debug crypto ipv6 ipsec

To display IP Security (IPSec) events for IPv6 networks, use the **debug crypto ipv6 ipsec** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug crypto ipv6 ipsec

no debug crypto ipv6 ipsec

Syntax Description

This command has no arguments or keywords.

Command Default

Debugging for IPv6 IPSec events is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Use this command to display IPSec events while setting up or removing policy definitions during OSPF configuration.

Examples

The following example enables the display of IPSec events for IPv6 networks:

```
Router# debug crypto ipv6 ipsec
```

Related Commands

Command	Description
debug crypto engine	Displays debugging messages about crypto engines, which perform encryption and decryption.
debug crypto ipv6 packet	Displays debug messages for IPv6 packets allowing you to see the contents of packets outbound from a Cisco router when the remote node is not a Cisco node.
debug crypto socket	Displays communication between the client and IPSec during policy setup and removal processes.
debug ipv6 ospf authentication	Displays the interaction between OSPF and IPSec, including creation or removal of policies.

debug crypto ipv6 packet

To display the contents of IPv6 packets, use the **debug crypto ipv6 packet** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug crypto ipv6 packet

no debug crypto ipv6 packet

Syntax Description

This command has no arguments or keywords.

Command Default

Debugging for IPv6 IPSec packets is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Consult Cisco Technical Support before using this command.

Use this command to display the contents of IPv6 packets. This command is useful when the remote node is not a Cisco device and communication between the Cisco and non-Cisco router cannot be established. This command enables you to look at the contents of the packets outbound from the Cisco router.

This command examines the content of every IPv6 packet and may slow network performance.

Examples

This example shows the output of each packet when the **debug crypto ipv6 packet** command is enabled:

```
Router# debug crypto ipv6 packet

Crypto IPv6 IPSEC packet debugging is on

Router#
*Oct 30 16:57:06.330:
IPSECv6:before Encapsulation of IPv6 packet:
0E37A7C0:                  6E000000 00285901          n....(Y.
0E37A7D0:FE800000 00000000 020A8BFF FED42C1D  ~...........~T,.
0E37A7E0:FF020000 00000000 00000000 00000005  ................
0E37A7F0:03010028 01010104 00000001 8AD80000  ...(.........X..
0E37A800:00000006 01000013 000A0028 0A0250CF  ...........(..PO
0E37A810:01010104 0A0250CF                    ......PO
*Oct 30 16:57:06.330:
IPSECv6:Encapsulated IPv6 packet
:
0E37A7B0:6E000000 00403301 FE800000 00000000  n....@3.~.......
0E37A7C0:020A8BFF FED42C1D FF020000 00000000  ....~T,.........
```

```
0E37A7D0:00000000 00000005 59040000 000022B8  ........Y....."8
0E37A7E0:0000001A 38AB1ED8 04C1C6FB FF1248CF  ....8+.X.AF{..HO
0E37A7F0:03010028 01010104 00000001 8AD80000  ...(.........X..
0E37A800:00000006 01000013 000A0028 0A0250CF  ...........(..PO
0E37A810:01010104 0A0250CF                    ......PO
*Oct 30 16:57:11.914:
IPSECv6:Before Decapsulation of IPv6 packet
:
0E004A50:                  6E000000 00403301          n....@3.
0E004A60:FE800000 00000000 023071FF FE7FE81D  ~........0q.~.h.
0E004A70:FF020000 00000000 00000000 00000005  ................
0E004A80:59040000 000022B8 00001D88 F5AC68EE  Y....."8....u,hn
0E004A90:1AC00088 947C6BF2 03010028 0A0250CF  .@...|kr...(..PO
0E004AA0:00000001 E9080000 00000004 01000013  ....i...........
0E004AB0:000A0028 0A0250CF 01010104 01010104  ...(..PO........
0E004AC0:
*Oct 30 16:57:11.914:
IPSECv6:Decapsulated IPv6 packet
:
0E004A70:6E000000 00285901 FE800000 00000000  n....(Y.~.......
0E004A80:023071FF FE7FE81D FF020000 00000000  .0q.~.h.........
0E004A90:00000000 00000005 03010028 0A0250CF  ...........(..PO
0E004AA0:00000001 E9080000 00000004 01000013  ....i...........
0E004AB0:000A0028 0A0250CF 01010104 01010104  ...(..PO........
0E004AC0:
*Oct 30 16:57:16.330:
IPSECv6:before Encapsulation of IPv6 packet:
0E003DC0:                  6E000000 00285901          n....(Y.
0E003DD0:FE800000 00000000 020A8BFF FED42C1D  ~...........~T,.
0E003DE0:FF020000 00000000 00000000 00000005  ................
0E003DF0:03010028 01010104 00000001 8AD80000  ...(.........X..
0E003E00:00000006 01000013 000A0028 0A0250CF  ...........(..PO
0E003E10:01010104 0A0250CF                    ......PO
*Oct 30 16:57:16.330:
IPSECv6:Encapsulated IPv6 packet
:
0E003DB0:6E000000 00403301 FE800000 00000000  n....@3.~.......
0E003DC0:020A8BFF FED42C1D FF020000 00000000  ....~T,.........
0E003DD0:00000000 00000005 59040000 000022B8  ........Y....."8
0E003DE0:0000001B F8E3C4E2 4CC4B690 DDF32B5C  ....xcDbLD6.]s+\
0E003DF0:03010028 01010104 00000001 8AD80000  ...(.........X..
0E003E00:00000006 01000013 000A0028 0A0250CF  ...........(..PO
0E003E10:01010104 0A0250CF                    ......PO
```

Related Commands

Command	Description
debug crypto engine	Displays debugging messages about crypto engines, which perform encryption and decryption.
debug crypto ipv6 ipsec	Displays IPSec events for IPv6 networks.
debug crypto socket	Displays communication between the client and IPSec during policy setup and removal processes.

debug dmvpn

To display debug Dynamic Multipoint VPN (DMVPN) session information, use the **debug dmvpn** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug dmvpn {**all** | **error** | **detail** | **packet**} {**all** | *debug-type*}

no debug dmvpn {**all** | **error** | **detail** | **packet**} {**all** | *debug-type*}

Syntax Description

all	Enables all levels of debugging.
error	Enables error-level debugging.
detail	Enables detail-level debugging.
packet	Enables packet-level debugging.
all	Enables NHRP, sockets, tunnel protection, and crypto debugging.
debug-type	The type of debugging that you want to enable. The following keywords can be specified for the *debug-type* argument: • **nhrp** — Enables Next Hop Resolution Protocol (NHRP) debugging only. • **crypto** — Enables crypto Internet Key Exchange (IKE) and IPsec debugging. • **tunnel** — Enables tunnel protection debugging. • **socket** — Enables crypto secure socket debugging. The keywords can be used alone, or in any combination with each other, but each keyword can be used only once.

Command Default

DMVPN debugging is disabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.5	This command was modified. This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

You must specify both the level and the type of debugging that you want to enable. The debugging levels are all, error, detail, or packet. You can enable NHRP, crypto Internet Key Exchange (IKE) and IPsec, tunnel protection, and crypto secure socket debugging at any of the four debugging levels.

To enable conditional DMVPN debugging, you must first specify the level and type of debugging that you want to enable, and then use the **debug dmvpn condition** command to specify the conditions that you want to enable.

Error-Level Debugging

When error-level debugging is enabled with the **debug dmvpn error** command, the following debugging commands are enabled by default:

- **debug crypto ipsec error**
- **debug crypto isakmp error**
- **debug nhrp error**

Detail-Level Debugging

When detail-level debugging is enabled with the **debug dmvpn detail** command, the following debugging commands are enabled by default:

- **debug crypto ipsec**
- **debug crypto isakmp**
- **debug crypto sockets**
- **debug nhrp**
- **debug nhrp cache**
- **debug nhrp rate**
- **debug tunnel protection**

Packet-Level Debugging

When packet-level debugging is enabled with the **debug dmvpn packet** command, the following debugging commands are enabled by default:

- **debug nhrp extension**
- **debug nhrp packet**

Note Executing the **debug dmvpn all** command with a high number of active sessions may result in high CPU utilization and large data output.

NHRP Shortcut Route Debugging

When shortcut switching is enabled on the router, the system looks up the NHRP shortcut route in the Routing Information Base (RIB) in order to forward the packet to the next-hop in the DMVPN cloud.

Table 14 describes the debug messages displayed by the router when shortcut switching and NHRP debugging are both enabled.

Table 14 ***Sample Messages for Shortcut Switching and NHRP***

Event	Sample Message

NHRP successfully adds a route to the RIB	`*Feb 21 13:11:24.043: NHRP: Adding route entry for 172.16.99.0 to RIB`
	`*Feb 21 13:11:24.043: NHRP: Route addition to RIB successful`

NHRP is unable to add a route to the RIB	`*Feb 21 13:11:24.043: NHRP: Adding route entry for 172.16.99.0 to RIB`
	`*Feb 21 13:11:24.043: NHRP: Route addition to RIB failed`

NHRP removes a route from the RIB	`*Feb 21 13:11:24.043: NHRP: Deleting route entry for 172.16.99.0 from RIB`
NHRP evicts a route from the RIB	`*Mar 1 18:24:29.371: NHRP: Route entry 172.16.22.0/24 clobbered by distance`
NHRP changes the administrative distance	`*Mar 1 00:14:16.799: NHRP: Administrative distance changed to 240`

Examples

The following example shows how to enable all debugging levels for DMVPN tunnel debugging:

```
Router# debug dmvpn all tunnel
```

Related Commands

Command	Description
debug crypto error	Enables error debugging for a crypto area.
debug crypto ipsec	Displays IPsec events.
debug crypto isakmp	Displays messages about IKE events.
debug dmvpn condition	Display conditional debug DMVPN session information.
debug nhrp condition	Enables NHRP conditional debugging.
debug nhrp error	Displays NHRP error-level debugging information.

debug dmvpn condition

To display conditional debug Dynamic Multipoint VPN (DMVPN) session information, use the **debug dmvpn condition** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug dmvpn condition {**unmatched** | **peer** {**nbma** | **tunnel** {*ipv4-address* | *ipv6-address*}} | **vrf** *vrf-name* | **interface tunnel** *tunnel-interface*}

no debug dmvpn condition [**unmatched** | **peer** {**nbma** | **tunnel** {*ipv4-address* | *ipv6-address*}} | **vrf** *vrf-name* | **interface tunnel** *number*]

Syntax Description

unmatched	Specifies debugging when context information is not available.
peer	Specifies information for a specific DMVPN peer.
nbma	Displays DMVPN information based on the peer mapping nonbroadcast access (NBMA) address.
tunnel	Displays DMVPN information based on the peer Virtual Private Network (VPN) address.
ipv4-address	The DMVPN peer IPv4 address.
ipv6-address	The DMVPN peer IPv6 address. **Note** Cisco IOS XE Release 2.5 does not support the *ipv6-address* argument.
vrf	Displays information based on the specified virtual routing and forwarding (VRF) name.
vrf-name	The VRF name.
interface	Displays DMVPN information based on a specific interface.
tunnel	Specifies the tunnel address for a DMVPN peer.
number	The tunnel interface number.

Command Default

DMVPN conditional debugging is disabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	The *ipv6-address* argument was added.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

Conditional debugging is enabled only after the DMVPN debugging type and level have been specified using the **debug dmvpn** command.

Console Output

The following **debug dmvpn** commands do not have any console output on the Cisco 3845 and Cisco 7200 series routers:

- **debug dmvpn condition interface**
- **debug dmvpn condition peer**
- **debug dmvpn condition unmatched**
- **debug dmvpn condition vrf**

Note When the **debug dmvpn condition unmatched** command is enabled on the Cisco 3845 and Cisco 7200 series routers, issuing the **show debugging** command does not produce any console output.

Examples

The following example shows how to enable conditional DMVPN debugging for a specific peer NBMA address:

```
Router# debug dmvpn condition peer nbma 192.0.2.1
```

The following example shows how to enable conditional DMVPN debugging when context is not available to check against debugging conditions:

```
Router# debug dmvpn condition unmatched
```

The following example shows how to disable conditional debugging for a specific tunnel interface:

```
Router# no debug dmvpn condition interface tunnel 1
```

The following example shows how to disable all conditional debugging:

```
Router# no debug dmvpn condition
```

Related Commands

Command	Description
debug crypto error	Enables error debugging for a crypto area.
debug crypto ipsec	Displays IPsec events.
debug crypto isakmp	Displays messages about IKE events.
debug dmvpn	Displays debug DMVPN session information.
debug nhrp condition	Enables NHRP conditional debugging.
debug nhrp error	Displays NHRP error-level debugging information.

debug eigrp fsm

To display debugging information about Enhanced Interior Gateway Routing Protocol (EIGRP) feasible successor metrics (FSMs), use the **debug eigrp fsm** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug eigrp fsm

no debug eigrp fsm

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.4(6)T	Support for IPv6 was added.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

This command helps you observe EIGRP feasible successor activity and to determine whether route updates are being installed and deleted by the routing process.

Examples

The following is sample output from the **debug eigrp fsm** command:

```
Router# debug eigrp fsm

DUAL: dual_rcvupdate(): 172.25.166.0 255.255.255.0 via 0.0.0.0 metric 750080/0
DUAL: Find FS for dest 172.25.166.0 255.255.255.0. FD is 4294967295, RD is 42949
67295 found
DUAL: RT installed 172.25.166.0 255.255.255.0 via 0.0.0.0
DUAL: dual_rcvupdate(): 192.168.4.0 255.255.255.0 via 0.0.0.0 metric 4294967295/
4294967295
DUAL: Find FS for dest 192.168.4.0 255.255.255.0. FD is 2249216, RD is 2249216
DUAL:   0.0.0.0 metric 4294967295/4294967295not found Dmin is 4294967295
DUAL: Dest 192.168.4.0 255.255.255.0 not entering active state.
DUAL: Removing dest 192.168.4.0 255.255.255.0, nexthop 0.0.0.0
DUAL: No routes. Flushing dest 192.168.4.0 255.255.255.0
```

In the first line, DUAL stands for diffusing update algorithm. It is the basic mechanism within EIGRP that makes the routing decisions. The next three fields are the Internet address and mask of the destination network and the address through which the update was received. The metric field shows the metric stored in the routing table and the metric advertised by the neighbor sending the information. If shown, the term “Metric... inaccessible” usually means that the neighbor router no longer has a route to the destination, or the destination is in a hold-down state.

In the following output, EIGRP is attempting to find a feasible successor for the destination. Feasible successors are part of the DUAL loop avoidance methods. The FD field contains more loop avoidance state information. The RD field is the reported distance, which is the metric used in update, query, or reply packets.

The indented line with the "not found" message means a feasible successor (FS) was not found for 192.168.4.0 and EIGRP must start a diffusing computation. This means it begins to actively probe (sends query packets about destination 192.168.4.0) the network looking for alternate paths to 192.164.4.0.

```
DUAL: Find FS for dest 192.168.4.0 255.255.255.0. FD is 2249216, RD is 2249216
DUAL:   0.0.0.0 metric 4294967295/4294967295not found Dmin is 4294967295
```

The following output indicates the route DUAL successfully installed into the routing table:

```
DUAL: RT installed 172.25.166.0 255.255.255.0 via 0.0.0.0
```

The following output shows that no routes to the destination were discovered and that the route information is being removed from the topology table:

```
DUAL: Dest 192.168.4.0 255.255.255.0 not entering active state.
DUAL: Removing dest 192.168.4.0 255.255.255.0, nexthop 0.0.0.0
DUAL: No routes. Flushing dest 192.168.4.0 255.255.255.0
```

debug eigrp neighbor

To display neighbors discovered by the Enhanced Interior Gateway Routing Protocol (EIGRP), use the **debug eigrp neighbor** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug eigrp neighbor [**siatimer**] [**static**]

no debug eigrp neighbor [**siatimer**] [**static**]

Syntax Description

siatimer	(Optional) Stuck-in-active (SIA) timer messages.
static	(Optional) Static routes.

Command Default

Debugging for EIGRP neighbors is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.4(6)T	Support for IPv6 was added.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Examples

The following is sample output from the **debug eigrp neighbor** command:

```
Router# debug eigrp neighbor static

EIGRP Static Neighbors debugging is on

Router# configure terminal

Router(config)# router eigrp 100

Router(config-router)# neighbor 10.1.1.1 e3/1

Router(config-router)#
22:40:07:EIGRP:Multicast Hello is disabled on Ethernet3/1!
22:40:07:EIGRP:Add new static nbr 10.1.1.1 to AS 100 Ethernet3/1

Router(config-router)# no neighbor 10.1.1.1 e3/1

Router(config-router)#
22:41:23:EIGRP:Static nbr 10.1.1.1 not in AS 100 Ethernet3/1 dynamic list
22:41:23:EIGRP:Delete static nbr 10.1.1.1 from AS 100 Ethernet3/1
22:41:23:EIGRP:Multicast Hello is enabled on Ethernet3/1!
```

Related Commands

Command	Description
neighbor	Defines a neighboring router with which to exchange routing information.
show ip eigrp neighbors	Displays EIGRP neighbors.
show ipv6 eigrp neighbors	Displays IPv6 EIGRP neighbors.

debug eigrp packet

To display debugging information for Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 packets, use the **debug eigrp packet** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug eigrp packet [**SIAquery** | **SIAreply** | **ack** | **hello** | **ipxsap** | **probe** | **query** | **reply** | **request** | **retry** | **stub** | **terse** | **update** | **verbose**]

no debug eigrp packet

Syntax Description

SIAquery	(Optional) Displays information about Stuck-in-Active (SIA) query messages.
SIAreply	(Optional) Displays information about SIA reply messages.
ack	(Optional) Displays information about EIGRP acknowledgment packets.
hello	(Optional) Displays information about EIGRP hello packets.
ipxsap	(Optional) Displays information about IPX EIGRP SAP packets.
probe	(Optional) Displays information about EIGRP probe packets.
query	(Optional) Displays information about EIGRP query packets.
reply	(Optional) Displays information about EIGRP reply packets.
request	(Optional) Displays information about EIGRP request packets.
retry	(Optional) Displays information about EIGRP retry packets.
stub	(Optional) Displays information about EIGRP stub packets.
terse	(Optional) Displays information about all EIGRP packets except Hello packets.
update	(Optional) Displays information about EIGRP update packets.
verbose	(Optional) Displays information about all EIGRP packets.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.4	The keywords were supported.
12.4(6)T	Support for IPv6 was added.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

If a communication session is closing when it should not be, an end-to-end connection problem can be the cause. The **debug eigrp packet** command is useful for analyzing the messages traveling between the local and remote hosts.

Note Although this command accepts a number of keywords, we don’t recommend their use unless directed by TAC.

Examples

The following is sample output from the **debug eigrp packet** command:

```
Router# debug eigrp packet

EIGRP: Sending HELLO on Ethernet0/1
       AS 109, Flags 0x0, Seq 0, Ack 0
EIGRP: Sending HELLO on Ethernet0/1
       AS 109, Flags 0x0, Seq 0, Ack 0
EIGRP: Sending HELLO on Ethernet0/1
       AS 109, Flags 0x0, Seq 0, Ack 0
EIGRP: Received UPDATE on Ethernet0/1 from 192.195.78.24,
       AS 109, Flags 0x1, Seq 1, Ack 0
EIGRP: Sending HELLO/ACK on Ethernet0/1 to 192.195.78.24,
       AS 109, Flags 0x0, Seq 0, Ack 1
EIGRP: Sending HELLO/ACK on Ethernet0/1 to 192.195.78.24,
       AS 109, Flags 0x0, Seq 0, Ack 1
EIGRP: Received UPDATE on Ethernet0/1 from 192.195.78.24,
       AS 109, Flags 0x0, Seq 2, Ack 0
```

The output shows transmission and receipt of EIGRP packets. These packet types may be hello, update, request, query, or reply packets. The sequence and acknowledgment numbers used by the EIGRP reliable transport algorithm are shown in the output. Where applicable, the network-layer address of the neighboring router is also included.

Table 15 describes the significant fields shown in the display.

Table 15 debug eigrp packet Field Descriptions

Field	Description
EIGRP:	EIGRP packet information.
AS n	Autonomous system number.
Flags 0x0	A flag of 1 means the sending router is indicating to the receiving router that this is the first packet it has sent to the receiver. A flag of 2 is a multicast that should be conditionally received by routers that have the conditionally receive (CR) bit set. This bit gets set when the sender of the multicast has previously sent a sequence packet explicitly telling it to set the CR bit.
HELLO	Hello packets are the neighbor discovery packets. They are used to determine whether neighbors are still alive. As long as neighbors receive the hello packets the router is sending, the neighbors validate the router and any routing information sent. If neighbors lose the hello packets, the receiving neighbors invalidate any routing information previously sent. Neighbors also send hello packets.

debug eigrp transmit

To display transmittal messages sent by the Enhanced Interior Gateway Routing Protocol (EIGRP), use the **debug eigrp transmit** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug eigrp transmit [**ack**] [**build**] [**detail**] [**link**] [**packetize**] [**peerdown**] [**sia**] [**startup**] [**strange**]

no debug eigrp transmit [**ack**] [**build**] [**detail**] [**link**] [**packetize**] [**peerdown**] [**sia**] [**startup**] [**strange**]

Syntax Description

ack	(Optional) Information for acknowledgment (ACK) messages sent by the system.
build	(Optional) Build information messages (messages that indicate that a topology table was either successfully built or could not be built).
detail	(Optional) Additional detail for debug output.
link	(Optional) Information regarding topology table linked-list management.
packetize	(Optional) Information regarding topology table linked-list management.
peerdown	(Optional) Information regarding the impact on packet generation when a peer is down.
sia	(Optional) Stuck-in-active (SIA) messages.
startup	(Optional) Information regarding peer startup and initialization packets that have been transmitted.
strange	(Optional) Unusual events relating to packet processing.

Command Default

Debugging for EIGRP transmittal messages is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1	This command was introduced.
12.4(6)T	Support for IPv6 was added.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Examples

The following is sample output from the **debug eigrp transmit** command:

```
Router# debug eigrp transmit
```

```
EIGRP Transmission Events debugging is on
    (ACK, PACKETIZE, STARTUP, PEERDOWN, LINK, BUILD, STRANGE, SIA, DETAIL)

Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router#(config)# router eigrp 100
Router#(config-router)# network 10.4.9.0 0.0.0.255
Router#(config-router)#
5d22h: DNDB UPDATE 10.0.0.0/8, serno 0 to 1, refcount 0
Router#(config-router)#
```

debug fm ipv6 pbr

To enable IPv6 policy-based routing debugging, use the **debug fm ipv6 pbr** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug fm ipv6 policy [**all** | **events** | **vmrs**]

no debug fm ipv6 policy [**all** | **events** | **vmrs**]

Syntax Description

all	(Optional) Displays all PBR debugging information.
events	(Optional) Displays debugging information about PBR events.
vmrs	(Optional) Displays debugging information about PBR value mask results (VMRs).

Command Default

IPv6 policy-based routing debugging information is not displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SXI4	This command was introduced.

Usage Guidelines

Do not use the **debug fm ipv6 pbr** command unless you suspect a problem with IPv6 policy-based routing.

Examples

The following example enables IPv6 PBR debugging information:

```
Router# debug fm ipv6 pbr
```

debug fm raguard

To display information about router advertisement (RA) guard debugging activity, use the **debug fm raguard** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug fm raguard [**all** | **events** | **error** | **unusual** | **vmr**]

no debug fm raguard

Syntax Description

all	(Optional) All RA guard debugging information is displayed.
events	(Optional) Information about RA guard debugging events is displayed.
error	(Optional) Information about RA guard debugging errors is displayed.
unusual	(Optional) Information about unusual RA guard debugging events is displayed.
vmr	(Optional) Information about debugging value mask results (VMRs) is displayed.

Command Default

RA guard debugging information is not displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SXI4	This command was introduced.
12.2(54)SG	This command was modified. Support for Cisco IOS Release 12.2(54)SG was added.
12.2(50)SY	This command was modified. The **unusual** keyword was added.

Usage Guidelines

Do not use the **debug fm raguard** command unless you suspect a problem with IPv6 RA guard.

Examples

The following example enables you to view IPv6 RA guard debugging activity:

```
Router# debug fm raguard
```

debug ip flow cache

To enable debugging output for NetFlow cache, use the **debug ip flow cache** command in user EXEC or privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ip flow cache

no debug ip flow cache

Syntax Description

This command has no arguments or keywords.

Command Default

Debugging output for NetFlow data export is disabled.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(1)	This command was introduced.
12.3(1)	Debugging output for NetFlow v9 data export was added.
12.3(7)T	Debugging output for NetFlow for IPv6 was added.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following is sample output from the **debug ip flow export** command:

```
Router# debug ip flow cache
IP Flow cache allocation debugging is on

Router# show ipv6 flow

IP packet size distribution (0 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 0 bytes
  0 active, 0 inactive, 0 added
  0 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
SrcAddress                                  InpIf    DstAddress
                OutIf    Prot SrcPrt DstPrt Packets
c7200-vxr-2#
```

```
000037: 01:56:26: IPFLOW: Allocating Sub-Flow cache, without hash flags.
000038: 01:56:26: IPFLOW: Sub-Flow table enabled.
000039: 01:56:26: IPFLOW: Sub-Flow numbers are:
    24 sub-flows per chunk, 0 hashflag len,
    1 chunks allocated, 12 max chunks,
    24 allocated records, 24 free records, 960 bytes allocated
000040: 01:56:26: IPFLOW: Sub-Flow cache removed
```

Related Commands

Command	Description
export destination	Enables the exporting of information from NetFlow aggregation caches.
ip flow-aggregation cache	Enables NetFlow aggregation cache schemes.
ip flow-export	Enables the exporting of information in NetFlow cache entries.
ipv6 flow-aggregation cache	Enables NetFlow aggregation cache schemes for IPv6 configurations.
ipv6 flow export	Enables the exporting of information in NetFlow cache entries for IPv6 NetFlow configurations.
show ip cache flow aggregation	Displays the NetFlow aggregation cache configuration.
show ip flow export	Display the statistics for NetFlow data export.

debug ip flow export

To enable debugging output for NetFlow data export, use the **debug ip flow export** command in user EXEC or privileged EXEC mode. To disable debugging output for NetFlow data export, use the **no** form of this command.

debug ip flow export

no debug ip flow export

Syntax Description

This command has no keywords or arguments.

Command Default

Debugging output for NetFlow data export is disabled.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(1)	This command was introduced.
12.3(1)	Debugging output for NetFlow v9 data export was added.
12.3(7)T	This command was modified so that NetFlow v9 data is collected for both IPv4 and IPv6.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following is sample output from the **debug ip flow export** command:

```
Router# debug ip flow export

IP Flow export mechanism debugging is on
*Mar 6 22:56:21.627:IPFLOW:Sending export pak to 2001::FFFE/64 port 9999
*Mar 6 22:56:21.627:IPFLOW:Error sending export packet:Adjacency failure
```

Related Commands

Command	Description
export destination	Enables the exporting of information from NetFlow aggregation caches.
ipv6 flow-aggregation cache	Enables NetFlow aggregation cache schemes for IPv6.
ipv6 flow-export	Enables the exporting of information in NetFlow cache entries.

Command	Description
show ip cache flow aggregation	Displays the NetFlow accounting aggregation cache statistics.
show ip flow export	Displays the statistics for NetFlow data export.
show ipv6 flow export	Displays the statistics for NetFlow data export for IPv6.

debug ipv6 cef drop

To display debug messages for Cisco Express Forwarding for IPv6 (CEFv6) and distributed CEFv6 (dCEFv6) dropped packets, use the **debug ipv6 cef drop** command in privileged EXEC mode. To disable debug messages for CEFv6 and dCEFv6 dropped packets, use the **no** form of this command.

debug ipv6 cef drop [**rpf**]

no debug ipv6 cef drop

Syntax Description

rpf	(Optional) Displays packets dropped by the IPv6 CEF Unicast Reverse-Path Forwarding (Unicast RPF) feature.

Command Default

Debugging for CEFv6 and dCEFv6 dropped packets is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(25)S	The **rpf** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **debug ipv6 cef drop** command is similar to the **debug ip cef drops** command, except that it is IPv6-specific.

Note By default, the network server sends the output from **debug** commands and system error messages to the console. To redirect debug output, use the **logging** command options in global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on **debug** commands and redirecting debug output, refer to the Release 12.3 *Cisco IOS Debug Command Reference*.

Examples

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

```
Router# debug ipv6 cef drop

*Aug 30 08:20:51.169: IPv6-CEF: received packet on Serial6/0/2
*Aug 30 08:20:51.169: IPv6-CEF: found no adjacency for 2001:0DB8::1 reason 2
*Aug 30 08:20:51.169: IPv6-CEF: packet not switched: code 0x1
```

Table 16 describes the significant fields shown in the display.

Table 16 debug ipv6 cef drop Field Descriptions

Field	Description
IPv6-CEF: received packet on Serial6/0/2	Cisco Express Forwarding has received a packet addressed to the router via serial interface 6/0/2.
IPv6-CEF: found no adjacency for 2001:0DB8::1	Cisco Express Forwarding has found no adjacency for the IPv6 address prefix of 2001:0DB8::1.
IPv6-CEF: packet not switched	Cisco Express Forwarding has dropped the packet.

Related Commands

Command	Description
debug ipv6 cef events	Displays debug messages for CEFv6 and dCEFv6 general events.
debug ipv6 cef table	Displays debug messages for CEFv6 and dCEFv6 table modification events.

debug ipv6 cef events

To display debug messages for Cisco Express Forwarding for IPv6 (CEFv6) and distributed CEFv6 (dCEFv6) general events, use the **debug ipv6 cef events** command in privileged EXEC mode. To disable debug messages for CEFv6 and dCEFv6 general events, use the **no** form of this command.

debug ipv6 cef events

no debug ipv6 cef events

Syntax Description

This command has no arguments or keywords.

Command Default

Debugging for CEFv6 and dCEFv6 general events is not enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **debug ipv6 cef events** command is similar to the **debug ip cef events** command, except that it is IPv6-specific.

Note By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options in global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on **debug** commands and redirecting debug output, refer to the Release 12 *Cisco IOS Debug Command Reference*.

Examples

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

```
Router# debug ipv6 cef events

IPv6 CEF packet events debugging is on
Router#
*Aug 30 08:22:57.809: %LINK-3-UPDOWN: Interface Serial6/0/2, changed state to up
*Aug 30 08:22:58.809: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial6/0/2, changed
state to up
*Aug 30 08:23:00.821: CEFv6-IDB: Serial6/0/2 address 2001:0DB8::248 add download succeeded
```

Table 17 describes the significant fields shown in the display.

Table 17 debug ipv6 cef events Field Descriptions

Field	Description
Interface Serial6/0/2, changed state to up	Indicates that the interface hardware on serial interface 6/0/2 is currently active.
Line protocol on Interface Serial6/0/2, changed state to up	Indicates that the software processes that handle the line protocol consider the line usable for serial interface 6/0/2.
Serial6/0/2 address 2001:0DB8::248 add download succeeded	The IPv6 address 2001:0DB8::248 was downloaded successfully.

Related Commands

Command	Description
debug ipv6 cef table	Displays debug messages for CEFv6 and dCEFv6 table modification events.

debug ipv6 cef hash

To display debug messages for Cisco Express Forwarding for IPv6 (CEFv6) and distributed CEFv6 (dCEFv6) load-sharing hash algorithm events, use the **debug ipv6 cef hash** command in privileged EXEC mode. To disable debug messages for CEFv6 and dCEFv6 load-sharing hash algorithm events, use the **no** form of this command.

debug ipv6 cef hash

no debug ipv6 cef hash

Syntax Description

This command has no arguments or keywords.

Command Default

Debugging for CEFv6 and dCEFv6 load-sharing hash algorithm events is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **debug ipv6 cef hash** command is similar to the **debug ip cef hash** command, except that it is IPv6-specific.

Use this command when changing the load-sharing algorithm to display IPv6 hash table details.

Note By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options in global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server.

Related Commands

Command	Description
debug ipv6 cef events	Displays debug messages for CEFv6 and dCEFv6 general events.
debug ipv6 cef table	Displays debug messages for CEFv6 and dCEFv6 table modification events.

debug ipv6 cef receive

To display debug messages for Cisco Express Forwarding for IPv6 (CEFv6) and distributed CEFv6 (dCEFv6) packets that are process-switched on the router, use the **debug ipv6 cef receive** command in privileged EXEC mode. To disable debug messages for CEFv6 and dCEFv6 packets that are process-switched on the router, use the **no** form of this command.

debug ipv6 cef receive

no debug ipv6 cef receive

Syntax Description

This command has no arguments or keywords.

Command Default

Debugging for CEFv6 and dCEFv6 packets that are process-switched on the router is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **debug ipv6 cef receive** command is similar to the **debug ip cef receive** command, except that it is IPv6-specific.

Note By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options in global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on debug commands and redirecting debug output, refer to the Release 12 *Cisco IOS Debug Command Reference*.

Examples

The following is sample output from the **debug ipv6 cef receive** command when another router in the network pings 2001:0DB8::2 which is a local address on this box:

```
Router# debug ipv6 cef receive

IPv6 CEF packet receives debugging is on
router#
*Aug 30 08:25:14.869: IPv6CEF-receive: Receive packet for 2001:0DB8::2
```

```
*Aug 30 08:25:14.897: IPv6CEF-receive: Receive packet for 2001:0DB8::2
*Aug 30 08:25:14.925: IPv6CEF-receive: Receive packet for 2001:0DB8::2
*Aug 30 08:25:14.953: IPv6CEF-receive: Receive packet for 2001:0DB8::2
*Aug 30 08:25:14.981: IPv6CEF-receive: Receive packet for 2001:0DB8::2
```

Table 18 describes the significant fields shown in the display.

Table 18 debug ipv6 cef receive Field Descriptions

Field	Description
IPv6CEF-receive: Receive packet for 2001:0DB8::2	Cisco Express Forwarding has received a packet addressed to the router.

Related Commands

Command	Description
debug ipv6 cef events	Displays debug messages for CEFv6 and dCEFv6 general events.
debug ipv6 cef table	Displays debug messages for CEFv6 and dCEFv6 table modification events.

debug ipv6 cef table

To display debug messages for Cisco Express Forwarding for IPv6 (CEFv6) and distributed CEFv6 (dCEFv6) table modification events, use the **debug ipv6 cef table** command in privileged EXEC mode. To disable debug messages for CEFv6 and dCEFv6 table modification events, use the **no** form of this command.

debug ipv6 cef table [**background**]

no debug ipv6 cef table [**background**]

Syntax Description

background	(Optional) Sets CEFv6 and dCEFv6 table background updates.

Command Default

Debugging for CEFv6 and dCEFv6 table modification events is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **debug ipv6 cef table** command is similar to the **debug ip cef table** command, except that it is IPv6-specific.

This command is used to record CEFv6 and dCEFv6 table events related to the Forwarding Information Base (FIB) tables. Types of events include the following:

- Routing updates that populate the FIB tables
- Flushing of the FIB tables
- Adding or removing of entries to the FIB tables
- Table reloading process

Note By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options in global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on debug commands and redirecting debug output, refer to the *Cisco IOS Debug Command Reference*.

Examples

The following is sample output from the **debug ipv6 cef table** command when a static route is added:

```
Router# debug ipv6 cef table

IPv6 CEF table debugging is on

router(config)# ipv6 route 5555::/64 serial 2/0 3000::2
router(config)#
*Feb 24 08:46:09.187: IPv6CEF-Table: Event add, 5555::/64
*Feb 24 08:46:09.187: IPv6 CEF table: Created path_list 01184570
*Feb 24 08:46:09.187: IPv6 CEF table: Adding path 01181A80 to path_list 01184570 old path
count=0
*Feb 24 08:46:09.187: IPv6 CEF table: No matching list for path list 01184570
*Feb 24 08:46:09.187: IPv6 CEF table: Adding fib entry 0117EE80 to path_list 01184570 old
refcount=0
*Feb 24 08:46:09.187: IPv6 CEF table: Added path_list 01184570 to hash 50
*Feb 24 08:46:09.187: IPv6 CEF: Linking path 01181A80 to adjacency 01138E28
*Feb 24 08:46:09.187: IPv6 CEF table: Created 0 loadinfos for path_list 01184570
*Feb 24 08:46:09.187: IPv6CEF-Table: Validated 5555::/64
```

The following is sample output when the static route is removed:

```
router(config)# no ipv6 route 5555::/64 serial 2/0 3000::2
router(config)#
*Feb 24 08:46:43.871: IPv6CEF-Table: Event delete, 5555::/64
*Feb 24 08:46:43.871: IPv6CEF-Table: Invalidated 5555::/64
*Feb 24 08:46:43.871: IPv6CEF-Table: Deleted 5555::/64
*Feb 24 08:46:43.871: IPv6 CEF table: Removing fib entry 0117EE80 from path_list 01184570
old refcount=1
*Feb 24 08:46:43.871: IPv6 CEF table: Removed path_list 01184570 from hash 50
*Feb 24 08:46:43.871: IPv6 CEF table: Freeing path_list 01184570 refcount=0
*Feb 24 08:46:43.871: IPv6 CEF table: Freeing all 1 paths in path_list 01184570
*Feb 24 08:46:43.871: IPv6 CEF: deleting path 01181A80
```

Related Commands

Command	Description
debug ipv6 cef events	Displays debug messages for CEFv6 and dCEFv6 general events.

debug fm raguard

To enable debugging for IPv6 router advertisement (RA) guard, use the **debug fm raguard** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug fm raguard [**all** | **error** | **events** | **vmr**]

no debug fm raguard

Syntax Description

all	(Optional) Displays all RA guard information.
error	(Optional) Displays information about RA guard errors.
events	(Optional) Displays information about RA guard events.
vmr	(Optional) Displays information about variable-rate multimode (VMR) generation in RA guard.

Command Default

Debugging for the DHCP for IPv6 is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

The **debug fm raguard** command is used to show debug information related to the RA guard.

Examples

The following example enables debugging for RA guard for IPv6:

```
Router# debug fm raguard
```

debug ipv6 dhcp database

To enable debugging for the Dynamic Host Configuration Protocol (DHCP) for IPv6 binding database agent, use the **debug ipv6 dhcp database** command in privileged EXEC mode. To disable the display of debug messages for the DHCP for IPv6 binding database agent, use the **no** form of this command.

debug ipv6 dhcp database

no debug ipv6 dhcp database

Syntax Description

This command has no keywords or arguments.

Command Default

Debugging for the DHCP for IPv6 binding database agent is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The **debug ipv6 dhcp database** command enables debugging for DHCP for IPv6 database processing.

Examples

The following example enables debugging for the DHCP for IPv6 binding database agent:

```
Router# debug ipv6 dhcp database
```

Related Commands

Command	Description
debug ipv6 dhcp	Enables debugging for DHCP for IPv6.

debug ipv6 dhcp relay

To enable DHCP for IPv6 relay agent debugging, use the **debug ipv6 dhcp relay** command in user EXEC or privileged EXEC mode. To disable DHCP for IPv6 relay agent debugging, use the **no** form of this command.

debug ipv6 dhcp relay [**bulk-lease**]

no debug ipv6 dhcp relay [**bulk-lease**]

Syntax Description

bulk-lease	(Optional) Enables bulk lease query debugging flows.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(11)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.1(1)S	This command was modified. The **bulk-lease** keyword was added.

Usage Guidelines

The DHCP functions for IPv6 client, server, and relay agent are mutually exclusive on an interface. When one of these functions is enabled and a user tries to configure a different function on the same interface, one of the following messages is displayed: Interface is in DHCP client mode, Interface is in DHCP server mode, or Interface is in DHCP relay mode.

Examples

The following example enables DHCP for IPv6 relay agent debugging:

```
Router# debug ipv6 dhcp relay
```

Related Commands

Command	Description
debug ipv6 dhcp	Enables DHCP debugging for IPv6.

debug ipv6 eigrp

To display information about the Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 protocol, use the **debug ipv6 eigrp** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 eigrp [*as-number*] [**neighbor** *ipv6-address* | **notification** | **summary**]

no debug ipv6 eigrp

Syntax Description

as-number	(Optional) Autonomous system number.
neighbor *ipv6-address*	(Optional) IPv6 address of the neighboring router.
notification	(Optional) Displays EIGRP for IPv6 events and notifications in the console of the router.
summary	(Optional) Displays a summary of EIGRP for IPv6 routing information.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Because the **debug ipv6 eigrp** command generates a substantial amount of output, use it only when traffic on the network is light.

Examples

The following example enables debugging output:

```
Router# debug ipv6 eigrp
```

debug ipv6 icmp

To display debugging messages for IPv6 Internet Control Message Protocol (ICMP) transactions (excluding IPv6 ICMP neighbor discovery transactions), use the **debug ipv6 icmp** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 icmp

no debug ipv6 icmp

Syntax Description

This command has no arguments or keywords.

Command Default

Debugging for IPv6 ICMP is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command's output was modified on the Cisco 10000 series router for the PRE3 and PRE4.

Usage Guidelines

The **debug ipv6 icmp** command is similar to the **debug ip icmp** command, except that it is IPv6-specific.

Note By default, the network server sends the output from **debug** commands and system error messages to the console. To redirect debugging output, use the logging command options in global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server.

This command helps you determine whether the router is sending or receiving IPv6 ICMP messages. Use it, for example, when you are troubleshooting an end-to-end connection problem.

Note For more information about the fields in **debug ipv6 icmp** output, refer to RFC 2463, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6).*

Cisco 10000 Series Router Usage Guidelines

In Cisco IOS Release 12.2(33)SB, output from the **debug ipv6 icmp** command displays information similar to the following:

```
ICMPv6: Received echo reply from 2010:1:1:1:1:1:1:2
```

In Cisco IOS Release 12.2(31)SB, the **debug ipv6 icmp** command output displays information similar to the following:

```
ICMPv6: Received ICMPv6 packet from 2010:1:1:1:1:1:1:2, type 129
```

Examples

The following is sample output from the **debug ipv6 icmp** command:

```
Router# debug ipv6 icmp

13:28:40:ICMPv6:Received ICMPv6 packet from 2000:0:0:3::2, type 136
13:28:45:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 135
13:28:50:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 136
13:28:55:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 135
```

Table 19 describes significant fields shown in the first line of the display.

Table 19 debug ipv6 icmp Field Descriptions

Field	Description
13:28:40:	Indicates the time (hours:minutes:seconds) at which the ICMP neighbor discovery event occurred.
*n*w*n*d: (not shown in sample output)	Indicates time (weeks, days) since last reboot of the event occurring. For example, 1w4d: indicates the time (since the last reboot) of the event occurring was 1 week and 4 days ago.
ICMPv6:	Indication that this message describes an ICMP version 6 packet.
Received ICMPv6 packet from 2000:0:0:3::2	IPv6 address from which the ICMP version 6 packet is received.
type 136	The number variable indicates one of the following IPv6 ICMP message types: • 1—Destination unreachable. The router cannot forward a packet that was sent or received. • 2—Packet too big. The router attempts to send a packet that exceeds the maximum transmission unit (MTU) of a link between itself and the packet destination. • 3—Time exceeded. Either the hop limit in transit or the fragment reassembly time is exceeded. • 4—Parameter problem. The router attempts to send an IPv6 packet that contains invalid parameters. An example is a packet containing a next header type unsupported by the router that is forwarding the packet. • 128—Echo request. The router received an echo reply. • 129—Echo reply. The router sent an echo reply. • 133—Router solicitation messages. Hosts send these messages to prompt routers on the local link to send router advertisement messages. • 134—Router advertisement messages. Routers periodically send these messages to advertise their link-layer addresses, prefixes for the link, and other link-specific information. These messages are also sent in response to router solicitation messages. • 135—Neighbor solicitation messages. Nodes send these messages to request the link-layer address of a station on the same link. • 136—Neighbor advertisement messages. Nodes send these messages, containing their link-local addresses, in response to neighbor solicitation messages. • 137—Redirect messages. Routers send these messages to hosts when a host attempts to use a less-than-optimal first hop address when forwarding packets. These messages contain a better first hop address that should be used instead.

Following are examples of the IPv6 ICMP messages types that can be displayed by the **debug ipv6 icmp** command:

- ICMP echo request and ICMP echo reply messages. In the following example, an ICMP echo request is sent to address 2052::50 and an ICMP echo reply is received from address 2052::50.

```
1w4d:ICMPv6:Sending echo request to 2052::50
1w4d:ICMPv6:Received echo reply from 2052::50
```

- ICMP packet too big messages. In the following example, a router tried to forward a packet to destination address 2052::50 via the next hop address 2052::52. The size of the packet was greater than 1280 bytes, which is the MTU of destination address 2052::50. As a result, the router receives an ICMP packet too big message from the next hop address 2052::52.

```
1w4d:Received ICMP too big from 2052::52 about 2052::50, MTU=1300
```

- ICMP parameter problem messages. In the following example, an ICMP parameter problem message is received from address 2052::52.

```
1w4d:Received ICMP parameter problem from 2052::52
```

- ICMP time exceeded messages. In the following example, an ICMP time exceeded message is received from address 2052::52.

```
1w4d:Received ICMP time exceeded from 2052::52
```

- ICMP unreachable messages. In the following example, an ICMP unreachable message with code 1 is received from address 2052::52. Additionally, an ICMP unreachable message with code 1 is sent to address 2060::20 about address 2062::20.

```
1w4d:Received ICMP unreachable code 1 from 2052::52
1w4d:Sending ICMP unreachable code 1 to 2060::20 about 2062::20
```

Table 20 lists the codes for ICMP unreachable messages.

Table 20 ICMP Unreachable Messages—Code Descriptions

Code	Description
0	The router has no route to the packet destination.
1	Although the router has a route to the packet destination, communication is administratively prohibited.
3	The address is unreachable.
4	The port is unreachable.

Related Commands

Command	Description
debug ipv6 nd	Displays debugging messages for IPv6 ICMP neighbor discovery transactions.

debug ipv6 inspect

To display messages about Cisco IOS firewall events, use the **debug ipv6 inspect** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 inspect {**function-trace** | **object-creation** | **object-deletion** | **events** | **timers** | **protocol** | **detailed**}

no debug ipv6 inspect detailed

Syntax Description

function-trace	Displays messages about software functions called by the Cisco IOS firewall.
object-creation	Displays messages about software objects being created by the Cisco IOS firewall. Object creation corresponds to the beginning of Cisco IOS firewall-inspected sessions.
object-deletion	Displays messages about software objects being deleted by the Cisco IOS firewall. Object deletion corresponds to the closing of Cisco IOS firewall-inspected sessions.
events	Displays messages about Cisco IOS firewall software events, including information about Cisco IOS firewall packet processing.
timers	Displays messages about Cisco IOS firewall timer events such as when a Cisco IOS firewall idle timeout is reached.
protocol	Displays messages about Cisco IOS firewall-inspected protocol events, including details about the protocol's packets.
detailed	Use this form of the command in conjunction with other Cisco IOS firewall debugging commands. This causes detailed information to be displayed for all the other enabled Cisco IOS firewall debugging.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following example enables the display of messages about Cisco IOS firewall events:

```
debug ipv6 inspect
```

Related Commands

Command	Description
ipv6 inspect audit-trail	Turns on CBAC audit trail messages, which are displayed on the console after each Cisco IOS firewall session closes.
ipv6 inspect name	Defines a set of ipv6 inspection rules.
show ipv6 inspect	Displays CBAC configuration and session information.

debug ipv6 mfib

To enable debugging output on the IPv6 Multicast Forwarding Information Base (MFIB), use the **debug ipv6 mfib** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 mfib [**vrf** *vrf-name*] [*group-name* | *group-address*] [**adjacency** | **db** | **fs** | **init** | **interface** | **mrib** [**detail**] | **nat** | **pak** | **platform** | **ppr** | **ps** | **signal** | **table**]

no debug ipv6 mfib

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
group-name | *group-address*	(Optional) IPv6 address, name, or interface of the multicast group as defined in the Domain Name System (DNS) hosts table.
adjacency	(Optional) Enables debugging output for adjacency management activity.
db	(Optional) Enables debugging output for route database management activity.
fs	(Optional) Enables debugging output for fast switching activity.
init	(Optional) Enables debugging output for initialization or deinitialization activity.
interface	(Optional) Enables debugging output for IPv6 MFIB interfaces.
mrib	(Optional) Enables debugging output for communication with the MRIB.
detail	(Optional) Enables detailed debugging output regarding the MRIB.
nat	(Optional) Enables debugging output for Network Address Translation (NAT) events associated with all tables.
pak	(Optional) Enables debugging output for packet forwarding activity.
platform	(Optional) Enables debugging output related to the hardware platform use of application program interfaces (APIs).
ppr	(Optional) Enables debugging output for packet preservation events.
ps	(Optional) Enables debugging output for process-level-only packet forwarding activity.
signal	(Optional) Enables debugging output for activity regarding MFIB data-driven signaling to routing protocols.
table	(Optional) Enables debugging output for IPv6 MFIB table activity.

Command Modes

Privileged EXEC

Syntax Description

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series routers.
12.2(33)SRE	The **detail** keyword was added.
15.1(1)T	The **detail** keyword was added.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

If no keywords are used, all IPbv6 MFIB activity debugging output is displayed.

Examples

The following example enables debugging output for adjacency management activity on the IPv6 MFIB:

```
Router# debug ipv6 mfib adjacency
```

debug ipv6 mld

To enable debugging on Multicast Listener Discovery (MLD) protocol activity, use the **debug ipv6 mld** command in privileged EXEC mode. To restore the default value, use the **no** form of this command.

debug ipv6 mld [*group-name* | *group-address* | *interface-type*]

no debug ipv6 mld [*group-name* | *group-address* | *interface-type*]

Cisco IOS Release 12.0(26)S

debug ipv6 mld [**group** *group-name* | *group-address* | **interface** *interface-type*]

no debug ipv6 mld [**group** *group-name* | *group-address* | **interface** *interface-type*]

Syntax Description

group-name | *group-address* or **group** *group-name* | *group-address*	(Optional) IPv6 address or name of the multicast group.
interface-type or **interface** *interface-type*	(Optional) Interface type. For more information, use the question mark (**?**) online help function.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

This command helps discover whether the MLD protocol activities are working correctly. In general, if MLD is not working, the router process never discovers that there is a host on the network that is configured to receive multicast packets.

The messages displayed by the **debug ipv6 mld** command show query and report activity received from other routers and hosts. Use this command in conjunction with **debug ipv6 pim** to display additional multicast activity, to learn more information about the multicast routing process, or to learn why packets are forwarded out of particular interfaces.

Examples

The following example enables debugging on MLD protocol activity:

```
Router# debug ipv6 mld
```

Related Commands

Command	Description
debug ipv6 pim	Enables debugging on PIM protocol activity.

debug ipv6 mld explicit

To display information related to the explicit tracking of hosts, use the **debug ipv6 mld explicit** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug ipv6 mld explicit [*group-name* | *group-address*]

no debug ipv6 mld explicit [*group-name* | *group-address*]

Syntax Description

group-name | *group-address*	(Optional) IPv6 address or name of the multicast group.

Command Default

Debugging for the explicit tracking of hosts is not enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

When the optional *group-name* or *group-address* argument is not used, all debugging information is displayed.

Examples

The following example shows how to enable information to be displayed about the explicit tracking of hosts. The command output is self-explanatory:

```
Router# debug ipv6 mld explicit
```

```
00:00:56:MLD:ET host FE80::A8BB:CCFF:FE00:800 report for FF05::6 (0 srcs) on Ethernet1/0
00:00:56:MLD:ET host FE80::A8BB:CCFF:FE00:800 switch to exclude for FF05::6 on Ethernet1/0
00:00:56:MLD:ET MRIB modify for (*,FF05::6) on Ethernet1/0 new 100, mdf 100
```

debug ipv6 mld ssm-map

To display debug messages for Source Specific Multicast (SSM) mapping related to Multicast Listener Discovery (MLD), use the **debug ipv6 mld ssm-map** command in privileged EXEC mode. To disable debug messages for SSM mapping, use the **no** form of this command.

debug ipv6 mld ssm-map [*source-address*]

no debug ipv6 mld ssm-map [*source-address*]

Syntax Description

source-address	(Optional) Source address associated with an MLD membership for a group identified by the access list.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Consult Cisco technical support before using this command.

Examples

The following example allows debugging information for SSM mapping to be displayed:

```
Router# debug ipv6 mld ssm-map
```

Related Commands

Command	Description
ipv6 mld ssm-map enable	Enables the SSM mapping feature for groups in the configured SSM range
ipv6 mld ssm-map query dns	Enables DNS-based SSM mapping.
ipv6 mld ssm-map static	Configures static SSM mappings.
show ipv6 mld ssm-map	Displays SSM mapping information.

debug ipv6 mobile

To enable the display of debugging information for Mobile IPv6, use the **debug ipv6 mobile** command in privileged EXEC mode.

debug ipv6 mobile {**binding-cache** | **forwarding** | **home-agent** | **registration**}

Syntax Description

binding-cache	Events associated with the binding cache.
forwarding	Events associated with forwarding (tunneling) packets for which the router is acting as home agent.
home-agent	Events associated with the home agent, Dynamic Home Address Agent Discovery (DHAAD), Mobile prefix discovery (MPD), and generic home agent (HA) debugging and binding acknowledgments.
registration	Events associated with binding updates that are registrations.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The **debug ipv6 mobile** command enables the display of selected debugging information. You may use multiple command lines to enable concurrent debugging of multiple classes of information.

Examples

In the following example, debugging information is displayed for binding updates processing:

```
Router# debug ipv6 mobile registration
```

Related Commands

Command	Description
binding	Configures binding options for the Mobile IPv6 home agent feature in home-agent configuration mode.
ipv6 mobile home-agent (global configuration)	Enters home agent configuration mode.
ipv6 mobile home-agent (interface configuration)	Initializes and start the IPv6 Mobile home agent on a specific interface.
ipv6 mobile home-agent preference	Configures the home agent preference value on the interface.

debug ipv6 mobile networks

To display debugging messages for IPv6 mobile networks, use the **debug ipv6 mobile networks** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 mobile networks

no debug ipv6 mobile networks

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The **debug ipv6 mobile networks** command enables the display of selected debugging information.

Examples

The following example shows how to enable the display of debugging messages for IPv6 mobile networks:

```
Router# debug ipv6 mobile networks
```

Related Commands

Command	Description
ipv6 mobile router	Enables IPv6 NEMO functionality on a router and places the router in IPv6 mobile router configuration mode.

debug ipv6 mobile router

To display debugging messages for the IPv6 mobile router, use the **debug ipv6 mobile router** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 mobile router [**detail**]

no debug ipv6 mobile router

Syntax Description

detail	(Optional) Displays detailed mobile router debug messages.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The IPv6 mobile router operations can be debugged. The following conditions trigger debugging messages:

- Agent discovery
- Registration
- Mobile router state change
- Routes and tunnels created or deleted
- Roaming information

Debugging messages are prefixed with “MobRtr,” and detail messages are prefixed with “MobRtrX.”

Examples

The following example shows how to enable the display of debugging messages for the IPv6 mobile router:

```
Router# debug ipv6 mobile router
```

Related Commands

Command	Description
ipv6 mobile router	Enables IPv6 NEMO functionality on a router and places the router in IPv6 mobile router configuration mode.

debug ipv6 mrib client

To enable debugging on Multicast Routing Information Base (MRIB) client management activity, use the **debug ipv6 mrib client** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 mrib [**vrf** *vrf-name*] **client**

no debug ipv6 mrib client

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **debug ipv6 mrib client** command is used to display the activity in the MRIB associated with clients such as Protocol Independent Multicast (PIM) and Multicast Listener Discovery (MLD). If you are having difficulty with your client connections, use this command to display new clients being added and deleted.

The **debug ipv6 mrib client** command also displays information on when a new client is added to or deleted from the MRIB, when a client connection is established or torn down, when a client binds to a particular MRIB table, and when a client is informed that there are updates to be read.

Examples

The following example enables debugging on MRIB client management activity:

```
Router# debug ipv6 mrib client
```

Related Commands

Command	Description
debug ipv6 mrib route	Displays MRIB routing entry-related activity.

debug ipv6 mrib io

To enable debugging on Multicast Routing Information Base (MRIB) I/O events, use the **debug ipv6 mrib io** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 mrib [**vrf** *vrf-name*] **io**

no debug ipv6 mrib io

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **debug ipv6 mrib io** command to display information on when clients open and close MRIB I/O connections, when MRIB entry and interface updates are received and processed from clients, and when MRIB entry and interface updates are sent to clients.

Examples

The following example enables debugging on MRIB I/O events:

```
Router# debug ipv6 mrib io
```

debug ipv6 mrib proxy

To enable debugging on multicast routing information base (MRIB) proxy activity between the route processor and line cards on distributed router platforms, use the **debug ipv6 mrib proxy** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 mrib proxy

no debug ipv6 mrib proxy

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Use the **debug ipv6 mrib proxy** command to display information on connections that are being opened and closed and on MRIB transaction messages that are being passed between the route processor and line cards.

Examples

The following example enables debugging on MRIB proxy events:

```
Router# debug ipv6 mrib proxy
```

debug ipv6 mrib route

To display information about Multicast Routing Information Base (MRIB) routing entry-related activity, use the **debug ipv6 mrib route** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 mrib [**vrf** *vrf-name*] **route** [*group-name* | *group-address*]

no debug ipv6 mrib route

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
group-name | *group-address*	(Optional) IPv6 address or name of the multicast group.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

This command displays update information related to the route database made by MRIB clients, which is then redistributed to the clients.

Use this command to monitor MRIB route activity when discontinuity is found between the MRIB and the client database or between the individual client databases.

Examples

The following example enables the display of information about MRIB routing entry-related activity:

```
Router# debug ipv6 mrib route
```

Related Commands

Command	Description
show ipv6 mrib client	Displays information about the MRIB client management activity.

debug ipv6 mrib table

To enable debugging on Multicast Routing Information Base (MRIB) table management activity, use the **debug ipv6 mrib table** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 mrib [**vrf** *vrf-name*] **table**

no debug ipv6 mrib table

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **debug ipv6 mrib table** command to display information on new MRIB tables being added and deleted.

Examples

The following example enables debugging on MRIB table management activity:

```
Router# debug ipv6 mrib table
```

debug ipv6 nat

To display debug messages for Network Address Translation—Protocol Translation (NAT-PT) translation events, use the **debug ipv6 nat** command in privileged EXEC mode. To disable debug messages for NAT-PT translation events, use the **no** form of this command.

debug ipv6 nat [**detailed** | **port**]

no debug ipv6 nat [**detailed** | **port**]

Syntax Description

detailed	(Optional) Displays detailed information about NAT-PT translation events.
port	(Optional) Displays port allocation events.

Command Default

Debugging for NAT-PT translation events is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.3(2)T	The **port** keyword was added to support Port Address Translation (PAT), or overload, multiplexing multiple IPv6 addresses to a single IPv4 address or to an IPv4 address pool.

Usage Guidelines

The **debug ipv6 nat** command can be used to troubleshoot NAT-PT translation issues. If no keywords are specified, debugging messages for all NAT-PT protocol translation events are displayed.

Note By default, the network server sends the output from **debug** commands and system error messages to the console. To redirect debugging output, use the logging command options within global configuration mode. Destinations are the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server.

Caution Because the **debug ipv6 nat** command generates a substantial amount of output, use it only when traffic on the IPv6 network is low, so other activity on the system is not adversely affected.

Examples

The following example shows output for the **debug ipv6 nat** command:

```
Router# debug ipv6 nat

00:06:06: IPv6 NAT: icmp src (3002::8) -> (192.168.124.8), dst (2001::2) ->
(192.168.123.2)
00:06:06: IPv6 NAT: icmp src (192.168.123.2) -> (2001::2), dst (192.168.124.8) ->
(3002::8)
00:06:06: IPv6 NAT: icmp src (3002::8) -> (192.168.124.8), dst (2001::2) ->
(192.168.123.2)
00:06:06: IPv6 NAT: icmp src (192.168.123.2) -> (2001::2), dst (192.168.124.8) ->
(3002::8)
00:06:06: IPv6 NAT: tcp src (3002::8) -> (192.168.124.8), dst (2001::2) -> (192.168.123.2)
00:06:06: IPv6 NAT: tcp src (192.168.123.2) -> (2001::2), dst (192.168.124.8) -> (3002::8)
00:06:06: IPv6 NAT: tcp src (3002::8) -> (192.168.124.8), dst (2001::2) -> (192.168.123.2)
00:06:06: IPv6 NAT: tcp src (3002::8) -> (192.168.124.8), dst (2001::2) -> (192.168.123.2)
00:06:06: IPv6 NAT: tcp src (3002::8) -> (192.168.124.8), dst (2001::2) -> (192.168.123.2)
00:06:06: IPv6 NAT: tcp src (192.168.123.2) -> (2001::2), dst (192.168.124.8) -> (3002::8)
```

Table 21 describes the significant fields shown in the display.

Table 21 debug ipv6 nat Field Descriptions

Field	Description
IPv6 NAT:	Indicates that this is a NAT-PT packet.
icmp	Protocol of the packet being translated.
src (3000::8) -> (192.168.124.8)	The source IPv6 address and the NAT-PT mapped IPv4 address. **Note** If mapping IPv4 hosts to IPv6 hosts the first address would be an IPv4 address, and the second address an IPv6 address.
dst (2001::2) -> (192.168.123.2)	The destination IPv6 address and the NAT-PT mapped IPv4 address. **Note** If mapping IPv4 hosts to IPv6 hosts the first address would be an IPv4 address, and the second address an IPv6 address.

The following example shows output for the **debug ipv6 nat** command with the **detailed** keyword:

```
Router# debug ipv6 nat detailed

00:14:12: IPv6 NAT: address allocated 192.168.124.8
00:14:16: IPv6 NAT: deleted a NAT entry after timeout
```

debug ipv6 nd

To display debug messages for IPv6 Internet Control Message Protocol (ICMP) neighbor discovery transactions, use the **debug ipv6 nd** command in privileged EXEC mode. To disable debug messages for IPv6 ICMP neighbor discovery transactions, use the **no** form of this command.

debug ipv6 nd

no debug ipv6 nd

Syntax Description

This command has no arguments or keywords.

Command Default

Debugging for IPv6 ICMP neighbor discovery is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(4)T	The DAD: <*nnnn*::*nn*:> is unique, DAD: duplicate link-local <*nnnn*::*nn*:> on <*interface type*>, interface stalled, and Received NA for <*nnnn*::*nn*:> on <*interface type*> from <*nnnn*::*nn*:> fields were added to the command output.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command can help determine whether the router is sending or receiving IPv6 ICMP neighbor discovery messages.

Note By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options within global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on debug commands and redirecting debug output, refer to the *Cisco IOS Debug Command Reference*.

Examples

The following example shows output for the **debug ipv6 nd** command:

```
Router# debug ipv6 nd

13:22:40:ICMPv6-ND:STALE -> DELAY:2000:0:0:3::2
13:22:45:ICMPv6-ND:DELAY -> PROBE:2000:0:0:3::2
13:22:45:ICMPv6-ND:Sending NS for 2000:0:0:3::2 on FastEthernet0/0
13:22:45:ICMPv6-ND:Received NA for 2000:0:0:3::2 on FastEthernet0/0 from 2000:0:0:3::2
13:22:45:ICMPv6-ND:PROBE -> REACH:2000:0:0:3::2
13:22:45:ICMPv6-ND:Received NS for 2000:0:0:3::1 on FastEthernet0/0 from
FE80::203:A0FF:FED6:1400
13:22:45:ICMPv6-ND:Sending NA for 2000:0:0:3::1 on FastEthernet0/0

13:23:15: ICMPv6-ND: Sending NS for FE80::1 on Ethernet0/1
13:23:16: ICMPv6-ND: DAD: FE80::1 is unique.
13:23:16: ICMPv6-ND: Sending NS for 2000::2 on Ethernet0/1
13:23:16: ICMPv6-ND: Sending NS for 3000::3 on Ethernet0/1
13:23:16: ICMPv6-ND: Sending NA for FE80::1 on Ethernet0/1
13:23:17: ICMPv6-ND: DAD: 2000::2 is unique.
13:23:53: ICMPv6-ND: Sending NA for 2000::2 on Ethernet0/1
13:23:53: ICMPv6-ND: DAD: 3000::3 is unique.
13:23:53: ICMPv6-ND: Sending NA for 3000::3 on Ethernet0/1
3d19h: ICMPv6-ND: Sending NS for FE80::2 on Ethernet0/2
3d19h: ICMPv6-ND: Received NA for FE80::2 on Ethernet0/2 from FE80::2
3d19h: ICMPv6-ND: DAD: duplicate link-local FE80::2 on Ethernet0/2,interface stalled
3d19h: %IPV6-4-DUPLICATE: Duplicate address FE80::2 on Ethernet0/2
3d19h: ICMPv6-ND: Sending NS for 3000::4 on Ethernet0/3
3d19h: ICMPv6-ND: Received NA for 3000::4 on Ethernet0/3 from 3000::4
3d19h: %IPV6-4-DUPLICATE: Duplicate address 3000::4 on Ethernet0/3
```

Table 22 describes the significant fields shown in the display.

Table 22 debug ipv6 nd Field Descriptions

Field	Description
13:22:40:	Indicates the time (hours:minutes:seconds) at which the ICMP neighbor discovery event occrred.
ICMPv6-ND	Indicates that a state change is occurring for an entry in the IPv6 neighbors cache.
STALE	Stale state. This state of an neighbor discovery cache entry used to be “reachable,” but is now is “stale” due to the entry not being used. In order to use this address, the router must go through the neighbor discovery process in order to confirm reachability.
DELAY	Delayed state. Reachability for this ND cache entry is currently being reconfirmed. While in the delay state, upper-layer protocols may inform IPv6 that they have confirmed reachability to the entry. Therefore, there is no need to send a neighbor solicitation for the entry.
PROBE	Probe state. While in the probe state, if no confirmation is received from the upper-layer protocols about the reachability of the entry, a neighbor solicitation message is sent. The entry remains in the “probe” state until a neighbor advertisement message is received in response to the neighbor solicitation message.

Table 22 debug ipv6 nd Field Descriptions (continued)

Field	Description
Sending NS for...	Sending a neighbor solicitation message. In the example output, a neighbor solicitation message is sent on Fast Ethernet interface 0/0 to determine the link-layer address of 2000:0:0:3::2 on Fast Ethernet interface 0/0.
Received NA for...	Received a neighbor advertisement message. In the example output, a neighbor advertisement message is received from the address 2000:0:0:3::2 (the second address) that includes the link-layer address of 2000:0:0:3::2 (first address) from Ethernet interface 0/0.
REACH	Reachable state. An ND cache entry in this state is considered reachable, and the corresponding link-layer address can be used without needing to perform neighbor discovery on the address.
Received NS for...	Received neighbor solicitations. In the example output, the address FE80::203:A0FF:FED6:1400 (on Fast Ethernet interface 0/0) is trying to determine the link-local address of 2000:0:0:3::1.
Sending NA for...	Sending for neighbor advertisements. In the example output, a neighbor advertisement containing the link-layer address of 2000:0:0:3::1 (an address assigned to the Fast Ethernet interface 0/0 address) was sent.
DAD: FE80::1 is unique.	Duplicate address detection processing was performed on the unicast IPv6 address (a neighbor solicitation message was not received in response to a neighbor advertisement message that contained the unicast IPv6 address) and the address is unique.
3d19h:	Indicates time (days, hours) since the last reboot of the event occurring; 3d19h: indicates the time (since the last reboot) of the event occurring was 3 days and 19 hours ago.
DAD: duplicate link-local FE80::2 on Ethernet0/2, interface stalled	Duplicate address detection processing was performed on the link-local IPv6 address (the link-local address FE80::2 is used in the example). A neighbor advertisement message was received in response to a neighbor solicitation message that contained the link-local IPv6 address. The address is not unique, and the processing of IPv6 packets is disabled on the interface.
%IPV6-4-DUPLICATE: Duplicate address...	System error message indicating the duplicate address.
Received NA for 3000::4 on Ethernet0/3 from 3000::4	Duplicate address detection processing was performed on the global IPv6 address (the global address 3000::4 is used in the example). A neighbor advertisement message was received in response to a neighbor solicitation message that contained the global IPv6 address. The address is not unique and is not used.

Related Commands

Command	Description
debug ipv6 icmp	Displays debug messages for IPv6 ICMP transactions.
show ipv6 neighbors	Displays IPv6 neighbor discovery cache information.

debug ipv6 ospf

To display debugging information for Open Shortest Path First (OSPF) for IPv6, use the **debug ipv6 ospf** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 ospf [**adj** | **ipsec** | **database-timer** | **flood** | **hello** | **lsa-generation** | **retransmission**]

no debug ipv6 ospf [**adj** | **ipsec** | **database-timer** | **flood** | **hello** | **lsa-generation** | **retransmission**]

Syntax Description

adj	(Optional) Displays adjacency information.
ipsec	(Optional) Displays the interaction between OSPF and IPSec in IPv6 networks, including creation and removal of policy definitions.
database-timer	(Optional) Displays database-timer information.
flood	(Optional) Displays flooding information.
hello	(Optional) Displays hello packet information.
l2api	(Optional) Enables layer 2 and layer 3 application program interface (API) debugging.
lsa-generation	(Optional) Displays link-state advertisement (LSA) generation information for all LSA types.
retransmission	(Optional) Displays retransmission information.

Command Default

Debugging of OSPF for IPv6 is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated in Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated in Cisco IOS Release 12.2(18)S.
12.3(4)T	The **ipsec** keyword was added to support OSPF for IPv6 authentication for IPSec.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(25)T	The **l2api** keyword was added.

Usage Guidelines

Consult Cisco technical support before using this command.

Examples

The following example displays adjacency information for OSPF for IPv6:

```
Router# debug ipv6 ospf adj
```

debug ipv6 ospf database-timer rate-limit

To display debugging information about the current wait-time used for SPF scheduling, use the **debug ipv6 ospf database-timer rate-limit** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 ospf database-timer rate-limit [*acl-number*]

no debug ipv6 ospf database-timer rate-limit

Syntax Description

acl-number	(Optional) Access list number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Consult Cisco technical support before using this command.

Examples

The following example shows how to turn on debugging for SPF scheduling:

```
Router# debug ipv6 ospf database-timer rate-limit
```

debug ipv6 ospf events

To display information on Open Shortest Path First (OSPF)-related events, such as designated router selection and shortest path first (SPF) calculation, use the **debug ipv6 ospf events** command in privileged EXEC command. To disable debugging output, use the **no** form of this command.

debug ipv6 ospf events

no debug ipv6 ospf events

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Consult Cisco technical support before using this command.

Examples

The following example displays information on OSPF-related events:

```
Router# debug ipv6 ospf events
```

debug ipv6 ospf graceful-restart

To enable debugging for IPv6 graceful-restart-related events, use the **debug ipv6 ospf graceful-restart** command in privileged EXEC mode.

debug ipv6 ospf graceful-restart

Syntax Description

This command has no arguments or keywords.

Command Default

Debugging is not enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

The **debug ipv6 ospf graceful-restart** command helps troubleshoot graceful-restart-related events on both graceful-restart-capable and graceful-restart-aware routers.

Examples

The following example enables debugging for graceful-restart-related events:

```
Router# debug ipv6 ospf graceful-restart

00:03:41: OSPFv3: GR timer started for ospf process 1 for 120 secs,
00:03:43: OSPFv3: GR  Build Grace LSA for interface Ethernet0/0
00:03:43: OSPFv3: GR Flood grace lsa on Ethernet0/0
00:03:43: OSPFv3: GR complete check for area 0 process 1
00:03:43: OSPFv3: GR wait, Ethernet0/0 in area 0 not yet complete
00:03:45: OSPFv3: GR Re-flood Grace LSA on Ethernet0/0
00:04:01: OSPFv3: GR  initial wait expired
00:04:01: OSPFv3: GR complete check for area 0 process 1
00:04:01: OSPFv3: GR wait, Ethernet0/0 in area 0 not yet complete
00:04:07: OSPFv3: GR complete check for area 0 process 1
00:04:07: OSPFv3: GR re-sync completed in area 0, process 1
00:04:07: OSPFv3: GR complete check for process 1
00:04:07: OSPFv3: process 1: GR re-sync completed for all neighbors
00:04:07: OSPFv3: scheduling rtr lsa for area 0 process 1
00:04:07: OSPFv3: Post GR, flood maxaged grace-LSA on Ethernet0/0
```

Related Commands

Command	Description
graceful-restart	Enables the OSPFv3 graceful restart feature on a graceful-restart-capable router.
graceful-restart helper	Enables the OSPFv3 graceful restart feature on a graceful-restart-aware router.
show ipv6 ospf graceful-restart	Displays OSPFv3 graceful restart information.

debug ipv6 ospf lsdb

To display database modifications for Open Shortest Path First (OSPF) for IPv6, use the **debug ipv6 ospf lsdb** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 ospf lsdb

no debug ipv6 ospf lsdb

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Consult Cisco technical support before using this command.

Examples

The following example displays database modification information for OSPF for IPv6:

```
Router# debug ipv6 ospf lsdb
```

debug ipv6 ospf monitor

To display debugging information about the current wait-time used for shortest path first (SPF) scheduling, use the **debug ipv6 ospf monitor** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 ospf monitor

no debug ipv6 ospf monitor

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Consult Cisco technical support before using this command.

Examples

The following example shows debugging information about SPF scheduling:

```
Router# debug ipv6 ospf monitor
```

```
Sep 27 08:29:49.319: OSPFv3: Schedule SPF in area 0
        Change in LS ID 0.0.0.0, LSA type P
*Sep 27 08:29:49.327: OSPFv3: reset throttling to 5000ms next wait-interval 10000ms
*Sep 27 08:29:49.327: OSPFv3: schedule SPF: spf_time 00:09:36.032 wait_interval 5000ms
IOU_Topvar#
*Sep 27 08:29:54.331: OSPFv3: Begin SPF at 581.036ms, process time 40ms
*Sep 27 08:29:54.331:       spf_time 00:09:36.032, wait_interval 5000ms
*Sep 27 08:29:54.331: OSPFv3: Setting next wait-interval to 10000ms
*Sep 27 08:29:54.331: OSPFv3: End SPF at 581.036ms, Total elapsed time 0ms
*Sep 27 08:29:54.331:       Schedule time 00:09:41.036, Next wait_interval 10000ms
*Sep 27 08:29:54.331:       Intra: 0ms, Inter: 0ms, External: 0ms
*Sep 27 08:29:54.331:       R: 0, N: 0
*Sep 27 08:29:54.331:       SN: 0, SA: 0, X5: 0, X7: 0
*Sep 27 08:29:54.331:       SPF suspends: 0 intra, 0 total
```

debug ipv6 ospf packet

To display information about each Open Shortest Path First (OSPF) for IPv6 packet received, use the **debug ipv6 ospf packet** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 ospf packet

no debug ipv6 ospf packet

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Consult Cisco technical support before using this command.

Examples

The following example displays information about each OSPF for IPv6 packet received:

```
Router# debug ipv6 ospf packet
```

debug ipv6 ospf spf statistic

To display statistical information while running the shortest path first (SPF) algorithm, use the **debug ipv6 ospf spf statistic** command in privileged EXEC mode. To disable the debugging output, use the **no** form of this command.

debug ipv6 ospf spf statistic

no debug ipv6 ospf spf statistic

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **debug ipv6 ospf spf statistic** command displays the SPF calculation times in milliseconds, the node count, and a time stamp. Consult Cisco technical support before using this command.

Examples

The following example displays statistical information while running the SPF algorithm:

```
Router# debug ipv6 ospf spf statistics
```

Related Commands

Command	Description
debug ipv6 ospf	Displays debugging information for the OSPFv3 for IPv6 feature.
debug ipv6 ospf events	Displays information on OSPFv3-related events.
debug ipv6 ospf packet	Displays information about each OSPFv3 packet received.

debug ipv6 packet

To display debug messages for IPv6 packets, use the **debug ipv6 packet** command in privileged EXEC mode. To disable debug messages for IPv6 packets, use the **no** form of this command.

debug ipv6 packet [**access-list** *access-list-name*] [**detail**]

no debug ipv6 packet [**access-list** *access-list-name*] [**detail**]

Syntax Description

access-list *access-list-name*	(Optional) Specifies an IPv6 access list. The access list name cannot contain a space or quotation mark, or begin with a numeric
detail	(Optional) May display additional detailed information about the IPv6 packet.

Command Default

Debugging for IPv6 packets is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	The **access-list** and **detail** keywords, and the *access-list-name* argument, were added.
12.2(13)T	The **access-list** and **detail** keywords, and the *access-list-name* argument, were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **debug ipv6 packet** command is similar to the **debug ip packet** command, except that it is IPv6-specific.

Note By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options within global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on debug commands and redirecting debug output, refer to the *Cisco IOS Debug Command Reference*.

IPv6 debugging information includes packets received, generated, and forwarded. Fast-switched packets do not generate messages. When an IPv6 access list is specified by using the **access-list** keyword and *access-list-name* argument, only packets matching the access list permit entries are displayed.

Caution Because the **debug ipv6 packet** command generates a substantial amount of output, use it only when traffic on the IPv6 network is low, so other activity on the system is not adversely affected.

Examples

The following example shows output for the **debug ipv6 packet** command:

```
Router# debug ipv6 packet

13:25:40:IPV6:source 2000:0:0:3::1 (local)
13:25:40:      dest 2000:0:0:3::2 (FastEthernet0/0)
13:25:40:      traffic class 96, flow 0x0, len 143+195, prot 6, hops 64, originating
13:25:40:IPv6:Sending on FastEthernet0/0
13:25:40:IPV6:source 2000:0:0:3::2 (FastEthernet0/0)
13:25:40:      dest 2000:0:0:3::1
13:25:40:      traffic class 96, flow 0x0, len 60+14, prot 6, hops 64, forward to ulp
13:25:45:IPV6:source FE80::203:E4FF:FE12:CC1D (local)
13:25:45:      dest FF02::9 (Ethernet1/1)
13:25:45:      traffic class 112, flow 0x0, len 72+1428, prot 17, hops 255, originating
13:25:45:IPv6:Sending on Ethernet1/1
13:25:45:IPV6:source FE80::203:E4FF:FE12:CC00 (local)
13:25:45:      dest 2000:0:0:3::2 (FastEthernet0/0)
13:25:45:      traffic class 112, flow 0x0, len 72+8, prot 58, hops 255, originating
13:25:45:IPv6:Sending on FastEthernet0/0
13:25:45:IPV6:source 2000:0:0:3::2 (FastEthernet0/0)
13:25:45:      dest FE80::203:E4FF:FE12:CC00
13:25:45:      traffic class 112, flow 0x0, len 64+14, prot 58, hops 255, forward to ulp
13:25:45:IPV6:source FE80::203:A0FF:FED6:1400 (FastEthernet0/0)
13:25:45:      dest 2000:0:0:3::1
13:25:45:      traffic class 112, flow 0x0, len 72+14, prot 58, hops 255, forward to ulp
```

Table 23 describes the significant fields shown in the display.

Table 23 debug ipv6 packet Field Descriptions

Field	Description
IPV6:	Indicates that this is an IPv6 packet.
source 2000:0:0:3::1 (local)	The source address in the IPv6 header of the packet.
dest 2000:0:0:3::2 (FastEthernet0/0)	The destination address in the IPv6 header of the packet.
traffic class 96	The contents of the traffic class field in the IPv6 header.
flow 0x0	The contents of the flow field of the IPv6 header. The flow field is used to label sequences of packets for which special handling is necessary by IPv6 routers.
len 64+14	The length of the IPv6 packet. The length is expressed as two numbers with a plus (+) character between the numbers. The first number is the length of the IPv6 portion (IPv6 header length plus payload length). The second number is the entire datagram size minus the first number.

Table 23 debug ipv6 packet Field Descriptions (continued)

Field	Description
prot 6	The protocol field in the IPv6 header. Describes the next layer protocol that is carried by the IPv6 packet. In the example, the protocol 58 signifies that the next layer protocol is ICMPv6.
hops 64	The hops field in the IPv6 packet. This field is similar in function to the IPv4 time-to-live field.
originating	The presence of this field indicates that the packet shown was originated by the router.
Sending on FastEthernet0/0	Specifies the interface on which the packet was sent.
forward to ulp	Indicates that the packet was received by the router at the destination address and was forwarded to an upper-layer protocol (ulp) for processing.

debug ipv6 pim

To enable debugging on Protocol Independent Multicast (PIM) protocol activity, use the **debug ipv6 pim** command in privileged EXEC mode. To restore the default value, use the **no** form of this command.

debug ipv6 pim [*group-name* | *group-address* | **interface** *interface-type* | **bsr** | **group** | **neighbor**]

no debug ipv6 pim [*group-name* | *group-address* | **interface** *interface-type* | **bsr** | **group** | **neighbor**]

Syntax Description

group-name | *group-address*	(Optional) IPv6 address or name of the multicast group.
interface *interface-type*	(Optional) Displays debugging statistics about a specific interface type.
bsr	(Optional) Displays debugging statistics specific to bootstrap router (BSR) protocol operation.
group	(Optional) Displays debugging information about group-related activity.
neighbor	(Optional) Displays debugging statistics related to hello message processing and neighbor cache management.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.0(28)S	The **bsr** keyword was added.
12.2(25)S	The **bsr** keyword was added.
12.3(11)T	The **bsr** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

This command helps discover whether the PIM protocol activities are working correctly.

The messages displayed by the **debug ipv6 pim** command show all PIM protocol messages, such as joins and prunes, received from or sent to other routers. Use this command in conjunction with **debug ipv6 mld** to display additional multicast activity, to learn more information about the multicast routing process, or to learn why packets are forwarded out of particular interfaces.

Examples

The following example enables debugging on PIM activity:

```
Router# debug ipv6 pim
```

Related Commands

Command	Description
debug ipv6 mld	Enables debugging on MLD protocol activity.