



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 2](#)
- [ipv4 unnumbered \(point-to-point -BNG\), on page 4](#)
- [ipv4 unreachable disable \(BNG\), on page 6](#)
- [ipv4 verify unicast source reachable-via \(BNG\), on page 8](#)
- [ipv6 enable \(BNG\), on page 10](#)
- [ipv6 mtu \(BNG\), on page 12](#)
- [ipv6 unreachable disable \(BNG\), on page 14](#)
- [show ipv4 interface \(BNG\), on page 16](#)
- [show ipv4 traffic \(BNG\), on page 19](#)
- [show ipv6 interface \(BNG\), on page 21](#)
- [show ipv6 neighbors \(BNG\), on page 25](#)
- [show ipv6 neighbors summary \(BNG\), on page 29](#)
- [show ipv6 traffic \(BNG\), on page 30](#)

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

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.2.0	This command was supported in the dynamic template configuration mode for BNG.

Usage Guidelines

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

Task ID	Operations
ipv4	read, write

Task ID	Operations
network	read, write
config-services	read, write

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

Command	Description
show ipv4 interface (BNG), on page 16	Displays the MTU status of interfaces configured for IPv4.

ipv4 unnumbered (point-to-point -BNG)

To enable IPv4 processing on a point-to-point interface without assigning an explicit IPv4 address to that interface, use the **ipv4 unnumbered** command in an appropriate configuration mode. To disable this feature, use the **no** form of this command.

ipv4 unnumbered *interface-type interface-instance*

Syntax Description

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

interface-instance Either a physical interface instance or a virtual interface instance as follows:

- Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation.
 - *rack*: Chassis number of the rack.
 - *slot*: Physical slot number of the modular services card or line card.
 - *module*: Module number. A physical layer interface module (PLIM) is always 0.
 - *port*: Physical port number of the interface.

Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RSP0) and the module is CPU0. Example: interface MgmtEth0/RSP0 /CPU0/0.

- Virtual interface instance. Number range varies depending on interface type.

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

Command Default

IPv4 processing on a point-to-point interface is disabled unless an IPv4 address is assigned explicitly to that interface.

Command Modes

Interface configuration (for releases prior to R4.2.0)

Dynamic template configuration (for releases R4.2.0 onward)

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.2.0	This command was supported in the dynamic template configuration mode for BNG.

Usage Guidelines

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).

Task ID	Task ID	Operations
	ipv4	read, write
	network	read, write
	config-services	read, write

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 0/1/1/0
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 unreachable disable (BNG)

To disable the generation of IPv4 Internet Control Message Protocol (ICMP) unreachable messages, use the **ipv4 unreachable disable** command in an appropriate configuration mode. To re-enable the generation of ICMP unreachable messages, use the **no** form of this command.

ipv4 unreachable disable

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

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.2.0	This command was supported in the dynamic template configuration mode for BNG.

Usage Guidelines

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

Task ID	Operations
ipv4	read, write
network	read, write
config-services	read, write

Examples

For releases prior to R4.2.0, this example shows how to disable the generation of ICMP unreachable messages on GigabitEthernetinterface 0/1/1/0:

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/1/0
RP/0/RSP0/CPU0:router(config-if)# ipv4 unreachable 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 unreachable 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	any	Enables loose unicast RPF checking. If loose unicast RPF is enabled, a packet is not forwarded unless its source prefix exists in the routing table.
	rx	Enables strict unicast RPF checking. If strict unicast RPF is enabled, a packet is not forwarded unless its source prefix exists in the routing table and the output interface matches the interface on which the packet was received.
	allow-default	(Optional) Enables the matching of default routes. This option applies to both loose and strict RPF.
	allow-self-ping	(Optional) Enables the router to ping out an interface. This option applies to both loose and strict RPF.
Command Default	IPv4 unicast RPF is disabled.	
Command Modes	Dynamic template configuration	
Command History	Release	Modification
	Release 3.7.2	This command was introduced.
	Release 4.2.0	This command was supported in the dynamic template configuration mode for BNG.
Usage Guidelines	To enter the dynamic template configuration mode, run dynamic-template command in the Global Configuration mode.	
	Use the ipv4 verify unicast source reachable-via interface command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through a router. Malformed or forged source addresses can indicate denial-of-service (DoS) attacks based on source IP address spoofing.	
	When strict unicast RPF is enabled on an interface, the router examines all packets received on that interface. The router checks to make sure that the source address appears in the routing table and matches the interface on which the packet was received.	
	When loose unicast RPF is enabled on an interface, the router examines all packets received on that interface. The router checks to make sure that the source address can be reached through any of the router interfaces.	
Task ID	Task ID	Operations
	ipv4	read, write
	network	read, write

Task ID	Operations
config-services	read, write

Examples

This example shows how to configure strict RPF on dynamic template configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv4 verify unicast source reachable-via
rx
```

ipv6 enable (BNG)

To enable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **ipv6 enable** command in an appropriate configuration mode. To disable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **no** form of this command.

ipv6 enable

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

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.3.0	This command was supported in the dynamic template configuration mode for BNG.

Usage Guidelines

The **ipv6 enable** command automatically configures an IPv6 link-local unicast address on the interface while also enabling the interface for IPv6 processing. The **no ipv6 enable** command does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address.

For BNG, ensure you run this command in the dynamic template configuration mode. To enter the dynamic template configuration mode, run **dynamic-template** command in the Global Configuration mode.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

This example (not applicable for BNG) shows how to enable IPv6 processing on 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 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

Command	Description
show ipv6 interface (BNG), on page 21	Displays the usability status of interfaces configured for IPv6.

ipv6 mtu (BNG)

To set the maximum transmission unit (MTU) size of IPv6 packets sent on an interface, use the **ipv6 mtu** command in an appropriate configuration mode. To restore the default MTU size, use the **no** form of this command.

ipv6 mtu *bytes*

Syntax Description	<i>bytes</i> 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> <tr> <th>Release</th><th>Modification</th></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> </table>	Release	Modification	Release 3.7.2	This command was introduced.	Release 4.3.0	This command was supported in the dynamic template configuration mode for BNG.
Release	Modification						
Release 3.7.2	This command was introduced.						
Release 4.3.0	This command was supported in the dynamic template configuration mode for BNG.						
Usage Guidelines	<p>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.</p> <p>All devices on a physical medium must have the same protocol MTU to operate.</p> <p>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.</p>						
 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> <tr> <th>Task ID</th><th>Operations</th></tr> <tr> <td>ipv6</td><td>read, write</td></tr> <tr> <td>network</td><td>read, write</td></tr> </table>	Task ID	Operations	ipv6	read, write	network	read, write
Task ID	Operations						
ipv6	read, write						
network	read, write						

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 0/1/1/0 to 1350 bytes:

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/1/0
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:

```
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp foo
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv6 mtu 1350
```

Related Commands

Command	Description
show ipv6 interface (BNG), on page 21	Displays the usability status of interfaces configured for IPv6.

ipv6 unreachable disable (BNG)

To disable the generation of IPv6 Internet Control Message Protocol (ICMP) unreachable messages, use the **ipv6 unreachable disable** command in an appropriate configuration mode. To re-enable the generation of ICMP unreachable messages, use the **no** form of this command.

ipv6 unreachable 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> <tr> <th>Release</th><th>Modification</th></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> </table>	Release	Modification	Release 3.7.2	This command was introduced.	Release 4.3.0	This command was supported in the dynamic template configuration mode for BNG.		
Release	Modification								
Release 3.7.2	This command was introduced.								
Release 4.3.0	This command was supported in the dynamic template configuration mode for BNG.								
Usage Guidelines	<p>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.</p> <p>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.</p> <p>This command affects a number of ICMP unreachable messages.</p> <p>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.</p>								
Task ID	<table> <tr> <th>Task ID</th><th>Operations</th></tr> <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> </table>	Task ID	Operations	ipv6	read, write	network	read, write	config-services	read, write
Task ID	Operations								
ipv6	read, write								
network	read, write								
config-services	read, write								
Examples	<p>This example (not applicable for BNG) shows how to disable the generation of ICMP unreachable messages on GigabitEthernet interface 0/6/0/0:</p> <pre>RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/6/0/0 RP/0/RSP0/CPU0:router(config-if)# ipv6 unreachable disable</pre>								

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 unreachable disable
```

show ipv4 interface (BNG)

To display the usability status of interfaces configured for IPv4, use the **show ipv4 interface** command in the EXEC mode.

show ipv4 [**vrf** *vrf-name*] **interface** [{*type interface-path-id* | **brief** | **summary**}]

Syntax Description	vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
	<i>vrf-name</i>	(Optional) Name of a VRF.
	<i>type</i>	Interface type. For more information, use the question mark (?) online help function.
	<i>interface-path-id</i>	Either a physical interface instance or a virtual interface instance as follows: <ul style="list-style-type: none"> Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <ul style="list-style-type: none"> <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface.
	Note	In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RSP0) and the module is CPU0. Example: interface MgmtEth0/RSP0 /CPU0/0.
		<ul style="list-style-type: none"> Virtual interface instance. Number range varies depending on interface type. <p>For more information about the syntax for the router, use the question mark (?) online help function.</p>
	brief	(Optional) Displays the primary IPv4 addresses configured on the router's interfaces and their protocol and line states.
	summary	(Optional) Displays the number of interfaces on the router that are assigned, unassigned, or unnumbered.
Command Default	If VRF is not specified, the software displays the default VRF.	
Command Modes	EXEC mode	
Command History	Release	Modification
	Release 3.7.2	This command was introduced.
	Release 4.2.0	This command was supported for BNG.

Usage Guidelines

The **show ipv4 interface** command provides output similar to the **show ipv6 interface** command, except that it is IPv4-specific.

The interface name will be displayed only if the name belongs to the VRF instance. If the *vrf-name* is not specified then the interface instance will be displayed only if the interface belongs to the default VRF.

Task ID**Task ID Operations**

ipv4	read
------	------

network	read
---------	------

Examples

This is the sample output of the **show ipv4 interface** command:

```
RP/0/RSP0/CPU0:router# show ipv4 interface

Loopback0 is Up, line protocol is Up
  Internet address is 10
  .0.0.1/8

  Secondary address 10.0.0.2/8
  MTU is 1514 (1514 is available to IP)
  Multicast reserved groups joined: 10.0.0.1
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
gigabitethernet0/0/0/0 is Up, line protocol is Up
  Internet address is 10.25.58.1/16
  MTU is 1514 (1500 is available to IP)
  Multicast reserved groups joined: 10.0.224.1
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
gigabitethernet0/0/0/0 is Shutdown, line protocol is Down
  Vrf is default (vrfid 0x60000000)
  Internet protocol processing disabled
```

This table describes the significant fields shown in the display.

Table 1: show ipv4 interface Command Field Descriptions

Field	Description
Loopback0 is Up	If the interface hardware is usable, the interface is marked “Up.” For an interface to be usable, both the interface hardware and line protocol must be up.
line protocol is Up	If the interface can provide two-way communication, the line protocol is marked “Up.” For an interface to be usable, both the interface hardware and line protocol must be up.

Field	Description
Internet address	IPv4 Internet address and subnet mask of the interface.
Secondary address	Displays a secondary address, if one has been set.
MTU	Displays the IPv4 MTU ¹ value set on the interface.
Multicast reserved groups joined	Indicates the multicast groups this interface belongs to.
Directed broadcast forwarding	Indicates whether directed broadcast forwarding is enabled or disabled.
Outgoing access list	Indicates whether the interface has an outgoing access list set.
Inbound access list	Indicates whether the interface has an incoming access list set.
Proxy ARP	Indicates whether proxy ARP ² is enabled or disabled on an interface.
ICMP redirects	Specifies whether ICMPv4 ³ redirects are sent on this interface.
ICMP unreachable	Specifies whether unreachable messages are sent on this interface.
Internet protocol processing disabled	Indicates an IPv4 address has not been configured on the interface.

¹ MTU = maximum transmission unit

² ARP = Address Resolution Protocol address resolution protocol

³ ICMPv4 = Internet Control Message Protocol 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> <tr> <th>Release</th><th>Modification</th></tr> <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> </table>	Release	Modification	Release 3.7.2	This command was introduced .	Release 4.2.0	This command was supported for BNG.
Release	Modification						
Release 3.7.2	This command was introduced .						
Release 4.2.0	This command was supported for BNG.						
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> <tr> <th>Task ID</th><th>Operations</th></tr> <tr> <td>ipv4</td><td>read</td></tr> <tr> <td>network</td><td>read</td></tr> </table>	Task ID	Operations	ipv4	read	network	read
Task ID	Operations						
ipv4	read						
network	read						

Examples

This is the sample output of the **show ipv4 traffic** command:

```
RP/0/RSP0/CPU0:router# show ipv4 traffic

IP statistics:
  Rcvd: 16372 total, 16372 local destination
        0 format errors, 0 bad hop count
        0 unknown protocol, 0 not a gateway
        0 security failures, 0 bad source, 0 bad header
        0 with options, 0 bad, 0 unknown
  Opts: 0 end, 0 nop, 0 basic security, 0 extended security
        0 strict source rt, 0 loose source rt, 0 record rt
        0 stream ID, 0 timestamp, 0 alert, 0 cipso
  Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
        0 fragmented, 0 fragment count
  Bcast: 0 sent, 0 received
  Mcast: 0 sent, 0 received
  Drop: 0 encapsulation failed, 0 no route, 0 too big, 0 sanity address check
  Sent: 16372 total

ICMP statistics:
  Sent: 0 admin unreachable, 0 network unreachable
        0 host unreachable, 0 protocol unreachable
        0 port unreachable, 0 fragment unreachable
        0 time to live exceeded, 0 reassembly ttl exceeded
        5 echo request, 0 echo reply
        0 mask request, 0 mask reply
```

show ipv4 traffic (BNG)

```

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 2: show ipv4 traffic Command Field Descriptions

Field	Description
bad hop count	Occurs when a packet is discarded because its TTL ⁴ field was decremented to zero.
encapsulation failed	Usually indicates that the router had no ARP request entry and therefore did not send a datagram.
format errors	Indicates a gross error in the packet format, such as an impossible Internet header length.
IP statistics Rcvd total	Indicates the total number of local destination and other packets received in the software plane. It does not account for the IP packets forwarded or discarded in hardware.
no route	Counted when the Cisco IOS XR software discards a datagram it did not know how to route.

⁴ TTL = time-to-live

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.
<i>vrf-name</i>	(Optional) Name of a VRF.
<i>type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>interface-path-id</i>	<p>(Optional) Either a physical interface instance or a virtual interface instance as follows:</p> <ul style="list-style-type: none"> Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <ul style="list-style-type: none"> <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. <p>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.</p> <ul style="list-style-type: none"> Virtual interface instance. Number range varies depending on interface type. <p>For more information about the syntax for the router, use the question mark (?) online help function.</p>
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

show ipv6 interface (BNG)

Command History	Release	Modification
	Release 3.7.2	This command was introduced.
	Release 4.3.0	This command was supported for BNG.
	Release 5.1.2	The link-local and global keywords were added to the command.

Usage Guidelines

The **show ipv6 interface** command provides output similar to the **show ipv4 interface** command, except that it is IPv6-specific.

Use the **link-local** or **global** keywords along with the **brief** keyword to view the link local or global IPv6 addresses.

Task ID	Task ID	Operations
	ipv6	read

Examples

This is the sample output of the **show ipv6 interface** command:

```
RP/0/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 unreachable 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 3: show ipv6 interface Command Field Descriptions

Field	Description
GigabitEthernet0 /3/0/0 is Shutdown, line protocol is Down	Indicates whether the interface hardware is currently active (whether line signal is present) and whether it has been taken down by an administrator. If the interface hardware is usable, the interface is marked "Up." For an interface to be usable, both the interface hardware and line protocol must be up.

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	<p>The state of the address in relation to duplicate address detection. States can be any of the following:</p> <ul style="list-style-type: none"> • duplicate—The address is not unique and is not being used. If the duplicate address is the link-local address of an interface, the processing of IPv6 packets is disabled on that interface. • tentative—Duplicate address detection is either pending or under way on this interface. <p>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.</p>
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
```

Interface	IPv6-Address	Status	Protocol
GigabitEthernet0/0/0/0	fe80::fe:8ff:feeb:26c5	Up	Up
GigabitEthernet0/0/0/1	fe80::4f:88ff:fea0:8c9d	Up	Up
GigabitEthernet0/0/0/3	unassigned	Shutdown	Down
GigabitEthernet0/0/0/4	unassigned	Shutdown	Down

This is the sample output of the **show ipv6 interface brief global** command:

show ipv6 interface (BNG)

```
RP/0/RSP0/CPU0:router#show ipv6 interface brief global
```

Interface	IPv6-Address	Status	Protocol
GigabitEthernet0/0/0/0	2001:db8::1	Up	Up
GigabitEthernet0/0/0/1	2001:db8::2	Up	Up
GigabitEthernet0/0/0/3	unassigned	Shutdown	Down
GigabitEthernet0/0/0/4	unassigned	Shutdown	Down

This is the sample output of the **show ipv6 interface type interface-path-id brief link-local** command:

```
RP/0/RSP0/CPU0:router#show ipv6 interface gigabitEthernet 0/0/0/0 brief link-local
```

Interface	IPv6-Address	Status	Protocol
GigabitEthernet0/0/0/0	fe80::fe:8ff:feeb:26c5	Up	Up

This is the sample output of the **show ipv6 interface type interface-path-id brief global** command:

```
RP/0/RSP0/CPU0:router#show ipv6 interface gigabitEthernet 0/0/0/0 brief global
```

Interface	IPv6-Address	Status	Protocol
GigabitEthernet0/0/0/0	2001:db8::1	Up	Up

This is the sample output of the **show ipv6 vrf vrf-name interface brief link-local** command:

```
RP/0/RSP0/CPU0:router#show ipv6 vrf vrf1 interface brief link-local
```

Interface	IPv6-Address	Status	Protocol
GigabitEthernet0/0/0/2	fe80::46:c8ff:fe22:daae	Up	Up

This is the sample output of the **show ipv6 vrf vrf-name interface brief global** command:

```
RP/0/RSP0/CPU0:router#show ipv6 vrf vrf1 interface brief global
```

Interface	IPv6-Address	Status	Protocol
GigabitEthernet0/0/0/2	2001:db8::2	Up	Up

This is the sample output of the **show ipv6 vrf vrf-name interface type interface-path-id brief link-local** command:

```
RP/0/RSP0/CPU0:router#show ipv6 vrf vrf1 interface gigabitEthernet 0/0/0/2 brief link-local
```

Interface	IPv6-Address	Status	Protocol
GigabitEthernet0/0/0/2	fe80::46:c8ff:fe22:daae	Up	Up

This is the sample output of the **show ipv6 vrf vrf-name interface type interface-path-id brief global** command:

```
RP/0/RSP0/CPU0:router#show ipv6 vrf vrf1 interface gigabitEthernet 0/0/0/2 brief global
```

Interface	IPv6-Address	Status	Protocol
GigabitEthernet0/0/0/2	2001:db8::2	Up	Up

Related Commands

Command	Description
show ipv4 interface (BNG) , on page 16	Displays the usability status of interfaces configured for IPv4.

show ipv6 neighbors (BNG)

To display the IPv6 neighbor discovery cache information, use the **show ipv6 neighbors** command in the EXEC mode.

show ipv6 neighbors [{*type interface-path-id* | **location** *node-id*}]

Syntax Description	<i>type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
	<i>interface-path-id</i>	(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 <i>node-id</i>	(Optional) Designates a node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Command Default All IPv6 neighbor discovery cache information is displayed.

Command History	Release	Modification
	Release 3.7.2	This command was introduced.
	Release 4.3.0	This command was supported for BNG.

Usage Guidelines When the *interface-type* and *interface-number* arguments are not specified, cache information for all IPv6 neighbors is displayed. Specifying the *interface-type* and *interface-number* arguments displays only cache information about the specified interface.

Task ID	Task ID	Operations
	ipv6	read

Examples

This is the sample output of the **show ipv6 neighbors** command when entered with an interface type and number:

```
RP/0/RSP0/CPU0:router# show ipv6 neighbors gigabitethernet 0/0/0/0
```

```
IPv6 Address                               Age Link-layer Addr State Interface
2000:0:0:4::2                             0 0003.a0d6.141e REACH gigabitethernet2
FE80::203:A0FF:FED6:141E                  0 0003.a0d6.141e REACH gigabitethernet2
3001:1::45a                              - 0002.7d1a.9472 REACH gigabitethernet2
```

This is the sample output of the **show ipv6 neighbors** command when entered with an IPv6 address:

show ipv6 neighbors (BNG)

```
RP/0/RSP0/CPU0:router# show ipv6 neighbors 2000:0:0:4::2
```

IPv6 Address	Age	Link-layer Addr	State	Interface
2000:0:0:4::2	0	0003.a0d6.141e	REACH	gigabitethernet2

This is the sample output of the **show ipv6 neighbors** command:

```
RP/0/RSP0/CPU0:router# show ipv6 neighbors
```

IPv6 Address	Age	Link-layer Addr	State	Interface	Location
2001:1::3	130	0011.9400.0003	REACH	BE1	0/0/CPU0
2001:1::4	335	0011.9400.0004	REACH	BE1	0/0/CPU0
2001:1::5	314	0011.9400.0005	REACH	BE1	0/0/CPU0
2001:1::6	291	0011.9400.0006	REACH	BE1	0/0/CPU0
2001:1::7	235	0011.9400.0007	REACH	BE1	0/0/CPU0
2001:1::8	340	0011.9400.0008	REACH	BE1	0/0/CPU0
2001:1::9	230	0011.9400.0009	REACH	BE1	0/0/CPU0
2001:1::a	99	0011.9400.000a	REACH	BE1	0/0/CPU0
2001:1::b	291	0011.9400.000b	REACH	BE1	0/0/CPU0
2001:1::c	226	0011.9400.000c	REACH	BE1	0/0/CPU0
2001:1::d	272	0011.9400.000d	REACH	BE1	0/0/CPU0
2001:1::e	14	0011.9400.000e	REACH	BE1	0/0/CPU0
2001:1::f	299	0011.9400.000f	REACH	BE1	0/0/CPU0
2001:1::10	131	0011.9400.0010	REACH	BE1	0/0/CPU0
2001:1::11	70	0011.9400.0011	REACH	BE1	0/0/CPU0
2001:1::12	131	0011.9400.0012	REACH	BE1	0/0/CPU0
2001:1::13	137	0011.9400.0013	REACH	BE1	0/0/CPU0
2001:1::14	290	0011.9400.0014	REACH	BE1	0/0/CPU0
2001:1::15	19	0011.9400.0015	REACH	BE1	0/0/CPU0
2001:1::16	158	0011.9400.0016	REACH	BE1	0/0/CPU0
2001:1::17	35	0011.9400.0017	REACH	BE1	0/0/CPU0
2001:1::18	222	0011.9400.0018	REACH	BE1	0/0/CPU0

This is the sample output of the **show ipv6 neighbors** command when entered with a location:

```
RP/0/RSP0/CPU0:router# show ipv6 neighbors location 0/2/CPU0
```

IPv6 Address	Age	Link-layer Addr	State	Interface	Location
2001:3::2	119	0013.9400.0002	REACH	BE3	0/2/CPU0
2001:3::3	179	0013.9400.0003	DELAY	BE3	0/2/CPU0
2001:3::4	166	0013.9400.0004	REACH	BE3	0/2/CPU0
2001:3::5	78	0013.9400.0005	REACH	BE3	0/2/CPU0
2001:3::6	19	0013.9400.0006	REACH	BE3	0/2/CPU0
2001:3::7	173	0013.9400.0007	REACH	BE3	0/2/CPU0
2001:3::8	140	0013.9400.0008	REACH	BE3	0/2/CPU0
2001:3::9	163	0013.9400.0009	REACH	BE3	0/2/CPU0
2001:3::a	40	0013.9400.000a	REACH	BE3	0/2/CPU0
2001:3::b	90	0013.9400.000b	REACH	BE3	0/2/CPU0
2001:3::c	35	0013.9400.000c	REACH	BE3	0/2/CPU0
2001:3::d	114	0013.9400.000d	REACH	BE3	0/2/CPU0
2001:3::e	117	0013.9400.000e	REACH	BE3	0/2/CPU0
2001:3::f	157	0013.9400.000f	REACH	BE3	0/2/CPU0
2001:3::10	9	0013.9400.0010	REACH	BE3	0/2/CPU0
2001:3::11	120	0013.9400.0011	REACH	BE3	0/2/CPU0
2001:3::12	87	0013.9400.0012	REACH	BE3	0/2/CPU0
2001:3::13	180	0013.9400.0013	DELAY	BE3	0/2/CPU0
2001:3::14	103	0013.9400.0014	REACH	BE3	0/2/CPU0
2001:3::15	132	0013.9400.0015	REACH	BE3	0/2/CPU0

```

2001:3::16      33    0013.9400.0016 REACH BE3      0/2/CPU0
2001:3::17      150   0013.9400.0017 REACH BE3      0/2/CPU0
2001:3::18      117   0013.9400.0018 REACH BE3      0/2/CPU0
2001:3::19      48    0013.9400.0019 REACH BE3      0/2/CPU0
2001:3::1a      67    0013.9400.001a REACH BE3      0/2/CPU0
2001:3::1b      91    0013.9400.001b REACH BE3      0/2/CPU0
2001:3::1c      33    0013.9400.001c REACH BE3      0/2/CPU0
2001:3::1d      174   0013.9400.001d DELAY BE3      0/2/CPU0
2001:3::1e      144   0013.9400.001e REACH BE3      0/2/CPU0
2001:3::1f      121   0013.9400.001f REACH BE3      0/2/CPU0
2001:3::20      53    0013.9400.0020 REACH BE3      0/2/CPU0

```

This table describes significant fields shown in the display.

Table 4: show ipv6 neighbors Command Field Descriptions

Field	Description
IPv6 Address	IPv6 address of neighbor or interface.
Age	Time (in minutes) since the address was confirmed to be reachable. A hyphen (-) indicates a static entry.
Link-layer Addr	MAC address. If the address is unknown, a hyphen (-) is displayed.
State	<p>The state of the neighbor cache entry. These are the states for dynamic entries in the IPv6 neighbor discovery cache:</p> <ul style="list-style-type: none"> • INCMP (incomplete)—Address resolution is being performed on the entry. A neighbor solicitation message has been sent to the solicited-node multicast address of the target, but the corresponding neighbor advertisement message has not yet been received. • reach (reachable)—Positive confirmation was received within the last ReachableTime milliseconds that the forward path to the neighbor was functioning properly. While in reach state, the device takes no special action as packets are sent. • stale—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. While in stale state, the device takes no action until a packet is sent. • delay—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. A packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the delay state, send a neighbor solicitation message and change the state to probe. • probe—A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer milliseconds until a reachability confirmation is received. <p>These are the possible states for static entries in the IPv6 neighbor discovery cache:</p> <ul style="list-style-type: none"> • reach (reachable)—The interface for this entry is up. • INCMP (incomplete)—The interface for this entry is down. <p>Note Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache; therefore, the descriptions for the INCMP (incomplete) and reach (reachable) states are different for dynamic and static cache entries.</p>

 show ipv6 neighbors (BNG)

Field	Description
Interface	Interface from which the address is reachable.

Related Commands

Command	Description
show ipv6 neighbors summary (BNG), on page 29	Displays summary information for the neighbor entries.

show ipv6 neighbors summary (BNG)

To display summary information for the neighbor entries, use the **show ipv6 neighbors summary** command in the EXEC mode.

show ipv6 neighbors summary

Syntax Description

None

Command Default

The default value is disabled.

Command Modes

EXEC mode

Command History

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

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ipv6	read

Examples

This is the sample output of the **show ipv6 neighbors summary** command that shows the summary information for the neighbor entries:

```
RP/0/RSP0/CPU0:router# show ipv6 neighbors summary

Mcast nbr entries:
  Subtotal: 0
Static nbr entries:
  Subtotal: 0
Dynamic nbr entries:
  Subtotal: 0

Total nbr entries: 0
```

Related Commands

Command	Description
show ipv6 neighbors (BNG), on page 25	Displays IPv6 neighbor discovery cache information.

show ipv6 traffic (BNG)

To display the IPv6 traffic statistics, use the **show traffic** command in the EXEC mode.

show ipv6 traffic [brief]

Syntax Description	brief (Optional) Displays only IPv6 and Internet Control Message Protocol version 6 (ICMPv6) traffic statistics.						
Command Default	None						
Command History	<table> <tr> <th>Release</th><th>Modification</th></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 for BNG.</td></tr> </table>	Release	Modification	Release 3.7.2	This command was introduced.	Release 4.3.0	This command was supported for BNG.
Release	Modification						
Release 3.7.2	This command was introduced.						
Release 4.3.0	This command was supported for BNG.						
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> <tr> <th>Task ID</th><th>Operations</th></tr> <tr> <td>ipv6</td><td>read</td></tr> <tr> <td>network</td><td>read</td></tr> </table>	Task ID	Operations	ipv6	read	network	read
Task ID	Operations						
ipv6	read						
network	read						

Examples

This is the sample output of the **show ipv6 traffic** command:

```
RP/0/RSP0/CPU0:router# show ipv6 traffic

IPv6 statistics:
  Rcvd: 0 total, 0 local destination
        0 source-routed, 0 truncated
        0 format errors, 0 hop count exceeded
        0 bad header, 0 unknown option, 0 bad source
        0 unknown protocol
        0 fragments, 0 total reassembled
        0 reassembly timeouts, 0 reassembly failures
        0 reassembly max drop
        0 sanity address check drops
  Sent: 0 generated, 0 forwarded
        0 fragmented into 0 fragments, 0 failed
        0 no route, 0 too big
  Mcast: 0 received, 0 sent

ICMP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 too short
        0 unknown error type
  unreach: 0 routing, 0 admin, 0 neighbor,
           0 address, 0 port, 0 unknown
  parameter: 0 error, 0 header, 0 option,
             0 unknown
```

```

    0 hopcount expired, 0 reassembly timeout,
    0 unknown timeout, 0 too big,
    0 echo request, 0 echo reply
Sent: 0 output, 0 rate-limited
      unreachable: 0 routing, 0 admin, 0 neighbor,
                   0 address, 0 port, 0 unknown
      parameter: 0 error, 0 header, 0 option
                0 unknown
    0 hopcount expired, 0 reassembly timeout,
    0 unknown timeout, 0 too big,
    0 echo request, 0 echo reply

Neighbor Discovery ICMP statistics:
  Rcvd: 0 router solicit, 0 router advert, 0 redirect
        0 neighbor solicit, 0 neighbor advert
  Sent: 0 router solicit, 0 router advert, 0 redirect
        0 neighbor solicit, 0 neighbor advert

UDP statistics:
    0 packets input, 0 checksum errors
    0 length errors, 0 no port, 0 dropped
    0 packets output

TCP statistics:s
    0 packets input, 0 checksum errors, 0 dropped
    0 packets output, 0 retransmitted

```

This table describes the significant fields shown in the display.

Table 5: show ipv6 traffic Command Field Descriptions

Field	Description
Rcvd:	Statistics in this section refer to packets received by the router.
total	Total number of packets received by the software.
local destination	Locally destined packets received by the software.
source-routed	Packets seen by the software with RH.
truncated	Truncated packets seen by the software.
bad header	An error was found in generic HBH, RH, DH, or HA. Software only.
unknown option	Unknown option type in IPv6 header.
unknown protocol	Protocol specified in the IP header of the received packet is unreachable.
Sent:	Statistics in this section refer to packets sent by the router.
forwarded	Packets forwarded by the software. If the packet cannot be forwarded in the first lookup (for example, the packet needs option processing), then the packet is not included in this count, even if it ends up being forwarded by the software.
Mcast:	Multicast packets.
ICMP statistics:	Internet Control Message Protocol statistics.

 `show ipv6 traffic (BNG)`**Related Commands**

Command	Description
show ipv4 traffic (BNG), on page 19	Displays statistics about IPv4 traffic.