or on a particular location or for a specific SERG.

Switchover is triggered from the slave only when you choose the force option. The use of this option on either master or slave overrides any negotiation or arbitration rules.

Even for manual (or admin-triggered) switchovers, it is highly recommended to initiate triggers through operations on the underlying access, to ensure consistency between the BNG and access roles or status. When switchover happens, logs that indicate the reason of the switchover, are generated on the system console and reported on a per SERG basis on both peering routers. After the switchover, you must check the SERG details on both peering routers to ensure consistency and to ensure that session service is not interrupted.

You must ensure consistency between the roles of the underlying access interfaces (active-standby or up-down) and the BNG SERG role (master or slave). Failing this, the traffic may get disrupted especially when a proper access-tracking is not used.

To ensure network and service stability, it is recommended not to perform back to back switchovers (even though the feature allows it). After a reload, you must ensure sufficient stabilization time for any router or line card (LC) recovery and sync. Until then it must only be in slave or standby mode (through a hold-time or pre-empt mechanism in the underlying access). Depending on the integration aspects with RADIUS or PCRF, accounting updates may be sent from both master and slave after the switchover. Therefore, it is recommended to give sufficient time for these operations to complete and stabilize.
This example shows how to initiate session redundancy switchover for a particular SERG:

```
RP/0/RSP0/CPU0:router# session redundancy switchover group 210
```
session redundancy synchronize

To initiate or verify synchronization or consistency between sessions on the master and slave routers in a session redundancy scenario in BNG, use the `session redundancy synchronize` command in EXEC mode.

```
session redundancy synchronize [{group group-num|location node-id}]
```

**Syntax Description**

- `group` Specifies the session redundancy group (SERG) number to be synchronized.
  - `group-num` The SERG number.
    - The range is from 1 to 999.
- `location` Specifies a particular location to be synchronized.

**Command Default**

None

**Command Modes**

Exec.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Synchronization may be required in these scenarios:

- When errors are detected between master and slave due to transient resource constraints.
- To fix inconsistencies or errors when the BNG or the SERG configuration is changed on master or slave.
- Prior to performing a planned or admin-initiated maintenance activity.

You can initiate synchronization for all groups on the router, or on a particular location or for a specific SERG. This command can be issued on either master or slave (recommendation is to give on master first, and then on the slave only if it is still required).

Logs are generated on the router console to indicate the status of synchronization. However, it may take further time for any session inconsistency to be resolved and it must be verified using `show session session` command, or by checking the service status of the concerned session.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to initiate session redundancy synchronization for a particular SERG:

```
RP/0/RSP0/CPU0:router# session redundancy synchronize group 210
```
state-control-route

To control the route advertisement to the core network, based on the role of the subscriber redundancy group (SRG), use the `state-control-route` command in subscriber redundancy group configuration mode. To disable this feature, use the `no` form of this command.

```
state-control-route {ipv4 ipv4-address|ipv6 {iana|iapd} ipv6-address} [vrf vrf-name] [tag tag-value]
no state-control-route {ipv4 ipv4-address|ipv6 {iana|iapd} ipv6-address} [vrf vrf-name] [tag tag-value]
```

**Syntax Description**

- **tag tag-value** Specifies the option to filter out summary routes to be redistributed through the routing protocol, to get advertised to the core.
- **vrf vrf-name** Specifies the option to add summary route for a specific VRF, for a subscriber.

See Usage Guidelines section for more details.

**Command Default**

Disabled

**Command Modes**

Subscriber redundancy group

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>6.3.1</td>
<td>Added the support for <code>vrf</code> option, as part of the support for multiple state control route for each subscriber redundancy group (SRG).</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The route-policy with the respective tag (that is, tag 1 in this example) must be already defined, before configuring the `state-control-route` command.

The `vrf vrf-name` option helps to add state control routes in VRF routing table. If the `vrf` option is not specified, then the routes are added in the default VRF, that is, global routing table.

A maximum of 30 state control routes can be added in each subscriber redundancy group (SRG), with a limit of 10 state control routes for each route type. That is, user can have a maximum 10 IPv4 routes, 10 IANA routes and 10 IAPD routes in each SRG. In these 30 routes, user can have routes in either the default or the non-default VRF.

**Task ID**

```
Task ID   Operation
config-services read,
           write
```

This example shows how to filter out the summary routes to be advertised to the core:

```
RP/0/RSP0/CPU0:router(config-subscr-red-group)#state-control-route ipv4 192.0.2.0/9 tag 1
RP/0/RSP0/CPU0:router(config-subscr-red-group)#state-control-route ipv6 iana 2001:DB8::/32
```
This example shows how to add multiple summary routes for each SRG:

```
RP/0/RSP0/CPU0:router(config-subscr-red-group)#state-control-route ipv6 iapd 2001:DB8:1::1/32
tag 1
```

```
RP/0/RSP0/CPU0:router(config-subscr-red-group)#state-control-route ipv4 192.0.2.0/9 vrf vrf-name tag 1
```
subscriber arp scale-mode-enable

To prevent default ARP entry creations (mainly in deployment scenarios where the unnumbered subscriber access-interfaces inherit all the attributes, including the secondary IP addresses, from the associated loopback interface) per subscriber interface, use the **subscriber arp scale-mode-enable** command in Global Configuration mode. To disable this feature, use the **no** form of this command.

**subscriber arp scale-mode-enable**

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

None

**Command Modes**

Global Configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to prevent default ARP entry creations per subscriber interface in BNG:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# subscriber arp scale-mode-enable
```
### subscriber arp uncond-proxy-arp-enable

To enable unconditional proxy ARP responses in BNG so as to allow communication with static IP addresses, use the `subscriber arp uncond-proxy-arp-enable` command in Global Configuration mode. To disable unconditional proxy ARP responses in BNG, use the `no` form of this command.

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

None

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to enable unconditional proxy ARP responses in BNG:

```plaintext
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# subscriber arp uncond-proxy-arp-enable
```
**subscriber featurette dhcp-renew-author**

To enable AAA authorization during subscriber session lease renewal, use the **subscriber featurette dhcp-renew-author** command in Global Configuration mode. To disable this feature, use the **no** form of this command.

```
subscriber featurette dhcp-renew-author
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

None

**Command Modes**

Global Configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

```
Task ID  Operation
aaa      read, write
```

This example shows how to enable AAA authorization during DHCP renew or rebind event in BNG:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# subscriber featurette dhcp-renew-author
RP/0/RSP0/CPU0:router(config-subscriber)# commit
```
subscriber featurette identity-change

To enable identity change for DHCP Remote-Id parameter, thereby allowing modification of the subscriber service, use the `subscriber featurette identity-change` command in Global Configuration mode. To disable this feature, use the `no` form of this command.

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

None

**Command Modes**

Global Configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read,</td>
</tr>
<tr>
<td></td>
<td>write</td>
</tr>
</tbody>
</table>

This example shows how to enable identity change for DHCP Remote-Id parameter to allow modification of the subscriber service in BNG:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# subscriber featurette identity-change
```
subscriber redundancy

To enable subscriber redundancy feature globally in BNG and to enter the subscriber redundancy configuration sub mode, use the `subscriber redundancy` command in Global Configuration mode. To remove the configurations for subscriber redundancy feature in BNG, use the `no` form of this command.

```
subscriber redundancy
```

This command has no keywords or arguments.

### Command Default

None

### Command Modes

Global Configuration mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The option `slave-mode` is not supported in BNG geo redundancy. The default redundancy mode is hot-standby.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to enter subscriber redundancy sub mode to configure subscriber redundancy options:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# subscriber redundancy
RP/0/RSP0/CPU0:router(config-subscr-red)#
```
subscriber redundancy group

To configure subscriber redundancy group (SRG) in BNG, use the `subscriber redundancy group` command in Global Configuration mode. To remove the subscriber redundancy group configuration, use the `no` form of this command.

```
subscriber redundancy group group-id [description line]
```

**Syntax Description**
- `group-id` Group identifier name that needs to be configured on the BNG pair routers.
- `description` Specifies the description for the specific SRG.
- `line` Description for the specific SRG, in words.

**Command Default**
None

**Command Modes**
Global Configuration mode

**Command History**
- **Release** 5.2.2
  - This command was introduced.

**Usage Guidelines**
For successful peering between the BNG pair routers, the same `group-id` must be configured on both the routers.

You can configure multiple groups (with unique IDs) for peering with the same peer router or across different peer routers.

The SRG does not get activated until the first access-interface is assigned under it.

**Task ID**

```
Task ID     Operation
config-services  read,
               write
```

This example shows how to configure a subscriber redundancy group (SRG) in BNG:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# subscriber redundancy group 1
RP/0/RSP0/CPU0:router(config-subscr-red-group)#
```
subscriber redundancy switchover

To execute subscriber redundancy switchover in BNG, use the **subscriber redundancy switchover** command in EXEC mode.

```
subscriber redundancy switchover [{group group-num|location node-id}] [force]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>group</strong></td>
<td>Specifies the subscriber redundancy group (SRG) number to be switchover.</td>
</tr>
<tr>
<td><strong>group-num</strong></td>
<td>The SRG number. The range is from 1 to 999.</td>
</tr>
<tr>
<td><strong>location</strong></td>
<td>Specifies a particular location to be switchover.</td>
</tr>
<tr>
<td><strong>force</strong></td>
<td>Specifies a forced switchover.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **subscriber redundancy activate** command is currently not supported.

In most cases, the switchovers are triggered automatically by changes in the underlying access interfaces or due to other failures. This command is used for planned maintenance events or for exceptional cases where implementation of access-tracking is not possible or desired. It can be used to initiate switchover for all groups on the router, or on a particular location or for a specific SRG.

Switchover is triggered from the slave only when you choose the **force** option. The use of this option on either master or slave overrides any negotiation or arbitration rules.

Even for manual (or admin-triggered) switchovers, it is highly recommended to initiate triggers through operations on the underlying access, to ensure consistency between the BNG and access roles or status. When switchover happens, logs that indicate the reason of the switchover, are generated on the system console and reported on a per SRG basis on both peering routers. After the switchover, you must check the SRG details on both peering routers to ensure consistency and to ensure that subscriber service is not interrupted.

You must ensure consistency between the roles of the underlying access interfaces (active-standby or up-down) and the BNG SRG role (master or slave). Failing this, the traffic may get disrupted especially when a proper access-tracking is not used.

To ensure network and service stability, it is recommended not to perform back to back switchovers (even though the feature allows it). After a reload, you must ensure sufficient stabilization time for any router or line card (LC) recovery and sync. Until then it must only be in slave or standby mode (through a hold-time or pre-empt mechanism in the underlying access). Depending on the integration aspects with RADIUS or PCRF, accounting updates may be sent from both master and slave after the switchover. Therefore, it is recommended to give sufficient time for these operations to complete and stabilize.
This example shows how to initiate subscriber redundancy switchover for a particular SRG:

```
RP/0/RSP0/CPU0:router# subscriber redundancy switchover group 210
```
subscriber redundancy synchronize

To initiate or verify synchronization or consistency between sessions on the master and slave routers in a subscriber redundancy scenario in BNG, use the **subscriber redundancy synchronize** command in EXEC mode.

```
subscriber redundancy synchronize [{group group-num|location node-id}]
```

**Syntax Description**
- **group**
  - Specifies the subscriber redundancy group (SRG) number to be synchronized.
  - **group-num**
    - The SRG number.
    - The range is from 1 to 999.
- **location**
  - Specifies a particular location to be synchronized.

**Command Default**
None

**Command Modes**
EXEC mode

**Command History**
- **Release**
  - **Modification**
  - Release 5.2.2
    - This command was introduced.

**Usage Guidelines**
Synchronization may be required in these scenarios:

- When errors are detected between master and slave due to transient resource constraints.
- To fix inconsistencies or errors when the BNG or the SRG configuration is changed on master or slave.
- Prior to performing a planned or admin-initiated maintenance activity.

You can initiate synchronization for all groups on the router, or on a particular location or for a specific SRG. This command can be issued on either master or slave (recommendation is to give on master first, and then on the slave only if it is still required).

Logs are generated on the router console to indicate the status of synchronization. However, it may take further time for any session inconsistency to be resolved and it must be verified using **show subscriber session** command, or by checking the service status of the concerned subscriber.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>read,</td>
<td>write</td>
</tr>
</tbody>
</table>

This example shows how to initiate subscriber redundancy synchronization for a particular SRG:
subscriber redundancy synchronize

RP/0/RSP0/CPU0:router# subscriber redundancy synchronize group 210

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>subscriber redundancy switchover, on page 569</td>
<td>Executes subscriber redundancy switchover in BNG.</td>
</tr>
</tbody>
</table>
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.

```
session_limit  Limit for subscriber sessions.
               The range is from 1 to 200000.
```

Syntax Description

Command Default

None

Command Modes

Global Configuration mode

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.2.0</td>
<td>The <code>session_limit</code> was made an optional parameter for the <code>no</code> form of this command.</td>
</tr>
</tbody>
</table>

Usage Guidelines

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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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
```

This example shows how to remove the subscriber sessions limit configuration:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# no subscriber session limit
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show subscriber session, on page 608</td>
<td>Displays the subscriber management session information.</td>
</tr>
</tbody>
</table>
tracking-disable (BNG)

To disable the use of tracking objects status for automatic switchovers in BNG geo redundancy, use the `tracking-disable` command in subscriber redundancy group (SRG) or session redundancy group (SERG) configuration mode.

To re-enable the use of tracking objects status for automatic switchovers, use the `no` prefix for this command.

**tracking-disable**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>This command has no keywords or arguments.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Default</td>
<td>None</td>
</tr>
<tr>
<td>Command Modes</td>
<td>Subscriber redundancy group configuration.</td>
</tr>
<tr>
<td></td>
<td>Session redundancy group configuration.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.2</td>
<td>This command was introduced for SRG.</td>
</tr>
<tr>
<td>6.2.1</td>
<td>This command was introduced for SERG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This is an optional command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to temporarily disable the use of tracking objects status for automatic switchovers in BNG geo redundancy:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# subscriber redundancy
RP/0/RSP0/CPU0:router(config-subscr-red)# group 1
RP/0/RSP0/CPU0:router(config-subscr-red-group)# tracking-disable
```
virtual-mac

To configure the virtual MAC explicitly for a specific subscriber redundancy group (SRG), while BNG being in master redundancy mode, use the `virtual-mac` command in subscriber redundancy group configuration sub-mode. To remove this configuration, use the `no` form of this command.

```
virtual-mac virtual-mac
```

**Syntax Description**
- `virtual-mac` Virtual MAC address.

**Command Default**
None

**Command Modes**
Subscriber redundancy group configuration.

**Command History**
- **Release** 5.2.2
- **Modification** This command was introduced.

**Usage Guidelines**
The usage guidelines of this command remain the same as that for `virtual-mac-prefix` command.

**Task ID**
- **Operation** read, write

This example shows how to configure virtual MAC explicitly for an SRG in a subscriber redundancy feature scenario in BNG:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# subscriber redundancy
RP/0/RSP0/CPU0:router(config-subscr-red)# group 1
RP/0/RSP0/CPU0:router(config-subscr-red-gr)# virtual-mac 0001.0002.0001
```

**Related Commands**
- **Command** `virtual-mac-prefix, on page 577`
- **Description** Configures the gateway MAC (for the subscribers) used by BNG while being in master redundancy mode.
virtual-mac-disable

To disable the inheritance of the virtual MAC prefix for a specific subscriber redundancy group (SRG), use the `virtual-mac-prefix` command in subscriber redundancy group configuration mode. To re-enable the inheritance of the virtual MAC prefix, use the `no` form of this command.

**virtual-mac-disable**

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
None

**Command Modes**
Subscriber redundancy group configuration.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The virtual MAC configuration must be done before any subscriber session is set up because any change in this configuration affects the gateway MAC as seen by the CPE devices causing service disruption of existing sessions.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read,</td>
</tr>
<tr>
<td></td>
<td>write</td>
</tr>
</tbody>
</table>

This example shows how to disable the inheritance of the virtual MAC prefix for a specific subscriber redundancy group in BNG:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# subscriber redundancy
RP/0/RSP0/CPU0:router(config-subscr-red)# group 1
RP/0/RSP0/CPU0:router(config-subscr-red-group)# virtual-mac-disable
```
virtual-mac-prefix

To configure the gateway MAC (for the subscribers) used by BNG while being in master redundancy mode, use the `virtual-mac-prefix` command in subscriber redundancy configuration mode. To remove this configuration, use the `no` form of this command.

```
virtual-mac-prefix  virtual-mac
```

**Syntax Description**

| virtual-mac | Virtual mac prefix address. |

**Command Default**

None

**Command Modes**

Subscriber redundancy configuration.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The virtual MAC configuration must be done before any subscriber session is set up because any change in this configuration affects the gateway MAC as seen by the CPE devices causing service disruption of existing sessions.

The virtual MAC configuration is required for access protocols such as MST-AG, G.8032 and so on, where interface MAC is not same for the two peering routers.

The easiest way to provision virtual MAC is to select a locally-administered unicast MAC prefix (the last four digits must be zero (0)) and configure it on all redundant BNGs. This ensures that each subscriber redundancy group (SRG) gets its own vMAC, which is offset by the group ID, automatically.

The virtual MAC can alternatively be configured for a specific SRG by using `virtual-mac` command in subscriber redundancy group configuration sub-mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to configure virtual MAC prefix in a subscriber redundancy feature scenario in BNG:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# subscriber redundancy
RP/0/RSP0/CPU0:router(config-subscr-red)# virtual-mac-prefix 0001.0002.0000
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>virtual-mac, on page 575</td>
<td>Configures the virtual MAC explicitly for a specific subscriber redundancy group (SRG), while BNG being in master redundancy mode.</td>
</tr>
</tbody>
</table>
show sessionmon license

To display the subscriber session statistics required for BNG Smart Licensing, use the `show sessionmon license` command in the EXEC mode.

```
show sessionmon license [detail] statistics
```

**Syntax Description**

- `statistics` Displays the peak hour session statistics.
- `detail` (Optional) Displays the detailed session statistics that include current statistics along with the peak hour statistics.

**Command Default**

None

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

One license is required for every group of 8000 subscribers or a fraction of it. For example, two licenses are required for 9000 subscribers.

The license is consumed based on the peak count, and not on the current count.

**Task ID**

```
Task ID  Operation
network  read
```

This is a sample output of the `show sessionmon license statistics` command for non-Geo redundancy sessions. Here, two A9K-BNG-LIC-8K licenses are triggered for active sessions, as the session count is more than 8000.

```
Router# show sessionmon license statistics
Mon Mar 21 18:34:10.726 IST

Active  Standby
--------  -------
Peak (24 hours)  8001  0
```

This is a sample output of the `show sessionmon license detail statistics` command for non-Geo redundancy sessions. Here, one A9K-BNG-LIC-8K license is triggered for active sessions, as the session count is less than 8000.

```
Router# show sessionmon license detail statistics
Thu Jun 23 11:58:36.089 IST

Active  Standby
--------  -------
```
This is a sample output of the `show sessionmon license detail statistics` command for Geo redundancy sessions. Here, six A9K-BNG-LIC-8K licenses are triggered for active sessions and two A9K-BNG-ADV-8K licenses are triggered for standby sessions.

```text
Router#show sessionmon license detail statistics
Thu Jun 23 11:58:36.089 IST
nodename = node0_0_CPU0

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Number of active session on the router.</td>
</tr>
<tr>
<td>Standby</td>
<td>Number of standby session on the router.</td>
</tr>
<tr>
<td>Current</td>
<td>Current session count.</td>
</tr>
<tr>
<td>Peak (24 hours)</td>
<td>Peak number of session within a 24 hour time frame.</td>
</tr>
</tbody>
</table>
```

```text
nodename = node0_1_CPU0

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Number of active session on the router.</td>
</tr>
<tr>
<td>Standby</td>
<td>Number of standby session on the router.</td>
</tr>
<tr>
<td>Current</td>
<td>Current session count.</td>
</tr>
<tr>
<td>Peak (24 hours)</td>
<td>Peak number of session within a 24 hour time frame.</td>
</tr>
</tbody>
</table>
```

```text
nodename = node0_0_CPU0

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current</td>
<td>1000 0</td>
</tr>
<tr>
<td>Peak (24 hours)</td>
<td>1500 0</td>
</tr>
</tbody>
</table>
```
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|session
{state|subscriber-label | label}|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 mode

**Command History**

```
Release 4.2.0  This command was introduced.
Release 5.3.0  A new output field, Template Interface Id, was added to show subscriber database session
```

**Usage Guidelines**

If the *Template Interface Id* field displays a value of 0x00000000, it indicates that the subscriber is not using templates. If that field displays a non-zero value (for example, 0x00802c80), it indicates that the subscriber is using template with that particular interface-handle value.

**Task ID**

```
read
```

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 :
```

**Broadband Network Gateway Command Reference for Cisco ASR 9000 Series Routers**

580
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

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# 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_SESSIONDESTROYED = SUBDB_CB_EVENT_NONE
SUBDB_SPI_CB_SESSIONASSOCIATED = SUBDB_CB_EVENT_ALL
SUBDB_SPI_CB_SESSIONUNASSOCIATED = 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 = 0
BPI AIPC Information:

- 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

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'
```

This is a sample output of the `show subscriber database session subscriber-label` command, with subscriber templates enabled:

```
RP/0/RSP0/CPU0:router# show subscriber database session subscriber-label 0x42
Fri Nov 7 16:14:20.683 IST
```

```
Subscriber Object Information
------------------------------------------
Subscriber Label:    0x00000042
Session State:      CFG_DONE
Activate Request Identifier: 26
Transaction Identifier (PD or PAD): None
```
PD Request Identifier: 15
PD Request Options: 0x00000003
Config Changed Due to Template Change: FALSE
Destroy Request Received: NO
Destroy Request Identifier: 0
Creator of Connection Gone: FALSE
Number of Pending BPI Request Sent: 0
Current Apply Level for the Added/Modified Feature Tree: None
Current Apply Level for the Deleted Feature Tree: None
Delete Notification Done: TRUE
Add/Modify Notification Done: TRUE
Need to be rolled back: FALSE
Rollback in progress: FALSE
Server restart apply: FALSE
Rollback performed: FALSE
Replication pending: FALSE
Activate timer running: FALSE
Apply timer running: FALSE
Event queue size: 0
Restart Vector: 0x00000000
Template Interface Id: 0x00802c80

Add/Modify Level Tree (Number of Levels = 0):
----------------------------------------------

Delete Level Tree (Number of Levels = 0):
----------------------------------------------

show subscriber database
show subscriber database template

To display the template interface handle and template session information of a subscriber session, use the `show subscriber database template` command in the EXEC mode.

```
show subscriber database template [{parent-if-handle if-handle|parent-if-name interface-type interface-name}] [location node-id]
```

**Syntax Description**

- **parent-if-handle**: (Optional) Specifies parent interface handle.
- **if-handle**: Hex value of parent interface handle. The range is from 0 to ffffffff.
- **parent-if-name**: (Optional) Specifies the parent interface name.
- **interface-type**: Specifies the interface type.
- **interface-name**: (Optional) Display the node location by interface.
- **location**: (Optional) Displays the fully qualified location specification of an interface.
- **node-id**: Displays the fully qualified location specification of an interface.

**Command Default**

None

**Command Modes**

EXEC mode

**Command History**

```
Release 5.3.0
This command was introduced.
```

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

```
Task ID Operation
network read
```

This is a sample output of the `show subscriber database template` command:

```
RP/0/RSP0/CPU0:router# show subscriber database template

Location 0/RSP0/CPU0
---------------------------------------------
Interface Tmpl-Ifhandle Tmpl-Sub-Label Session Count
---------------------------------------------
Bundle-Ether121.104.tmlpl2 0x00000c60 0xfc000012 1
<<<<<< check here
Bundle-Ether121.104.tmlpl1 0x00000c20
Bundle-Ether121.104.tmlpl3 0x00000ca0
Bundle-Ether121.104.tmlpl4 0x00000ce0
Bundle-Ether121.104.tmlpl5 0x00000d20
Bundle-Ether121.104.tmlpl6 0x00000d60
Bundle-Ether121.104.tmlpl7 0x00000da0
```
This is a sample output of the `show subscriber database template parent-if-handle` command:

```
RP/0/RSP0/CPU0:router# show subscriber database template parent-if-handle 0x1d80
Fri Nov 7 15:41:02.982 IST
Location 0/1/CPU0
--------------------------------
Interface   Tmpl-Ifhandle   Tmpl-Sub-Label Session Count
-------------------------------- ------------- -------------- -------------
Bundle-Ether1.1.tmpl11 0x00802c80 0xfc000001 1
Bundle-Ether1.1.tmpl12 0x00802d80
Bundle-Ether1.1.tmpl13 0x00802e80
Bundle-Ether1.1.tmpl14 0x00802f80
Bundle-Ether1.1.tmpl15 0x00803080
```

This is a sample output of the `show subscriber database template parent-if-name` command:

```
RP/0/RSP0/CPU0:router# show subscriber database template parent-if-name Bundle-Ether1.1
Fri Nov 7 15:41:14.363 IST
Location 0/1/CPU0
--------------------------------
Interface             Tmpl-Ifhandle   Tmpl-Sub-Label Session Count
-------------------------------- ------------- -------------- -------------
Bundle-Ether1.1.tmpl11 0x00802c80 0xfc000001 1
Bundle-Ether1.1.tmpl12 0x00802d80
Bundle-Ether1.1.tmpl13 0x00802e80
Bundle-Ether1.1.tmpl14 0x00802f80
Bundle-Ether1.1.tmpl15 0x00803080
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show subscriber database, on page 580</code></td>
<td>Displays the configuration details of subscriber database.</td>
</tr>
<tr>
<td><code>show ipsubscriber template-interface, on page 328</code></td>
<td>Displays the template information for the IP subscriber interfaces.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ma</code></td>
<td>Displays the subscriber accounting feature management agent information.</td>
</tr>
<tr>
<td><code>statistics</code></td>
<td>Displays the accounting feature statistics.</td>
</tr>
<tr>
<td><code>debug</code></td>
<td>Displays the debug statistics.</td>
</tr>
<tr>
<td><code>location</code></td>
<td>Specifies the location of the node.</td>
</tr>
<tr>
<td><code>subscriber-label</code></td>
<td>Specifies the unique subscriber ID.</td>
</tr>
<tr>
<td><code>subscriber-id</code></td>
<td>ID of the subscriber, in hexadecimal.</td>
</tr>
<tr>
<td><code>summary</code></td>
<td>Displays the summary data.</td>
</tr>
<tr>
<td><code>trace</code></td>
<td>Displays the accounting feature ltrace data.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>Displays trace of all errors and events.</td>
</tr>
<tr>
<td><code>error</code></td>
<td>Displays trace of errors.</td>
</tr>
<tr>
<td><code>event</code></td>
<td>Displays trace of events.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.2.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 5.1</td>
<td>The show command output was extended to display session Idle Timeout feature information.</td>
</tr>
<tr>
<td>Release 5.3.0</td>
<td>The show command output was extended to display the prepaid feature information.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.
This is the sample output of the `show subscriber feature accounting` command in the EXEC mode:

```plaintext
RP/0/RSP0/CPU0:router# show subscriber feature accounting ma subscriber-label 0x40
Substrate Label: 0x40 Interface: Gi0/0/0.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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout value</td>
<td>Specifies the timeout value configured for that particular subscriber session.</td>
</tr>
<tr>
<td>Threshold value</td>
<td>Specifies the threshold value configured for that particular subscriber session, to decide on the duration of the session inactivity.</td>
</tr>
<tr>
<td>Timeout direction: both</td>
<td>Specifies that both the ingress and egress traffic is considered for the determination of the idle time for that particular subscriber session.</td>
</tr>
</tbody>
</table>

This is a sample output of the `show subscriber feature accounting` command, with the DIAMETER prepaid feature configured:

```plaintext
RP/0/RSP0/CPU0:router# show subscriber feature accounting ma subscriber-label 0x42
Substrate Label: 0x42 Interface: Gi0/0/0.pppoe3
Feature: Session Accounting Method-list: default
Feature: Service Accounting Service-ID: 0x4000004 Method-list: default Periodic interval: 6000
Flow Label: 0x4 Direction: Both Ingress and Egress Feature: Prepaid Prepaid-Config: foo4
FSM-Type FSM-State Threshold
-----------------------------------------------
Volume FSM NEW-QUOTA-ARRIVED 0
Time FSM NOT-ACTIVE 60
Quota-type : Input-Volume Output-Volume Bi-Directional-Volume
---------------------------------------------------------------
New-Arrived : 0 0 600
New-Used : 0 0 0
```
Total-arrived: 0 0 1200
Total-Used : 0 0 0
Pre-Tariff : 0 0 0
Post-Tariff : 0 0 0
num is a[0] is 0
num is a[1] is 0
num is a[2] is 57
num is a[3] is 1918
Waiting for Volume Quota update: 57 seconds.

<table>
<thead>
<tr>
<th>Time (in seconds):</th>
<th>Quota-Time</th>
<th>Validity-Time</th>
<th>Holding-Time</th>
<th>Tariff-Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>New-Arrived</td>
<td>0</td>
<td>2000</td>
<td>66</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>2000</td>
<td>66</td>
<td>0</td>
</tr>
<tr>
<td>Expiry in</td>
<td>0</td>
<td>1918</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>State</td>
<td>DISABLED</td>
<td>ENABLED</td>
<td>DISABLED</td>
<td>DISABLED</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show subscriber database, on page 580</td>
<td>Displays the configuration details of subscriber database.</td>
</tr>
<tr>
<td>show subscriber manager statistics, on page 592</td>
<td>Displays the subscriber management internal manager information.</td>
</tr>
<tr>
<td>show subscriber running-config, on page 606</td>
<td>Displays the subscriber running configuration derived from dynamic template.</td>
</tr>
<tr>
<td>show subscriber session, on page 608</td>
<td>Displays the subscriber management session information.</td>
</tr>
</tbody>
</table>
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 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 mode

**Command History**

- **Release**: 4.2.0
- **Modification**: This command was introduced.

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>read</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show subscriber session, on page 608</td>
<td>Displays the subscriber management session information.</td>
</tr>
<tr>
<td>ipsUBscriber interface, on page 311</td>
<td>Enables interface based static session in BNG.</td>
</tr>
</tbody>
</table>
show subscriber manager statistics

To display the subscriber management internal manager information, use the `show subscriber manager statistics` command in the EXEC mode mode.

```
show subscriber manager statistics {AAA COA|HA|PPSM|PRE|SVM|debug|performance|summary}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Displays the Authentication, Authorization, Accounting Coordinator statistics.</td>
</tr>
<tr>
<td>HA</td>
<td>Displays the High Availability statistics.</td>
</tr>
<tr>
<td>PPSM</td>
<td>Displays the Policy Plane Session Manager statistics.</td>
</tr>
<tr>
<td>PRE</td>
<td>Displays the Policy Rule Engine statistics.</td>
</tr>
<tr>
<td>SVM</td>
<td>Displays the Service Manager statistics.</td>
</tr>
<tr>
<td>debug</td>
<td>Displays the debug statistics.</td>
</tr>
<tr>
<td>performance</td>
<td>Displays the performance statistics.</td>
</tr>
<tr>
<td>summary</td>
<td>Displays the summary statistics.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.2.0</td>
<td>The output of <code>show subscriber manager statistics command was modified to track the statistics for singleton and multiple-service CoA requests separately for </code>show subscriber manager statistics AAA COA [ location &lt;&gt; ]<code>, to display the Multi-Service field for </code>show subscriber manager statistics AAA COA<code>, </code>show subscriber manager statistics PRE event<code>, and </code>show subscriber manager statistics PRE action total location &lt;&gt;<code>commands, and to display MA-CoA RB Success and MA-CoA RB Failure fields for</code>show subscriber manager statistics SVM events location &lt;&gt;` command.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

```
Task ID Operation
    network  read
```

This is the sample output of the `show subscriber manager statistics` command in the EXEC mode mode:
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 29: show subscriber manager statistics Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Policy errors</td>
<td>Specifies the errors in the control policy.</td>
</tr>
<tr>
<td>Attribute format warnings</td>
<td>Specifies the attribute format warnings.</td>
</tr>
<tr>
<td>User Profile Statistics</td>
<td>Specifies the user profile statistics.</td>
</tr>
<tr>
<td>Session Disconnect Flow Control</td>
<td>Specifies the session disconnect flow control.</td>
</tr>
</tbody>
</table>

These are the sample outputs for the `show subscriber manager statistics` command with multi-action CoA enabled, in EXEC mode mode:

```
RP/0/0/CPU0server:# show subscriber manager statistics AAA COA

Wed Jun 27 10:08:37.331 EDT

{ CHANGE OF AUTHORIZATION STATISTICS }

Location: 0/0/CPU0

CoA Requests:

<table>
<thead>
<tr>
<th>Type</th>
<th>Received</th>
<th>Acked</th>
<th>NAKed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Logon</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Account Logoff</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Account Update</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Disconnect</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Single Service Logon</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Single Service Logoff</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Multiple Service</td>
<td>10</td>
<td>10</td>
<td>0</td>
</tr>
</tbody>
</table>

Errors:
None

RP/0/0/CPU0:server#
```

In the above show output, see the **Multiple Service** row to fetch information on how many MA-CoA requests were issued, the number of MA-CoA requests acknowledged, and the number of MA-CoA requests that were not acknowledged.

```
RP/0/0/CPU0server:# show subscriber manager statistics PRE event

Wed Jun 27 11:00:27.029 EDT

{ EVENT STATISTICS }

Location: 0/0/CPU0

Events executed
------------------------
3                       2     1     0

Detail Statistics
------------------------
<table>
<thead>
<tr>
<th>Type</th>
<th>Total</th>
<th>Success</th>
<th>Fail</th>
<th>Pending</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>------</td>
<td>---------</td>
<td>------</td>
<td>---------</td>
</tr>
</tbody>
</table>
```

---

Broadband Network Gateway Command Reference for Cisco ASR 9000 Series Routers
In the above show output, see the Multi-Service and Exception rows to fetch debug information related to MA-CoA requests.
<table>
<thead>
<tr>
<th>Type</th>
<th>Total</th>
<th>Success</th>
<th>Fail</th>
<th>Pending</th>
</tr>
</thead>
<tbody>
<tr>
<td>authenticate</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>unauthenticate</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>authorize</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>accounting start</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>accounting stop</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>accounting update</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>set-timer</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>stop-timer</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>disconnect</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>collect</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>quota-replenish</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>prepaid</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>proxy</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>activate</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>deactivate</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>multi-service</td>
<td>5</td>
<td>5</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>inline policy</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>session-update</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>session-up</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>session-down</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>session-idle</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>apply user profile</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>query ANCP</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>monitor</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

In the above show output, see the **multi-service** row to fetch debug information related to MA-CoA requests.

```
RP/0/RSP0/CPU0:server# show subscriber manager statistics SVM events location 0/RSP0/CPU0
[14:09:23.571 UTC Thu Feb 13 2014] +++

[ IEDGE SVM EVENT STATISTICS ]

Location:

**SVM INTERNAL EVENT COUNTERS (125):**

<table>
<thead>
<tr>
<th>EVT</th>
<th>COUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sess Create invocations</td>
<td>0</td>
</tr>
<tr>
<td>Sess Create (bad client)</td>
<td>0</td>
</tr>
<tr>
<td>Sess Create (DUP)</td>
<td>0</td>
</tr>
<tr>
<td>Sess Create (BAD)</td>
<td>0</td>
</tr>
<tr>
<td>Sess Create (ASYNC)</td>
<td>0</td>
</tr>
<tr>
<td>Sess Create (BAD STATE)</td>
<td>0</td>
</tr>
<tr>
<td>SVMB (uB) Creates</td>
<td>1</td>
</tr>
<tr>
<td>SVMB (uB) Removes</td>
<td>0</td>
</tr>
<tr>
<td>SVMS (SB) Creates</td>
<td>14</td>
</tr>
<tr>
<td>SVMS (SB) Removes</td>
<td>10</td>
</tr>
<tr>
<td>SVMA (AS) Creates</td>
<td>14</td>
</tr>
<tr>
<td>SVMA (AS) Removes</td>
<td>0</td>
</tr>
<tr>
<td>SVM KEY Creates/Dups</td>
<td>43</td>
</tr>
<tr>
<td>SVM KEY Removes</td>
<td>25</td>
</tr>
<tr>
<td>Apply invocations</td>
<td>0</td>
</tr>
<tr>
<td>Apply (bad argument)</td>
<td>0</td>
</tr>
<tr>
<td>Apply (no memory)</td>
<td>0</td>
</tr>
<tr>
<td>Apply (missing create)</td>
<td>0</td>
</tr>
<tr>
<td>Apply (create error)</td>
<td>0</td>
</tr>
<tr>
<td>Apply (assoc error)</td>
<td>0</td>
</tr>
<tr>
<td>Apply (call back)</td>
<td>34</td>
</tr>
<tr>
<td>Apply (call back error)</td>
<td>0</td>
</tr>
<tr>
<td>Apply (successful)</td>
<td>24</td>
</tr>
<tr>
<td>Unapply invocations</td>
<td>0</td>
</tr>
</tbody>
</table>
```
In the above show output, see the **MA-CoA RB Success** and **MA-CoA RB Failure** rows to fetch debug information related to MA-CoA rollback success and failures.

```
RP/0/0/CPU0:# show subscriber manager statistics perf non-zero
Tue Jun 3 13:14:34.547 IST
[ IEDGE PERFORMANCE DATA ]

<table>
<thead>
<tr>
<th>Type</th>
<th>Ave(ms)</th>
<th>StdDev(ms)</th>
<th>Min(ms)</th>
<th>Max(ms)</th>
<th>Count</th>
</tr>
</thead>
</table>

RP/0/0/CPU0:# show subscriber manager statistics performance
Tue Jun 3 13:14:34.547 IST
[ IEDGE PERFORMANCE DATA ]

<table>
<thead>
<tr>
<th>Type</th>
<th>Ave(ms)</th>
<th>StdDev(ms)</th>
<th>Min(ms)</th>
<th>Max(ms)</th>
</tr>
</thead>
</table>

Transactions:
```
<table>
<thead>
<tr>
<th>Event</th>
<th>Time (in milliseconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Absolute-timeout request</td>
<td>0.0</td>
</tr>
<tr>
<td>Account logon event</td>
<td>0.0</td>
</tr>
<tr>
<td>Account logoff event</td>
<td>0.0</td>
</tr>
<tr>
<td>Account update event</td>
<td>0.0</td>
</tr>
<tr>
<td>Accounting request</td>
<td>0.0</td>
</tr>
<tr>
<td>Authentication continue</td>
<td>0.0</td>
</tr>
<tr>
<td>Session Activate request</td>
<td>0.0</td>
</tr>
<tr>
<td>Bind request</td>
<td>0.0</td>
</tr>
<tr>
<td>Flow disconnect ack</td>
<td>0.0</td>
</tr>
<tr>
<td>Flow disconnect event</td>
<td>0.0</td>
</tr>
<tr>
<td>Flow disconnect request</td>
<td>0.0</td>
</tr>
<tr>
<td>Flow start request</td>
<td>0.0</td>
</tr>
<tr>
<td>Idle Timeout request</td>
<td>0.0</td>
</tr>
<tr>
<td>Identity release request</td>
<td>0.0</td>
</tr>
<tr>
<td>Session update request</td>
<td>0.0</td>
</tr>
<tr>
<td>Keepalive status request</td>
<td>0.0</td>
</tr>
<tr>
<td>Link status request</td>
<td>0.0</td>
</tr>
<tr>
<td>Prepaid request</td>
<td>0.0</td>
</tr>
<tr>
<td>Service start event</td>
<td>0.0</td>
</tr>
<tr>
<td>Service stop event</td>
<td>0.0</td>
</tr>
<tr>
<td>Session disconnect ack</td>
<td>0.0</td>
</tr>
<tr>
<td>Session disconnect event</td>
<td>0.0</td>
</tr>
<tr>
<td>Session disconnect request</td>
<td>0.0</td>
</tr>
<tr>
<td>Session kill event</td>
<td>0.0</td>
</tr>
<tr>
<td>Session start request</td>
<td>0.0</td>
</tr>
<tr>
<td>Timer expiry event</td>
<td>0.0</td>
</tr>
<tr>
<td>Session deactivate request</td>
<td>0.0</td>
</tr>
<tr>
<td>Passthru Accounting request</td>
<td>0.0</td>
</tr>
<tr>
<td>Author no response event</td>
<td>0.0</td>
</tr>
<tr>
<td>Author failed event</td>
<td>0.0</td>
</tr>
<tr>
<td>Authen no response event</td>
<td>0.0</td>
</tr>
<tr>
<td>Authen failed event</td>
<td>0.0</td>
</tr>
<tr>
<td>Session Up and Update request</td>
<td>0.0</td>
</tr>
<tr>
<td>Session Down request</td>
<td>0.0</td>
</tr>
<tr>
<td>Session State AF Register</td>
<td>0.0</td>
</tr>
<tr>
<td>Session info update</td>
<td>0.0</td>
</tr>
<tr>
<td>Mobility Failure event</td>
<td>0.0</td>
</tr>
<tr>
<td>Session disconnect queuing</td>
<td>0.0</td>
</tr>
</tbody>
</table>
show subscriber redundancy group

To display the operational summary (including the active subscriber sessions under each subscriber redundancy group (SRG) and the transient sessions awaiting synchronization to the peer) of all the configured SRGs, use the `show subscriber redundancy group` command in the EXEC mode mode.

```
show subscriber redundancy group [group-id [{session|tunnel}]] [location node-id]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group</td>
<td>Displays the summary information of all SRGs.</td>
</tr>
<tr>
<td>group-id</td>
<td>Displays the detailed information of a specific SRG.</td>
</tr>
<tr>
<td>session</td>
<td>Displays the key information about the sessions active under the SRG.</td>
</tr>
<tr>
<td>tunnel</td>
<td>Displays the tunnel information specific to each SRG group.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.3.2</td>
<td>This command was modified to add the new keyword, tunnel.</td>
</tr>
<tr>
<td>Release 5.2.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The details listed under the `show subscriber redundancy group` command for a specific SRG include:

- Various applied operational parameters.
- Details of tracking objects registered on the SRG and their status. This shows if it is configured or not, if it is set in the SRG but unknown because the tracking object is not configured and shows the current status of object as reported.
- Details about the peer that include the status of connection and info (for example, its tracking status and roles) that it provided to this router in the previous negotiation, the timestamp of last negotiation and the time when the peer went up or down.
- Details about switchover that include the last role change along with the reason, number of switchovers and information regarding hold-timer (whether the timer is currently running and if running, the remaining time).
- The active subscriber session statistics and any pending updates or deletions to be sent to the peer.
- The session entries that experienced failures in synchronization with the peer. Generally, this may be seen on the slave where provisioning failed due to configuration mismatch or due to some other resource constraints.
- The number and list of active access sub-interfaces under the SRG.
The retry mechanisms of the subscriber redundancy feature take care of recovery from transient errors. Also, logs with more details on the specific errors are generated for persistent synchronization errors.

This is a sample output of the `show subscriber redundancy group` command:

```
RP/0/RSP0/CPU0:router#show subscriber redundancy group

Subscriber Redundancy Agent Group Summary
Flags : E - Enabled, D - Disabled, M - Preferred Master, S - Preferred Slave
       H - Hot Mode, W - Warm Mode, T - Object Tracking Enabled
P/S  : Peer Status
       I - Initialize, Y - Retry, X - Cleanup, T - Connecting
       L - Listening, R - Registered, C - Connected, E - Established
I/F Count: Interface Count
SS Count : Subscriber Session Count
-----------------------------------------------------------------------------------------
| Node Name | Group ID | Role | Flags | Peer Address | P/S | I/F Count | SS Count | Sync Pending |
-----------------------------------------------------------------------------------------
| 0/RSP0/CPU0 210 Master EMHT 11:2 E 1 8000 0 |
| 0/RSP0/CPU0 410 Slave EMHT 1.1.1.2 E 1 8000 0 |

Session Summary Count(Master/Slave/Total): 8000/8000/16000
```

This table describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initialize</td>
<td>Initial state when some configuration is incomplete or SRG is disabled.</td>
</tr>
<tr>
<td>Connecting or Listening or Registering</td>
<td>During the process of TCP connection establishment between client and server.</td>
</tr>
<tr>
<td>Connected or Established</td>
<td>TCP connection is done and moves to steady state after role negotiation.</td>
</tr>
<tr>
<td>Retry or Cleanup</td>
<td>Transient error conditions.</td>
</tr>
</tbody>
</table>

This is a sample output of the `show subscriber redundancy group` command that displays the key information about the sessions active under the SRG:

```
RP/0/RSP0/CPU0:router#show subscriber redundancy group 210

Subscriber Redundancy Group ID: 210
  Description : <<not-configured>>
  Status       : Enabled
  Init-Role    : Master
```
Negotiated-Role : Master       Current-Role : Master
Slave-mode : Not       Hold Time : 15
Virtual MAC Address : 0000.0000.2020
L2TP Source Address : <<not-configured>>
Core-Tracking : <<not-configured>>
Status : n/a
Access-Tracking : vlan210
Status : Up
Tracking Status : Enabled

Peer:
11::2       Status : Established
Role(Init/Neg/Cur): Slave/Slave/Slave
Tracking Status : Down

Last Neg-Time : 2014 Sep 12 07:12:11
Last Down-Time : 2014 Sep 11 14:26:45

Switchover:
Last Switchover : 2014 Sep 12 07:12:11       Reason : Object Tracking Status Change
Switchover Count : 4
Hold Time : Not-Running

Subscriber Session Statistics:
Count : 8000       Slave-Upd-Fail : 0
Pending Update : 0       Pending Delete : 0
Tunnel Count : 0

Interface Count : 1
Bundle-Ether1.10       Map-ID : 210

This table describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Init-role</td>
<td>Specifies if master-slave preference is set.</td>
</tr>
<tr>
<td>Negotiated-role</td>
<td>Specifies the desired role during previous and next role negotiation exchange.</td>
</tr>
<tr>
<td>Current-role</td>
<td>Specifies the current role assumed.</td>
</tr>
</tbody>
</table>

This is a sample output of the show subscriber redundancy group session command:

RP/0/RSP0/CPU0:router# show subscriber redundancy group 210 session

Subscriber Redundancy Agent Group Session
------------------------------------------------------------------
Parent Interface | MAC Address | In/Out VLAN | PPPoE/L2TP ID |
------------------------------------------------------------------
Bundle-Ether1.10 | 0000.680b.0102 | 0/210 | 0/0 |
Bundle-Ether1.10 | 0000.680b.0103 | 0/210 | 0/0 |
Bundle-Ether1.10 | 0000.680b.0104 | 0/210 | 0/0 |
Bundle-Ether1.10 | 0000.680b.0105 | 0/210 | 0/0 |
Bundle-Ether1.10 | 0000.680b.0106 | 0/210 | 0/0 |
Bundle-Ether1.10 | 0000.680b.0107 | 0/210 | 0/0 |
This is a sample output of the show subscriber redundancy group command that displays the tunnel information:

```
RP/0/RSP0/CPU0:router show subscriber redundancy group 1 tunnel

Subscriber Redundancy Agent Group Tunnel
Operational: SA-SRGA, L2-L2TP
    Flags: U-Update, D-Delete, S-InSync, F-TxListFail, T-Dirty

-------------------------------------
<table>
<thead>
<tr>
<th>L2TP TID</th>
<th>Operational Flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>4557</td>
<td>M-- SA(S) L2(S)</td>
</tr>
</tbody>
</table>
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show subscriber redundancy summary, on page 604</td>
<td>Displays the global status of BNG geo redundancy feature.</td>
</tr>
</tbody>
</table>
**show subscriber redundancy summary**

To display the global status of BNG geo redundancy feature, use the `show subscriber redundancy summary` command in the EXEC mode mode.

```
show subscriber redundancy summary [{group|interface}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group</td>
<td>Displays the subscriber redundancy summary of all configured SRGs.</td>
</tr>
<tr>
<td>interface</td>
<td>Displays the subscriber redundancy summary of all access sub-interfaces configured under SRGs.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The details listed under this output of this command include, the IPv4 and IPv6 addresses from the source-interface that is used for peering by this router, and the snapshot of the active subscriber redundancy groups, interfaces and their roles.

The details listed under `show subscriber redundancy summary group` output also include the attributes or settings of the SRGs in operation and their roles. The output also indicates the RP or LC where the control plane for the SRG is being hosted for troubleshooting purposes.

The details listed under `show subscriber redundancy summary interface` output also include the mapping group, ID and role of the SRGs.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>read</td>
</tr>
</tbody>
</table>

This is a sample output of the `show subscriber redundancy summary` command:

```
RP/0/RSP0/CPU0:router#show subscriber redundancy summary
Subscriber Redundancy Summary
  Status : Enabled          Process State: Active
  Preferred-Role: None      Hold Time  : 0
  Slave-Mode : <<not-configured>>
Source Interface: GigabitEthernet0/1/0/1
  VRF Name   : default
  IPv4 Address: 1.1.1.1
  IPv6 Address: 11::1
Group Statistics:
```
This is a sample output of the `show subscriber redundancy summary group` command:

```
RP/0/RSP0/CPU0:router#show subscriber redundancy summary group
Subscriber Redundancy Group Summary
Options: E - Enabled, D - Disabled
        M - Preferred Master, S - Preferred Slave
        H - Hot Mode, W - Warm Mode
        T - Object Tracking Enabled
-------------------------------------------------------------
ID | Role | Virtual MAC Addr | Peer Address | I/F Count | Options | Node
-------------------------------------------------------------
210 Master 0001.0002.00D2 11::2 2 EM-T 0/RSP0/CPU0
211 Master 0001.0002.00D3 11::2 1 EM-T 0/RSP0/CPU0
212 Master 0001.0002.00D4 11::2 1 EM-T 0/RSP0/CPU0
213 Master 0001.0002.00D5 11::2 1 EM-T 0/RSP0/CPU0
214 Master 0001.0002.00D6 11::2 1 EM-T 0/RSP0/CPU0
410 Slave 0001.0002.019A 1.1.1.2 2 EM-T 0/RSP0/CPU0
411 Slave 0001.0002.019B 1.1.1.2 1 EM-T 0/RSP0/CPU0
412 Slave 0001.0002.019C 1.1.1.2 1 EM-T 0/RSP0/CPU0
413 Slave 0001.0002.019D 1.1.1.2 1 EM-T 0/RSP0/CPU0
414 Slave 0001.0002.019E 1.1.1.2 1 EM-T 0/RSP0/CPU0
```

This is a sample output of the `show subscriber redundancy interface` command:

```
RP/0/RSP0/CPU0:router#show subscriber redundancy interface
Subscriber Redundancy Interface Summary
Status: E - Exists, F - Forward Reference
-----------------------------------------------------------
Interface Name | Status | Group ID | Map ID | Role
-----------------------------------------------------------
Bundle-Ether1.1 E 210 210 Master
Bundle-Ether1.10 E 210 210 Master
Bundle-Ether1.11 E 211 211 Master
Bundle-Ether1.12 E 212 212 Master
Bundle-Ether1.13 E 213 213 Master
Bundle-Ether1.14 E 214 214 Master
Bundle-Ether3.1 E 410 410 Slave
Bundle-Ether3.10 E 410 410 Slave
Bundle-Ether3.11 E 411 411 Slave
Bundle-Ether3.12 E 412 412 Slave
Bundle-Ether3.13 E 413 413 Slave
Bundle-Ether3.14 E 414 414 Slave
```
show subscriber running-config

To display the subscriber running configuration derived from dynamic template, use the `show subscriber running-config` command in EXEC mode.

```
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 mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>read</td>
</tr>
</tbody>
</table>

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 mode.

`show subscriber session {all [{detail|summary|username}] internal[location node-id][debug|filter|subscriber-label] session-id}`

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays all subscriber sessions.</td>
</tr>
<tr>
<td>debug</td>
<td>Displays unique subscriber session selected for debugging.</td>
</tr>
<tr>
<td>filter</td>
<td>Displays the search results of the subscriber session database based on the filter criteria.</td>
</tr>
<tr>
<td>subscriber-label</td>
<td>Displays the unique ID of the subscriber session.</td>
</tr>
<tr>
<td>session-id</td>
<td>Hex value of subscriber session ID. The range is from 0 to ffffffff.</td>
</tr>
</tbody>
</table>

Command Default: None

Command Modes: EXEC mode

Command History:
- 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.
- Release 5.2.0: The output of `show subscriber session all username` command was modified to display the fields, **Username**, **Interface**, **State** and **Subscriber IP Addr**, instead of **Type**, **Interface**, **State** and **Username**.

Usage Guidelines: For interface-based static sessions in the BNG, the value of **Type** field in the `show ips subscriber session` command output is displayed as **IP: Static**.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>read</td>
</tr>
<tr>
<td>config-services</td>
<td>read</td>
</tr>
</tbody>
</table>

These are some of the options for the `show subscriber session` command in the EXEC mode:

```
RP/0/RSP0/CPU0:router# show subscriber session all
```
This is the sample output of the `show subscriber session all` command:

```
Wed Jan 23 10:20:58.344 GMT
Codes: IN - Initialize, CN - Connecting, CD - Connected, AC - Activated,
ID - Idle, DN - Disconnecting, ED - End

<table>
<thead>
<tr>
<th>Type</th>
<th>Interface</th>
<th>State</th>
<th>Subscriber IP Addr / Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPPoE:PTA</td>
<td>Gi0/1/0/0.pppoe1</td>
<td>AC</td>
<td>100.0.0.1 (default)</td>
</tr>
<tr>
<td>PPPoE:PTA</td>
<td>Gi0/1/0/0.pppoe2</td>
<td>AC</td>
<td>100.0.0.1 (default)</td>
</tr>
<tr>
<td>PPPoE:PTA</td>
<td>Gi0/1/0/0.pppoe3</td>
<td>AC</td>
<td>100.0.0.1 (default)</td>
</tr>
<tr>
<td>PPPoE:PTA</td>
<td>Gi0/1/0/0.1.pppoe1</td>
<td>AC</td>
<td>100.0.0.1 (default)</td>
</tr>
<tr>
<td>PPPoE:PTA</td>
<td>Gi0/1/0/0.1.pppoe2</td>
<td>AC</td>
<td>100.0.0.1 (default)</td>
</tr>
<tr>
<td>PPPoE:PTA</td>
<td>Gi0/1/0/0.1.pppoe3</td>
<td>AC</td>
<td>100.0.0.1 (default)</td>
</tr>
<tr>
<td>PPPoE:PTA</td>
<td>Gi0/1/0/0.2.pppoe1</td>
<td>AC</td>
<td>100.0.0.1 (default)</td>
</tr>
<tr>
<td>PPPoE:PTA</td>
<td>Gi0/1/0/0.2.pppoe2</td>
<td>AC</td>
<td>100.0.0.1 (default)</td>
</tr>
<tr>
<td>PPPoE:PTA</td>
<td>Gi0/1/0/0.2.pppoe3</td>
<td>AC</td>
<td>100.0.0.1 (default)</td>
</tr>
<tr>
<td>PPPoE:PTA</td>
<td>Gi0/1/0/0.3.pppoe1</td>
<td>AC</td>
<td>100.0.0.1 (default)</td>
</tr>
<tr>
<td>PPPoE:PTA</td>
<td>Gi0/1/0/0.3.pppoe2</td>
<td>AC</td>
<td>100.0.0.1 (default)</td>
</tr>
<tr>
<td>PPPoE:PTA</td>
<td>Gi0/1/0/0.3.pppoe3</td>
<td>AC</td>
<td>100.0.0.1 (default)</td>
</tr>
<tr>
<td>PPPoE:PTA</td>
<td>Gi0/1/0/0.3.pppoe4</td>
<td>AC</td>
<td>100.0.0.1 (default)</td>
</tr>
<tr>
<td>PPPoE:PTA</td>
<td>Gi0/1/0/0.3.pppoe5</td>
<td>AC</td>
<td>100.0.0.1 (default)</td>
</tr>
<tr>
<td>PPPoE:PTA</td>
<td>Gi0/1/0/0.3.pppoe6</td>
<td>AC</td>
<td>100.0.0.1 (default)</td>
</tr>
<tr>
<td>PPPoE:PTA</td>
<td>Gi0/1/0/0.3.pppoe7</td>
<td>AC</td>
<td>100.0.0.1 (default)</td>
</tr>
<tr>
<td>PPPoE:PTA</td>
<td>Gi0/1/0/0.3.pppoe8</td>
<td>AC</td>
<td>100.0.0.1 (default)</td>
</tr>
<tr>
<td>PPPoE:PTA</td>
<td>Gi0/1/0/0.3.pppoe9</td>
<td>AC</td>
<td>100.0.0.1 (default)</td>
</tr>
<tr>
<td>PPPoE:PTA</td>
<td>Gi0/1/0/0.3.pppoe10</td>
<td>AC</td>
<td>100.0.0.1 (default)</td>
</tr>
<tr>
<td>PPPoE:PTA</td>
<td>Gi0/1/0/0.3.pppoe11</td>
<td>AC</td>
<td>100.0.0.1 (default)</td>
</tr>
<tr>
<td>PPPoE:PTA</td>
<td>Gi0/1/0/0.3.pppoe12</td>
<td>AC</td>
<td>100.0.0.1 (default)</td>
</tr>
<tr>
<td>PPPoE:PTA</td>
<td>Gi0/1/0/0.3.pppoe13</td>
<td>AC</td>
<td>100.0.0.1 (default)</td>
</tr>
<tr>
<td>PPPoE:PTA</td>
<td>Gi0/1/0/0.3.pppoe14</td>
<td>AC</td>
<td>100.0.0.1 (default)</td>
</tr>
</tbody>
</table>
```

Broadband Network Gateway Command Reference for Cisco ASR 9000 Series Routers
This table describes the significant fields shown in the display.

### **Table 30: show subscriber session Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Specifies the subscriber session type.</td>
</tr>
<tr>
<td>Interface</td>
<td>Specifies the interface type.</td>
</tr>
<tr>
<td>State</td>
<td>Specifies the states of the subscriber session such as initiate, connecting, connecting, activated, disconnected, idle, end.</td>
</tr>
<tr>
<td>Subscriber IP Addr / Prefix LNS Address (Vrf)</td>
<td>Specifies the IP address of the subscriber interface.</td>
</tr>
</tbody>
</table>

This is the sample output for the `show subscriber session` command in EXEC mode:

```
RP/0/0/CPU0:server#show subscriber session all detail internal location$
[14:09:18.244 UTC Thu Mar21 13 2019] +++
Interface: Bundle-Ether2.111.ip1
Circuit ID: Unknown
Remote ID: Unknown
Type: IP: DHCP-trigger
IPv4 State: Up, Thu Mar 21 17:26:42 2019
IPv4 Address: 95.1.10.133, VRF: vrf1
IPv4 Up helpers: 0x00000040 {IPSUB}
IPv4 Up requestors: 0x00000040 {IPSUB}
Mac Address: 0000.0201.8d8f
Account-Session Id: 00000001
Nas-Port: Unknown
User name: 0000.0201.8d8f
Formatted User name: unknown
Client User name: unknown
Outer VLAN ID: 11
Inner VLAN ID: 10
Subscriber Label: 0x00000040
```
In the following table, the descriptions for different SRG flags is provided:

<table>
<thead>
<tr>
<th>SRG Flags</th>
<th>SRG Flag Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEDGE_SRG_FLAG_NONE</td>
<td>0x000000000</td>
<td>SRG function is not supported.</td>
</tr>
<tr>
<td>IEDGE_SRG_MASTER_DEL_PENDING</td>
<td>0x000000001</td>
<td>Deletion is pending for SRG Master Subscriber.</td>
</tr>
</tbody>
</table>
### SRG Flags

<table>
<thead>
<tr>
<th>SRG Flags</th>
<th>SRG Flag Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>EDGE_SRG_MASTER_EOMS_INTF_PENDING</code></td>
<td>0x00000002</td>
<td>EOMS is pending.</td>
</tr>
<tr>
<td><code>EDGE_SRG_MASTER_EOMS_INTF_RECEIVED</code></td>
<td>0x00000004</td>
<td>EOMS is received.</td>
</tr>
<tr>
<td><code>EDGE_SRG_MASTER_EOMS_DEL_PENDING</code></td>
<td>0x00000008</td>
<td>EOMS is pending because there is delayed delete send for the session.</td>
</tr>
<tr>
<td><code>EDGE_SRG_SENT_TO_TXLIST</code></td>
<td>0x00000010</td>
<td>Session is sent over txlist successfully.</td>
</tr>
<tr>
<td><code>EDGE_SRG_DONT_SEND_TO_TXLIST</code></td>
<td>0x00000020</td>
<td>Don't send this session over txlist.</td>
</tr>
<tr>
<td><code>EDGE_SRG_ENCODE_DONE_IN_TXLIST</code></td>
<td>0x00000040</td>
<td>Encode callback is completed for this session in txlist.</td>
</tr>
<tr>
<td><code>EDGE_SRG_SKIP_INTF_ROLE_CHECK</code></td>
<td>0x00000080</td>
<td>Skip INTF-ROLE-CHECK to push data over txlist.</td>
</tr>
<tr>
<td><code>EDGE_SRG_TXLIST_ENFORCE_REPOSITION</code></td>
<td>0x00000100</td>
<td>Reposition entry in txlist.</td>
</tr>
<tr>
<td><code>EDGE_SRG_SLAVE_SEND_NACK</code></td>
<td>0x00000200</td>
<td>SRG-SLAVE has send NACK before delete.</td>
</tr>
<tr>
<td><code>EDGE_SRG_OPCODE_FLAG_NONE</code></td>
<td>0x00000400</td>
<td>No SRG sync.</td>
</tr>
<tr>
<td><code>EDGE_SRG_OPCODE_FLAG_UPDATE</code></td>
<td>0x00000800</td>
<td>OPCODE flag is created or updated.</td>
</tr>
<tr>
<td><code>EDGE_SRG_OPCODE_FLAG_DELETE</code></td>
<td>0x00001000</td>
<td>OPCODE flag is deleted.</td>
</tr>
<tr>
<td><code>EDGE_SRG_STATE_FLAG_NONE</code></td>
<td>0x00002000</td>
<td>SRG state is none.</td>
</tr>
<tr>
<td><code>EDGE_SRG_STATE_FLAG_MASTER</code></td>
<td>0x00004000</td>
<td>SRG State Master flags.</td>
</tr>
<tr>
<td><code>EDGE_SRG_STATE_FLAG_MASTER_IN_TXLIST</code></td>
<td>0x00008000</td>
<td>State Master flags in the txlist.</td>
</tr>
<tr>
<td><code>EDGE_SRG_STATE_FLAG_SLAVE</code></td>
<td>0x00100000</td>
<td>SRG State Slave flags.</td>
</tr>
<tr>
<td><code>EDGE_SRG_ROLE_CHANGE</code></td>
<td>0x00200000</td>
<td>SRG role change flags.</td>
</tr>
<tr>
<td><code>EDGE_SRG_FC_STATE_INFLIGHT</code></td>
<td>0x00400000</td>
<td>SRG flow control flags.</td>
</tr>
<tr>
<td><code>EDGE_SRG_STATE_FLAG_INVALID</code></td>
<td>0x00800000</td>
<td>SRG State flag is invalid.</td>
</tr>
<tr>
<td><code>EDGE_SRG_STATE_FLAG_SESSION_RESTORE</code></td>
<td>0x01000000</td>
<td>SRG State Session Restore flag.</td>
</tr>
</tbody>
</table>
This is the sample output of the `show subscriber session all username` command:

```
RP/0/0/CPU0:server#show subscriber session all username
Thu Mar 13 16:25:21.861 IST
Codes: IN - Initialize, CN - Connecting, CD - Connected, AC - Activated,
       ID - Idle, DN - Disconnecting, ED - End

Username  Interface  State        Subscriber IP Addr / Prefix
          LNS Address (Vrf)
--------------------------------------------------------------------------------
basic@cisco.com  Gi0/0/0/0.pppoe1  AC  10.0.0.2 (default)
basic@cisco.com  Gi0/0/0/0.pppoe2  AC  10.0.0.3 (default)
basic@cisco.com  Gi0/0/0/0.pppoe3  AC  10.0.0.1 (default)
basic@cisco.com  Gi0/0/0/0.1.pppoe1  AC  10.0.0.4 (default)
```

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 Address: 2001:2::b246, VRF: default
Delegated IPv6 Prefix: 3000:2:0:8546::/64, VRF: default
IPv6 Interface ID: 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]
```
This sample output of `show subscriber session all` command, displays the active IPv4 or IPv6 client sessions for a dual-stack configuration.

```
RP/0/RSP0/CPU0:router# show subscriber session all

Tue Jan 29 12:49:25.237 UTC

Codes: IN - Initialize, CN - Connecting, CD - Connected, AC - Activated, ID - Idle, DN - Disconnecting, ED - End

<table>
<thead>
<tr>
<th>Type</th>
<th>Interface</th>
<th>State</th>
<th>Subscriber IP Addr / Prefix LNS Address (Vrf)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP:DHCP</td>
<td>BE1.10.ip22</td>
<td>AC</td>
<td>10.10.10.10 (default)</td>
</tr>
</tbody>
</table>
```

This sample output of `show subscriber session all detail` command, displays the detailed information of the active IPv4 or IPv6 client sessions for a dual-stack configuration.

```
RP/0/RSP0/CPU0:router# show subscriber session all detail

Tue Jan 29 12:49:27.752 UTC
Interface: Bundle-Ether1.10.ip22
Circuit ID: Unknown
Remote ID: Unknown
Type: IP: DHCP-trigger
IPv4 State: Up, Tue Jan 29 12:46:32 2013
IPv4 Address: 10.10.10.10, VRF: default
IPv6 Address: 2001::2, VRF: default
IPv6 Interface ID: ..d..... (02 00 64 ff fe 01 01 02)
Mac Address: 0000.6401.0102
Account-Session Id: 0000001c
Nas-Port: Unknown
User name: 0000.6401.0102
Outer VLAN ID: 10
Subscriber Label: 0x00000055
Created: Tue Jan 29 12:46:32 2013
State: Activated
Authentication: unauthenticated
Access-interface: Bundle-Ether1.10

Policy Executed:

policy-map type control subscriber pm-src-mac
event Session-Start match-all [at Tue Jan 29 12:46:32 2013]

    class type control subscriber dual_stack_class_map do-all [Succeeded]
1    activate dynamic-template Dual_stack_IPoE [Succeeded]
2    authorize aaa list default [Succeeded]
```
show subscriber session

Acct-Session-Id: 0000001c
Method-list: default
Accounting started: Tue Jan 29 12:46:32 2013
Interim accounting: On, interval 1 mins
  Last successful update: Tue Jan 29 12:48:34 2013
  Next update in: 00:00:06 (dhms)
Last COA request received: unavailable
show subscriber session filter

To show the search results of the subscriber sessions database based on the filter criteria, use the `show subscriber session filter` command in the EXEC mode.

```
show subscriber session filter [interface type interface-path-id | ipv4-address ipv4_address | ipv6-address IANA ipv6_address | mac-address mac_address | state subscriber_state | username user_name | vrf vrf_name] [detail | location]
```

**Syntax Description**

- `interface` Filters on local subscriber interface name.
- `ipv4-address` Filters on subscriber IPv4 address.
- `ipv6-address IANA` Filters on subscriber IPv6 IANA address.
- `mac-address` Filters on subscriber MAC address.
- `state` Filters on subscriber session state.
- `username` Filters on user name.
- `vrf` Filters on subscriber within a particular vrf.

**Command Default**

None

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4.1</td>
<td>This command was modified to include an option to display the output for DHCP IPv6 IANA subscriber sessions.</td>
</tr>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 `dynamic-template` command to enter dynamic template configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>read</td>
</tr>
<tr>
<td>config-services</td>
<td>read</td>
</tr>
</tbody>
</table>

`RP/0/RSP0/CPU0:router# show subscriber session filter interface Bundle-ether100.10 0/1/0/3`  
`RP/0/RSP0/CPU0:router# show subscriber session filter ipv4-address 5.5.5.5 detail location 0/1/CPU0`
show subscriber session filter

This example shows a sample output of DHCP IPv6 IANA subscriber session details on a particular access-interface:

Fri Mar 9 13:56:26.710 EDT
Interface: Bundle-Ether512.10.ip10
Circuit ID: Unknown
Remote ID: Unknown
Type: IP: DHCP-trigger
IPv6 Address: 2001:DB8:1::1, VRF: default
IPv6 Interface ID: 0x00000248
Mac Address: A.B.C
Account-Session Id: 0000000a
Nas-Port: Unknown
User name: unknown
Formatted User name: unknown
Client User name: unknown
Outer VLAN ID: 10
Subscriber Label: 0x00000248
Created: Fri Mar 9 13:55:42 2018
State: Activated
Authentication: unauthenticated
Authorization: unauthorized
Access-interface: Bundle-Ether512.10
Policy Executed:
  policy-map type control subscriber pm-ipoe-httpe
    event Session-Start match-first [at Fri Mar 9 13:55:42 2018]
      class type control subscriber http://default [Succeeded]
        1 activate dynamic-template tmp1-dtmp1-1 [Succeeded]
        2 activate dynamic-template http://service-pldt [Succeeded]
Session Accounting: disabled
Last COA request received: unavailable

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>class-map type control subscriber, on page 103</td>
<td>Enables the class-map.</td>
</tr>
<tr>
<td>policy-map type control subscriber, on page 114</td>
<td>Enables the policy-map.</td>
</tr>
<tr>
<td>event, on page 107</td>
<td>Enables the event in the policy-map.</td>
</tr>
<tr>
<td>show subscriber session, on page 608</td>
<td>Displays the subscriber management session information.</td>
</tr>
</tbody>
</table>
show subscriber session history

To show the search results from the Unified Session History (USH) database for the subscriber sessions based on the key type, use the `show subscriber session history` command in the EXEC mode.

```
show subscriber session history [subscriber-mac mac-address | analytics | subscriber-ifhandle if-handle | subscriber-label subscriber-label | [subscriber-ip IPv4-address | vrf vrf-name] | [subscriber-ipv6 IPv6-address | vrf vrf-name] ] [disconnected | errored | location]
```

**Syntax Description**

- `subscriber-mac` Displays the event history for the specified subscriber MAC address.
- `analytics` Displays USH data analytics.
- `subscriber-ifhandle` Displays the event history for the specified subscriber interface handle.
- `subscriber-label` Displays the event history for the specified subscriber label.
- `subscriber-ip` Displays the event history for the specified subscriber IPv4 address.
- `subscriber-ipv6` Displays the event history for the specified subscriber IPv6 address.
- `vrf` Displays the event history for the specified subscriber within a particular vrf.
- `disconnected` Displays the event history for the successfully disconnected session.
- `errored` Displays the event history of an errored session.

**Command Default**

None

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.5.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

None

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>read</td>
</tr>
<tr>
<td>config-services</td>
<td>read</td>
</tr>
</tbody>
</table>

```
RP/0/RSP0/CPU0:router# show subscriber session history subscriber-mac 0020.9400.000c
RP/0/RSP0/CPU0:router# show subscriber session history subscriber-mac 0010.9400.0094 disconnected
RP/0/RSP0/CPU0:router# show subscriber session history subscriber-mac 0020.9400.000c errored
```
This example shows a sample output of the event history of an active subscriber which has the specified subscriber MAC address:

```
RP/0/RSP0/CPU0:router# show subscriber session history subscriber-mac 0020.9400.000c
oper/ush/&&/key path mac/0020.9400.000c/0
STAF event history
Subscriber state: Active
SubscriberMAC:0020.9400.000c
ifhandle: 0x0000cba0
sublabel: 0x00000052
ipv4 Address:192.168.1.42
ipv6 Address: No IPv6 address
vrf:0x60000000 (default)
```

<table>
<thead>
<tr>
<th>Time stamp</th>
<th>comp_name</th>
<th>event</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/07/2018 16:34:52:743135</td>
<td>dhcp</td>
<td>Discover pkt procsd</td>
</tr>
<tr>
<td>11/07/2018 16:34:52:743135</td>
<td>iedge</td>
<td>IPv4 Start</td>
</tr>
<tr>
<td>11/07/2018 16:34:52:747135</td>
<td>aaa</td>
<td>Radiusd received Authorization request</td>
</tr>
<tr>
<td>11/07/2018 16:34:52:748134</td>
<td>aaa</td>
<td>Radiusd successfully built Access-Request packet</td>
</tr>
<tr>
<td>11/07/2018 16:34:52:750134</td>
<td>aaa</td>
<td>Radiusd Successfully sent packet and started timeout handler</td>
</tr>
<tr>
<td>11/07/2018 16:34:52:753134</td>
<td>aaa</td>
<td>Radiusd received Access-Accept</td>
</tr>
<tr>
<td>11/07/2018 16:34:52:753134</td>
<td>aaa</td>
<td>Decode radius packet success</td>
</tr>
<tr>
<td>11/07/2018 16:34:52:753134</td>
<td>aaa</td>
<td>Radiusd sending reply back to client</td>
</tr>
<tr>
<td>11/07/2018 16:34:52:759133</td>
<td>dhcp</td>
<td>Session Created - Init state</td>
</tr>
<tr>
<td>11/07/2018 16:34:52:760133</td>
<td>dhcp</td>
<td>IP allocated - Init state</td>
</tr>
<tr>
<td>11/07/2018 16:34:52:764132</td>
<td>dhcp</td>
<td>Request pkt procsd - Post Offer sent</td>
</tr>
<tr>
<td>11/07/2018 16:34:52:764132</td>
<td>ipsub</td>
<td>IPSub intf creation started</td>
</tr>
<tr>
<td>11/07/2018 16:34:52:764132</td>
<td>ipsub</td>
<td>IPSub init callback from Ifmg</td>
</tr>
<tr>
<td>11/07/2018 16:34:52:764132</td>
<td>ipsub</td>
<td>IPSub session start event to iEdge</td>
</tr>
<tr>
<td>11/07/2018 16:34:52:764132</td>
<td>ipsub</td>
<td>IPSub init to Ifmgr</td>
</tr>
<tr>
<td>11/07/2018 16:34:52:884114</td>
<td>ipsub</td>
<td>IPSub received VRF details</td>
</tr>
<tr>
<td>11/07/2018 16:34:52:951103</td>
<td>iedge</td>
<td>SUBDB produce done</td>
</tr>
<tr>
<td>11/07/2018 16:34:52:976099</td>
<td>ipsub</td>
<td>IPSub RIB details added</td>
</tr>
<tr>
<td>11/07/2018 16:34:53:078084</td>
<td>ipsub</td>
<td>IPSub session up</td>
</tr>
</tbody>
</table>
This example shows a sample output of the event history of a successfully disconnected subscriber which has the specified subscriber MAC address:

```
RP/0/RSP0/CPU0# show subscriber session history subscriber-mac 0010.9400.0094
disconnected
```

```
Time stamp   comp_name   event
------------------   ---------   ------------
05/12/2016 12:45:35:328697   dhcp   Discover pkt procsd
05/12/2016 12:45:35:328697   ledge   IPv4 Start
05/12/2016 12:45:38:412225   ipsub   IPSub session up
05/12/2016 12:45:38:417224   ledge   IPv4 Up
05/12/2016 12:45:38:422223   ledge   SUBDB produce done
06/12/2016 07:07:12:330971   dhcp   Lease expired for client
```

This example shows a sample output of the event history of an errored subscriber session which has the specified subscriber MAC address:

```
RP/0/RSP0/CPU0# show subscriber session history subscriber-mac 0020.9400.000c
errored
```

```
Time stamp   comp_name   event
------------------   ---------   ------------
```
### show subscriber session history

<table>
<thead>
<tr>
<th>Time</th>
<th>Username</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/07/2018 16:32:33:783399</td>
<td>aaa</td>
<td>Radiusd Successfully sent packet and started timeout handler</td>
</tr>
<tr>
<td>11/07/2018 16:32:38:790633</td>
<td>aaa</td>
<td>Radiusd Successfully sent packet and started timeout handler</td>
</tr>
<tr>
<td>11/07/2018 16:32:43:801866</td>
<td>aaa</td>
<td>Radiusd Successfully sent packet and started timeout handler</td>
</tr>
<tr>
<td>11/07/2018 16:32:48:808100</td>
<td>aaa</td>
<td>Radius packet sending failed Reason: 'RADIUS' detected the 'fatal' condition 'No server information is available'</td>
</tr>
<tr>
<td>11/07/2018 16:32:48:808100</td>
<td>iedge</td>
<td>policy rule failed Reason: 'AAA_BASE' detected the 'fatal' condition 'Invalid state (aaa base lib error)'</td>
</tr>
</tbody>
</table>