



Monitoring and Troubleshooting

This chapter presents the following major topics:

- [Troubleshooting Multicast, page 4-1](#)
- [Show Commands, page 4-2](#)
- [Debug Commands, page 4-5](#)
- [Viewing HWRL Counters, page 4-6](#)

Troubleshooting Multicast

Several commands can be used to troubleshoot IP multicast (IPmc) networks:

- [mstat](#)
- [mrinfo](#)
- [mtrace](#)



Note

For more information, including syntax and examples, see “Monitoring and Maintaining IP Multicast” at the following URL:

http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a00804453e7.html

mstat

Use this command to see the IPmc path in ASCII graphic format. It traces the path between any two points in the network, shows drops and duplicates, time to live (TTL) thresholds, and delays at each node in the network. It is very useful when you need to locate congestion points in the network, or focus on a router with high drop/duplicate counts. Duplicates are indicated in the output as “negative” drops.

mrinfo

Use this command to see IPmc neighbor router information, router capabilities and code version, IPmc interface information, TTL thresholds, metrics, protocol, and status. It is useful when you need to verify IPmc neighbors, confirm that bidirectional neighbor adjacency exists, and verify that tunnels are up in both directions.

mtrace

Use this command to see the IPmc path from the source to the receive. It traces the path between points in the networks, showing TTL thresholds and delay at each node. When troubleshooting, use this command to find where IPmc traffic flow stops, to verify the path of IPmc traffic, and to identify suboptimal paths.

Show Commands

Show commands are presented for the following categories:

- [show ip](#)
- [show mls](#)

show ip

The following commands provide useful information about IP routing:

- [show ip igmp groups](#)
- [show ip igmp interface](#)
- [show ip pim neighbor](#)
- [show ip pim interface](#)
- [show ip mroute summary](#)
- [show ip mroute](#)
- [show ip mroute active](#)
- [show ip rpf](#)
- [show ip mroute count](#)
- [show ip pim rp mapping](#)

**Note**

For more information, including syntax and examples, see “Cisco IOS IP Command Reference, Volume 3 of 4: Multicast, Release 12.3, at the following URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_command_reference_chapter09186a008017cf20.html

show ip igmp groups

Use this command to see which IPmc groups are directly connected to the router, and which are learned by means of Internet Group Management Protocol (IGMP). You can use this command to verify that a source or receiver has actually joined the target group on the router interface. The “Last Reporter” column shows only one IGMP host, which indicates that it has sent either an unsolicited IGMP Join or IGMP Report in response to a IGMP Query from the Protocol Independent Multicast (PIM) router for that particular group. You should only see one “Last Reporter” per Group Address.

show ip igmp interface

Use this command to display IPmc-related information about an interface, and to verify that IGMP is enabled, that the correct version is running, the timers, Time To Live (TTL) threshold value, and that IGMP querier router are properly set. IGMP does not need to be configured on an interface. It is enabled by default when you configure **ip pim dense-mode** | **sparse-mode** | **sparse-dense-mode**.

show ip pim neighbor

Use this command to list the PIM neighbors discovered by the Cisco IOS.

show ip pim interface

Use this command to display information about interfaces configured for PIM. In addition, you can use it to verify that the correct PIM mode (dense or sparse) is configured on the interface, the neighbor count is correct, and the designated router (DR) is correct (which is critical for PIM sparse mode). Multi-access segments (such as Ethernet, Token Ring, FDDI) elect a DR based on highest IP address. Point-to-Point links do not display DR information.

show ip mroute summary

Use this command to display the summarized contents of the IPmc routing table. You can also use it to verify the active IPmc group(s) and which IPmc senders are active by looking at the timers and flags.

show ip mroute

Use this command to display the full contents of the IPmc routing table. When you troubleshoot, use this command to verify the following:

- The (S,G) and (*,G) state entries from the flags.
- Whether the incoming interface is correct. If it is not, check the unicast routing table.
- Whether the outgoing interface (or interfaces) is (or are) correct. For any that are incorrectly pruned, check the state in the downstream router.

show ip mroute active

Use this command to display the active traffic sources and groups above the threshold. When you troubleshoot, use it to verify active source groups, the traffic rate for each source, group (S,G) pair [you must have switched to Shortest Path Tree (SPT)], and to check if the target group IPmc traffic is being received. If the traffic is not being received, look for active traffic starting from the source towards the receiver.

show ip rpf

Use this command to display how IPmc routing does Reverse Path Forwarding (RPF). When you troubleshoot, use it to verify that the RPF information is correct. If it is not, check the unicast routing table for the source address. Also use the **ping** and **trace** commands on the source address to verify that unicast routing works. You may need to use Distance Vector Multicast Routing Protocol (DVMRP) routes or static mroutes to fix any unicast-multicast inconsistencies.

show ip mroute count

Use this command to verify that IPmc traffic is received, and to check on its flow rates and drops. If no traffic is received, work from the source to the receiver until you find where the traffic stops. You can also use this command to verify that traffic is being forwarded. If it is not, use the **show ip mroute** command to look for “Null Outgoing interface list” and RPF failures.

show ip pim rp mapping

Use this command to check the RP assignment by IPmc group range, and to verify that the source of RP learning (static or auto-RP) and the mapping are correct. If you find an error, check the local router configuration or auto-RP configuration.

show mls

The following command provides useful information about Multi-Layer Switching (MLS).

- [show mls rate-limit](#)
- [show mls cef adjacency](#)
- [show mls statistics](#)

show mls rate-limit

Use this command to see an exhaustive list of special-case hardware rate limiters (HWRLs). (See [Hardware Rate Limiters, page 2-13](#).) The following output shows all HWRLs available as of Cisco IOS Release 12.2(18)SXE.

```
Router# show mls rate-limit

Load for five secs: 1%/0%; one minute: 1%; five minutes: 0%
Time source is NTP, 17:57:48.508 PST Mon Mar 28 2005

Sharing Codes: S - static, D - dynamic
Codes dynamic sharing: H - owner (head) of the group, g - guest of the group
```

Rate Limiter Type	Status	Packets/s	Burst	Sharing
MCAST NON RPF	Off	-	-	-
MCAST DFLT ADJ	On	100000	100	Not sharing
MCAST DIRECT CON	Off	-	-	-
ACL BRIDGED IN	Off	-	-	-
ACL BRIDGED OUT	Off	-	-	-
IP FEATURES	Off	-	-	-
ACL VACL LOG	On	2000	1	Not sharing
CEF RECEIVE	Off	-	-	-
CEF GLEAN	Off	-	-	-
MCAST PARTIAL SC	On	100000	100	Not sharing
IP RPF FAILURE	On	100	10	Group:0 S
TTL FAILURE	Off	-	-	-
ICMP UNREAC. NO-ROUTE	On	100	10	Group:0 S
ICMP UNREAC. ACL-DROP	On	100	10	Group:0 S
ICMP REDIRECT	Off	-	-	-
MTU FAILURE	Off	-	-	-
MCAST IP OPTION	Off	-	-	-
UCAST IP OPTION	Off	-	-	-
LAYER_2 PDU	Off	-	-	-
LAYER_2 PT	Off	-	-	-
IP ERRORS	On	100	10	Group:0 S
CAPTURE PKT	Off	-	-	-
MCAST IGMP	Off	-	-	-
MCAST IPv6 DIRECT CON	Off	-	-	-
MCAST IPv6 ROUTE CNTL	Off	-	-	-
MCAST IPv6 *G M BRIDG	Off	-	-	-
MCAST IPv6 SG BRIDGE	Off	-	-	-
MCAST IPv6 DFLT DROP	Off	-	-	-
MCAST IPv6 SECOND. DR	Off	-	-	-
MCAST IPv6 *G BRIDGE	Off	-	-	-

show mls cef adjacency

See [Viewing HWRL Counters, page 4-6](#).

show mls statistics

See [Viewing HWRL Counters, page 4-6](#).

Debug Commands

The following debug commands provide useful information:

- `debug ip pim`
- `debug ip mpacket`
- `debug ip mrouting`



Note

For more information, including syntax and examples, see “Cisco IOS Debug Command Reference, Release 12.2,” at the following URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a0080087363.html

debug ip pim

Use this command to display PIM packets received and sent, and to display PIM-related events.

debug ip mpacket

Use this command to display IP multicast packets received and sent,

debug ip mrouting

Use this command to display changes to the IP multicast routing table.

Viewing HWRL Counters



Note

For background, see [Hardware Rate Limiters, page 2-13](#).

Although Cisco IOS does not currently have a summarized CLI output of hardware rate limiter (HWRL) counters, it is possible to monitor some of the more interesting ones through module-specific commands. HWRLs are implemented as a series of special Cisco Express Forwarding (CEF) adjacencies, which can be seen with the **show mls cef adjacency special** command. The output below has been reduced to the more interesting HWRL adjacencies. Note that the limiter type is shown in parentheses for each index.

```
Router> show mls cef adjacency special
```

```

Index: 0      smac: 0000.0000.0000, dmac: 0000.0000.0000
              mtu: 9234, vlan: 0, dindex: 0x0, l3rw_vld: 1
              format: MULTICAST, flags: 0x2000000C00 (mcast_fib_fail)
              met2: 0, met3: 0
              packets: 0, bytes: 0

Index: 3      smac: 0000.0000.0000, dmac: 0000.0000.0000
              mtu: 9234, vlan: 0, dindex: 0x0, l3rw_vld: 0
              format: MULTICAST, flags: 0x2000000800 (mcast_fib_rpf_fail)
              met2: 0, met3: 0
              packets: 0, bytes: 0

Index: 5      smac: 0000.0000.0000, dmac: 0000.0000.0000
              mtu: 9234, vlan: 0, dindex: 0x0, l3rw_vld: 1
              format: MULTICAST, flags: 0x2000000C00 (mcast_dir_conn)
              met2: 0, met3: 0
              packets: 0, bytes: 0

```

HWRL counters for each distributed forwarding card (DFC) can be seen by issuing the **show mls cef adjacency entry** command for each module. If no module is specified then the counters are shown for the policy feature card (PFC). For example, to see counters for the FIB-Miss HWRL (Index 0 from the above output) in a system that has DFC-based modules in slots 1 and 4, issue the commands as shown below. The first command below (without the module subcommand) shows the counters from the PFC3 on the Sup720. The counters from this command show traffic limited on cards that do not have DFC3 submodules.

```
Router> show mls cef adjacency entry 0
```

```
Index: 0      smac: 0000.0000.0000, dmac: 0000.0000.0000
              mtu: 9234, vlan: 0, dindex: 0x0, l3rw_vld: 1
              packets: 0, bytes: 0
```



Note The above output is identical to what is retrieved when the module where the Sup720 is located is specified. In other words, the above command is the equivalent of issuing a **show mls cef adjacency entry 0 module 5** command when the Sup720 is in slot 5.

```
Router> show mls cef adjacency entry 0 module 1
```

```
Index: 0      smac: 0000.0000.0000, dmac: 0000.0000.0000
              mtu: 9234, vlan: 0, dindex: 0x0, l3rw_vld: 1
              packets: 656, bytes: 891424
```

```
Router> show mls cef adjacency entry 0 module 4
```

```
Index: 0      smac: 0000.0000.0000, dmac: 0000.0000.0000
              mtu: 9234, vlan: 0, dindex: 0x0, l3rw_vld: 1
              packets: 5004164, bytes: 6775638056
```

These counters are not currently accessible by means of SNMP.

TTL and MTU failures can be seen in the output of the **show mls statistics** command, as shown below.



Note TTL and MTU failure counters are available only with the DFC3B and DFC3BXL. These counters include all packets failing TTL and MTU checks, both by HWRLs and by MSFC-RP software processing.

```
Router# show mls statistics
```

```
<---snip--->
```



Note Statistics for Module 4 are shown below.

Errors

```
MAC/IP length inconsistencies      : 0
Short IP packets received          : 0
IP header checksum errors         : 0
TTL failures                    : 721386
MTU failures                    : 0
```

```
<---snip--->
```



Note Statistics for Module 5 are shown below.

Errors

```
MAC/IP length inconsistencies      : 0
Short IP packets received          : 0
IP header checksum errors         : 0
TTL failures                    : 0
MTU failures                    : 0
```

```
Total packets L3 Switched by all Modules: 2733893197353 @ 3651668 pps
```

