show ip cef epoch

To display the epoch information for the adjacency table and all FIB tables, use the **show ip cef epoch** command.

show ip cef epoch

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

These **show** commands also display the epoch information for the following:

- **show ip cef summary**—Displays the table epoch for a specific FIB table.
- **show ip cef detail**—Displays the epoch value for each entry of a specific FIB table.
- **show adjacency summary**—Displays the adjacency table epoch.
- **show adjacency detail**—Displays the epoch value for each entry of the adjacency table.

Examples

This example shows how to display epoch information:

```
Router# show ip cef epoch
CEF epoch information:

Table:Default-table
  Table epoch:2 (164 entries at this epoch)

Adjacency table
  Table epoch:1 (33 entries at this epoch)
```

This example shows the output after you clear the epoch table and increment the epoch number:

```
Router# show ip cef epoch
CEF epoch information:

Table:Default-table
  Table epoch:2 (164 entries at this epoch)

Adjacency table
  Table epoch:1 (33 entries at this epoch)
```

```
Router# clear ip cef epoch full
Router# show ip cef epoch
CEF epoch information:

Table:Default-table
  Table epoch:3 (164 entries at this epoch)

Adjacency table
  Table epoch:2 (33 entries at this epoch)
Router#
```

Syntax Description

Command	Description
clear ip cef epoch full	Begins a new epoch and increments the epoch number for all tables (including the adjacency table).
show ip cef	Displays entries in the FIB or displays a summary of the FIB.

show ip cef inconsistency

To display the IP CEF inconsistencies, use the **show ip cef inconsistency** command.

show ip cef [**vrf** *vrf-name*] **inconsistency** [**records** [**detail**]]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a VRF instance.
records	(Optional) Displays all recorded inconsistencies.
detail	(Optional) Displays the detailed information for each CEF table entry.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command displays the recorded IP CEF inconsistency records found by the lc-detect, scan-rp, scan-rib, and scan-lc detection mechanisms.

You can configure the IP CEF-prefix consistency-detection mechanisms using the **ip cef table consistency-check** command.

Examples

This example shows how to display the recorded CEF inconsistency records:

```
Router# show ip cef inconsistency
Table consistency checkers (settle time 65s)
 lc-detect:running
  0/0/0 queries sent/ignored/received
 scan-lc:running [100 prefixes checked every 60s]
  0/0/0 queries sent/ignored/received
 scan-rp:running [100 prefixes checked every 60s]
  0/0/0 queries sent/ignored/received
 scan-rib:running [1000 prefixes checked every 60s]
  0/0/0 queries sent/ignored/received
Inconsistencies:0 confirmed, 0/16 recorded
```

Table 2-46 describes the fields shown in the display.

Table 2-46 show ip cef inconsistency Field Descriptions

Field	Description
settle time	Time after a recorded inconsistency is confirmed.
lc-detect running	Consistency checker lc-detect is running.
0/0/0 queries	Number of queries sent, ignored, and received.
Inconsistencies:	Number of inconsistencies confirmed and recorded. The maximum number of inconsistency records to be recorded is 16.

Related Commands

Command	Description
clear ip cef inconsistency	Clears the statistics and records for the CEF-consistency checker.

show ip cef summary

To display a summary of the IP CEF table, use the **show ip cef summary** command.

show ip cef summary

Syntax Description

This command has no keywords and arguments.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to display a summary of the IP CEF table:

```
Router# show ip cef summary
IP Distributed CEF with switching (Table Version 25), flags=0x0
  21 routes, 0 reresolve, 0 unresolved (0 old, 0 new), peak 1
  21 leaves, 16 nodes, 19496 bytes, 36 inserts, 15 invalidations
  0 load sharing elements, 0 bytes, 0 references
  universal per-destination load sharing algorithm, id 5163EC15
  3(0) CEF resets, 0 revisions of existing leaves
  Resolution Timer: Exponential (currently 1s, peak 1s)
  0 in-place/0 aborted modifications
  refcounts:  4377 leaf, 4352 node

  Table epoch: 0 (21 entries at this epoch)

Adjacency Table has 9 adjacencies
Router#
```

show ip cef vlan

To display the information about the IP CEF VLAN interface status, the configuration, and the prefixes for a specific interface, use the **show ip cef vlan** command.

show ip cef vlan *vlan-id* [**detail**]

Syntax Description

vlan-id	VLAN number; valid values are from 1 to 4094.
detail	(Optional) Displays the detailed information about the IP CEF VLAN interface.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to display the prefixes for a specific VLAN:

```
Router> show ip cef vlan 1003
Prefix              Next Hop             Interface
0.0.0.0/0           172.20.52.1          FastEthernet3/3
0.0.0.0/32          receive
10.7.0.0/16         172.20.52.1          FastEthernet3/3
10.16.18.0/23       172.20.52.1          FastEthernet3/3
Router>
```

This example shows how to display detailed IP CEF information for a specific VLAN:

```
Router> show ip cef vlan 1003 detail
IP Distributed CEF with switching (Table Version 2364), flags=0x0
  1383 routes, 0 reresolve, 0 unresolved (0 old, 0 new)
  1383 leaves, 201 nodes, 380532 bytes, 2372 inserts, 989 invalidations
  0 load sharing elements, 0 bytes, 0 references
  universal per-destination load sharing algorithm, id 9B6C9823
  3 CEF resets, 0 revisions of existing leaves
  refcounts:  54276 leaf, 51712 node
Adjacency Table has 5 adjacencies
Router>
```

show ip dhcp relay information trusted-sources

To list all the configured trusted interfaces, use the **show ip dhcp relay information trusted-sources** command.

show ip dhcp relay information trusted-sources

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to display a list of all the configured trusted interfaces:

```
Router# show ip dhcp relay information trusted-sources
List of trusted sources of relay agent information option:
Vlan60          Vlan62
Router#
```

Related Commands

Command	Description
ip dhcp relay information option trust-all	Enables all the interfaces as trusted sources of the DHCP relay-agent information option.
ip dhcp relay information trust	Enables an interface as a trusted source of the DHCP relay-agent information.

show ip dhcp snooping

To display the DHCP snooping configuration, use the **show ip dhcp snooping** command.

show ip dhcp snooping [**statistics** [**detail**]]

Syntax Description

statistics	(Optional) Displays statistics information about DHCP snooping.
detail	(Optional) Displays the detailed information about DHCP snooping.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to display the DHCP snooping configuration:

```
Router# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
5 10
Insertion of option 82 is enabled
Interface                Trusted     Rate limit (pps)
--------------------     -------     ----------------
FastEthernet6/11         no          10
FastEthernet6/36         yes         50
Router#
```

This example shows how to display the DHCP snooping statistics information:

```
Router# show ip dhcp snooping statistics
Packets Processed by DHCP Snooping                    = 0
Packets Dropped Because
   IDB not known                                       = 0
   Queue full                                          = 0
   Interface is in errdisabled                         = 0
   Rate limit exceeded                                 = 0
   Received on untrusted ports                         = 0
   Nonzero giaddr                                      = 0
   Source mac not equal to chaddr                      = 0
   No binding entry                                    = 0
   Insertion of opt82 fail                             = 0
   Unknown packet                                      = 0
   Interface Down                                      = 0
   Unknown output interface                            = 0
Router#
```

This example shows how to display detailed DHCP snooping statistics information:

```
Router# show ip dhcp snooping statistics detail
Packets Forwarded                                     = 0
Packets Dropped                                      = 0
Packets Dropped From untrusted ports                 = 0
Router#
```

Related Commands

Command	Description
clear ip dhcp snooping	Clears the IP DHCP table entries.
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping binding	Sets up and generates a DHCP binding configuration to restore bindings across reboots.
ip dhcp snooping database	Configures the DHCP snooping database.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
ip dhcp snooping packets	Enables DHCP snooping on the tunnel interface.
ip dhcp snooping verify mac-address	Verifies that the source MAC address in a DHCP packet matches the client hardware address on an untrusted port.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

show ip dhcp snooping binding

To display the DHCP snooping binding entries, use the **show ip dhcp snooping binding** command.

show ip dhcp snooping binding [*ip-address*] [*mac-address*] [**vlan** *vlan*]
[**interface** *interface interface-num*]

Syntax Description

ip-address	(Optional) IP address for the binding entries.
mac-address	(Optional) MAC address for the binding entries.
vlan *vlan*	(Optional) Specifies a valid VLAN number; valid values are from 1 to 4094.
interface *interface*	(Optional) Specifies the interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, and **tengigabitethernet**.
interface-num	Module and port number.

Command Default

If no argument is specified, the switch displays the entire DHCP snooping binding table.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

DHCP snooping is enabled on a VLAN only if both the global snooping and the VLAN snooping are enabled.

Examples

This example shows how to display the DHCP snooping binding entries for a switch:

```
Router# show ip dhcp snooping binding

MacAddress      IP Address     Lease (seconds)     Type              VLAN      Interface
-----------     -----------    ----------------    -------------      -----     ------------
0000.0100.0201   10.0.0.1         1600                 dhcp-snooping       100       FastEthernet3/1
Router#
```

This example shows how to display an IP address for DHCP snooping binding entries:

```
Router# show ip dhcp snooping binding 172.100.101.102

MacAddress      IP Address       Lease (seconds)     Type              VLAN     Interface
-----------     -----------      ----------------    -------------      -----    ------------
0000.0100.0201    172.100.101.102   1600                 dhcp-snooping       100       FastEthernet3/1
Router#
```

This example shows how to display the MAC address for the DHCP snooping binding entries:

```
Router# show ip dhcp snooping binding 55.5.5.2 0002.b33f.3d5f

MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------      ----  --------------------
00:02:B3:3F:3D:5F   55.5.5.2         492         dhcp-snooping       99 FastEthernet6/36
Router#
```

This example shows how to display the DHCP snooping binding entries’ MAC address for a specific VLAN:

```
Router# show ip dhcp snooping binding 55.5.5.2 0002.b33f.3d5f vlan 99

MacAddress          IpAddress        Lease(sec)  Type            VLAN  Interface
------------------  ---------------  ----------  -------------       ----  --------------------
00:02:B3:3F:3D:5F   55.5.5.2         479         dhcp-snooping       99    FastEthernet6/36
Router#
```

This example shows how to display the dynamic DHCP snooping binding entries:

```
Router# show ip dhcp snooping binding dynamic

MacAddress      IP Address     Lease (seconds)      Type              VLAN     Interface
-----------     -----------    ----------------     ------------      -----    ------------
0000.0100.0201   10.0.0.1         1600                 dhcp-snooping      100       FastEthernet3/1
Router#
```

This example shows how to display the DHCP snooping binding entries on VLAN 100:

```
Router# show ip dhcp snooping binding vlan 100

MacAddress      IP Address     Lease (seconds)     Type              VLAN     Interface
-----------     -----------    ----------------    ------------      -----    ------------
0000.0100.0201   10.0.0.1         1600                dhcp-snooping      100       FastEthernet3/1
Router#
```

This example shows how to display the DHCP snooping binding entries on Ethernet interface 0/1:

```
Router# show ip dhcp snooping binding interface fastethernet3/1

MacAddress      IP Address     Lease (seconds)     Type              VLAN     Interface
-----------     -----------    ----------------    ------------      -----    ------------
0000.0100.0201   10.0.0.1         1600                dhcp-snooping      100       FastEthernet3/1
Router#
```

Table 2-47 describes the fields in the **show ip dhcp snooping** command output.

Table 2-47 show ip dhcp snooping Command Output

Field	Description
Mac Address	Client hardware MAC address.
IP Address	Client IP address assigned from the DHCP server.
Lease (seconds)	IP address lease time.
Type	Binding type; statically configured from CLI or dynamically learned.
VLAN	VLAN number of the client interface.
Interface	Interface that connects to the DHCP client host.

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping binding	Sets up and generates a DHCP binding configuration to restore bindings across reboots.
ip dhcp snooping database	Configures the DHCP snooping database.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
ip dhcp snooping packets	Enables DHCP snooping on the tunnel interface.
ip dhcp snooping verify mac-address	Verifies that the source MAC address in a DHCP packet matches the client hardware address on an untrusted port.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

show ip dhcp snooping database

To display the status of the DHCP snooping database agent, use the **show ip dhcp snooping database** command.

show ip dhcp snooping database [**detail**]

Syntax Description

detail	(Optional) Provides additional operating state and statistics information.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to display the DHCP snooping database:

```
Router# show ip dhcp snooping database
Agent URL :
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running

Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts       :        0   Startup Failures :        0
Successful Transfers :        0   Failed Transfers :        0
Successful Reads     :        0   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :        0
Media Failures       :        0

Router#
```

This example shows how to view additional operating statistics:

```
Router# show ip dhcp snooping database detail
Agent URL : tftp://10.1.1.1/directory/file
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : 7 (00:00:07)
Abort Timer Expiry : Not Running

Last Succeded Time : None
Last Failed Time : 17:14:25 UTC Sat Jul 7 2001
Last Failed Reason : Unable to access URL.

Total Attempts       :       21   Startup Failures :        0
Successful Transfers :        0   Failed Transfers :       21
Successful Reads     :        0   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :       21
Media Failures       :        0

First successful access: Read

Last ignored bindings counters :
Binding Collisions    :        0   Expired leases    :        0
Invalid interfaces    :        0   Unsupported vlans :        0
Parse failures        :        0
Last Ignored Time : None

Total ignored bindings counters:
Binding Collisions    :        0   Expired leases    :        0
Invalid interfaces    :        0   Unsupported vlans :        0
Parse failures        :        0

Router#
```

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping binding	Sets up and generates a DHCP binding configuration to restore bindings across reboots.
ip dhcp snooping database	Configures the DHCP snooping database.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
ip dhcp snooping packets	Enables DHCP snooping on the tunnel interface.
ip dhcp snooping verify mac-address	Verifies that the source MAC address in a DHCP packet matches the client hardware address on an untrusted port.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

show ip flow-export

To display the information about the software-switched flows for the data export, including the main cache and all other enabled caches, use the **show ip flow export** command.

show ip flow export [**template** | **verbose**]

Syntax Description

template	(Optional) Displays export template statistics information.
verbose	(Optional) Displays verbose export statistics information.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to display the information about the software-switched flows for NDE:

```
Router# show ip flow export
Flow export v1 is disabled for main cache
  Version 1 flow records
  0 flows exported in 0 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
  0 export packets were dropped enqueuing for the RP
  0 export packets were dropped due to IPC rate limiting
Router#
```

This example shows how to display export template statistics information:

```
Router# show ip flow export template
 No Template export information
 No Option Templates exist
   Template Options Flag = 0
   Total number of Templates added = 0
   Total active Templates = 0
   Flow Templates active = 0
   Flow Templates added = 0
   Option Templates active = 0
   Option  Templates added = 0
   Template ager polls = 0
   Option Template ager polls = 0
Main cache version 9 export is disabled
Router#
```

This example shows how to display export verbose statistics information:

```
Router# show ip flow export verbose
Flow export v1 is disabled for main cache
  Version 1 flow records
  0 flows exported in 0 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
  0 export packets were dropped enqueuing for the RP
  0 export packets were dropped due to IPC rate limiting
Router#
```

Related Commands

Command	Description
clear adjacency	Clears the CEF adjacency table.
ip flow-aggregation cache	Creates a flow-aggregation cache and enters the aggregation cache configuration mode.

show ip igmp groups

To display the multicast groups with receivers that are directly connected to the router and that were learned through IGMP, use the **show ip igmp groups** command.

show ip igmp [**vrf** *vrf-name*] **groups** [*group-name* | *group-address* | *interface-type interface-number*] [**detail**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
group-name	(Optional) Name of the multicast group as defined in the DNS hosts table.
group-address	(Optional) Address of the multicast group in four-part, dotted-decimal notation.
interface-type	(Optional) Interface type.
interface-number	(Optional) Interface number.
detail	(Optional) Provides a detailed description of the sources that are known through IGMP Version 3 (IGMPv3), IGMP v3lite, or URL Rendezvous Directory (URD).

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

If you omit all optional arguments and keywords, the **show ip igmp groups** command displays all directly connected multicast groups by group address, interface type, and interface number.

Examples

This example shows how to display output from the **show ip igmp groups** command:

```
Router# show ip igmp groups

IGMP Connected Group Membership
Group Address      Interface        Uptime      Expires     Last Reporter
239.255.255.254    Ethernet3/1      1w0d        00:02:19    172.21.200.159
224.0.1.40         Ethernet3/1      1w0d        00:02:15    172.21.200.1
224.0.1.40         Ethernet3/3      1w0d        never       172.16.214.251
224.0.1.1          Ethernet3/1      1w0d        00:02:11    172.21.200.11
224.9.9.2          Ethernet3/1      1w0d        00:02:10    172.21.200.155
232.1.1.1          Ethernet3/1      5d21h       stopped     172.21.200.206
```

This example shows how to display output from the **show ip igmp groups** command with the *group-address* argument and **detail** keyword:

```
Router# show ip igmp groups 232.1.1.1 detail

Interface:      Ethernet3/2
Group:          232.1.1.1
Uptime:         01:58:28
Group mode:     INCLUDE
Last reporter:  10.0.119.133
CSR Grp Exp:    00:02:38
Group source list: (C - Cisco Src Report, U - URD, R - Remote)
  Source Address   Uptime    v3 Exp    CSR Exp   Fwd  Flags
  172.16.214.1     01:58:28  stopped   00:02:31  Yes  C
```

Table 2-48 describes the fields shown in the displays.

Table 2-48 show ip igmp groups Field Descriptions

Field	Description
Group Address	Address of the multicast group.
Interface	Interface through which the group is reachable.
Uptime	Time in weeks, days, hours, minutes, and seconds that this multicast group has been known.
Expires	Time in weeks, days, hours, minutes, and seconds until the entry expires. If an entry expires, then the entry (for a short period) shows "now" before it is removed. "never" indicates that the entry will not time out, because a local receiver is on this router for this entry. "stopped" indicates that timing out of this entry is not determined by this expire timer. If the router is in INCLUDE mode for a group, then the whole group entry times out after the last source entry has timed out (unless the mode is changed to EXCLUDE mode before it times out).
Last Reporter	Last host to report being a member of the multicast group. Both IGMP v3lite and URD require a v2-report.
Group mode:	Either INCLUDE or EXCLUDE. The group mode is based on the type of membership reports that are received on the interface for the group. In the output for the **show ip igmp groups detail** command, the EXCLUDE mode also shows the Expires: field for the group entry (not shown in the output).
CSR Grp Exp	Shown for multicast groups in the SSM range. It indicates the time (in hours, minutes, and seconds) since the last received group membership report was received. Cisco IOS software needs to use these reports for the operation of URD and IGMP v3lite, but the reports do not indicate group membership by themselves.
Group source list:	Details of which sources have been requested by the multicast group.
Source Address	IP address of the source.
Uptime	Time since the source state was created.

Table 2-48 show ip igmp groups Field Descriptions (continued)

Field	Description
v3 Exp	Time in hours, minutes, and seconds until the membership for the source times out according to IGMP operations. “stopped” displays if no member uses IGMPv3 (but only IGMP v3lite or URD).
CSR Exp	Time in hours, minutes, and seconds until the membership for the source times out according to IGMP v3lite or URD reports. “stopped” displays if members use only IGMPv3.
Fwd	Status of whether the router is forwarding multicast traffic due to this entry.
Flags	Information about the entry. The Remote flag indicates that an IGMPv3 report has been received by this source. The C flag indicates that an IGMP v3lite or URD report was received by this source. The U flag indicates that a URD report was received for this source.

Related Commands

Command	Description
ip igmp query-interval	Configures the frequency at which Cisco IOS software sends IGMP host query messages.

show ip igmp interface

To display the information about the IGMP-interface status and configuration, use the **show ip igmp interface** command.

show ip igmp [**vrf** *vrf-name*] **interface** [{*interface* [*interface-number*]} | {**null** *interface-number*} | {**vlan** *vlan-id*}]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
interface	(Optional) Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **atm**, and **ge-wan**.
interface-number	(Optional) Module and port number; see the "Usage Guidelines" section for valid values.
null *interface-number*	Specifies the null interface; the valid value is **0**.
vlan *vlan-id*	Specifies the VLAN; valid values are from 1 to 4094.

Command Default

If you do not specify a VLAN, information for VLAN 1 is shown.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

If you omit the optional arguments, the **show ip igmp interface** command displays information about all interfaces.

Examples

This example shows how to display IGMP information for VLAN 43:

```
Router# show ip igmp interface vlan 43
Vlan43 is up, line protocol is up
Internet address is 43.0.0.1/24
IGMP is enabled on interface
Current IGMP host version is 2
Current IGMP router version is 2
IGMP query interval is 60 seconds
IGMP querier timeout is 120 seconds
IGMP max query response time is 10 seconds
Last member query count is 2
Last member query response interval is 1000 ms
Inbound IGMP access group is not set
IGMP activity: 1 joins, 0 leaves
Multicast routing is enabled on interface
Multicast TTL threshold is 0
Multicast designated router (DR) is 43.0.0.1 (this system)
IGMP querying router is 43.0.0.1 (this system)
Multicast groups joined by this system (number of users):
224.0.1.40(1)
IGMP snooping is globally enabled
IGMP snooping is enabled on this interface
IGMP snooping fast-leave is disabled and querier is disabled
IGMP snooping explicit-tracking is enabled on this interface
IGMP snooping last member query interval on this interface is 1000 ms
Router#
```

Related Commands

Command	Description
clear ip igmp group	Deletes the entries for the IGMP-group cache.
show ip igmp snooping mrouter	Displays the information about the dynamically learned and manually configured multicast router interfaces.

show ip igmp snooping explicit-tracking

To display the information about the explicit host-tracking status for IGMPv3 hosts, use the **show ip igmp snooping explicit-tracking** command.

show ip igmp snooping explicit-tracking {**vlan** *vlan-id*}

Syntax Description

vlan *vlan-id*	Specifies the VLAN; see the "Usage Guidelines" section for valid values.

Command Default

If you do not specify a VLAN, information for VLAN 1 is shown.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Explicit host tracking is supported only with IGMPv3 hosts.

Examples

This example shows how to display the information about the explicit host-tracking status for IGMPv3 hosts:

```
Router# show ip igmp snooping explicit-tracking vlan 25

Source/Group       Interface Reporter Filter_mode
----------------------------------------------------------------------
10.1.1.1/226.2.2.2 Vl25:1/2 16.27.2.3 INCLUDE
10.2.2.2/226.2.2.2 Vl25:1/2 16.27.2.3 INCLUDE
Router#
```

Related Commands

Command	Description
ip igmp snooping explicit-tracking	Enables explicit host tracking.

show ip igmp snooping mrouter

To display the information about the dynamically learned and manually configured multicast router interfaces, use the **show ip igmp snooping mrouter** command.

show ip igmp snooping mrouter [{**vlan** *vlan-id*}]

Syntax Description

vlan *vlan-id*	(Optional) Specifies a VLAN; valid values are from 1 to 4094.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

You can also use the **show mac-address-table** command to display entries in the MAC-address table for a VLAN that has IGMP snooping enabled.

You can display IGMP snooping information for VLAN interfaces by entering the **show ip igmp vlan** *vlan-num* command.

Examples

This example shows how to display the information about IGMP snooping for a specific VLAN:

```
Router# show ip igmp snooping mrouter vlan 1
vlan            ports
-----+----------------------------------------
  1          Gi1/1,Gi2/1,Fa3/48,Router
Router#
```

Related Commands

Command	Description
ip igmp snooping mrouter	Configures a Layer 2 port as a multicast router port.

show ip igmp snooping rate-limit

To display the information about the IGMP snooping rate limit, use the **show ip igmp snooping rate-limit** command.

show ip igmp snooping rate-limit [**statistics** | **vlan** *vlan-id*]

Syntax Description

statistics	(Optional) Displays IGMP snooping statistics.
vlan *vlan-id*	(Optional) Specifies a VLAN; valid values are from 1 to 4094.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to display the statistics for IGMP snooping rate limiting:

```
Router# show ip igmp snooping rate-limit statistics

Max IGMP messages incoming rate : Not configured
Vlan   Incoming rate  Rate-limiting ON  Disable count  Time to Enable
-----+---------------+----------------+---------------+---------------+
222   1000            No               0
111   5999            Yes              3               185

Router#
```

This example shows how to display IGMP snooping rate-limit information for a specific VLAN:

```
Router# show ip igmp snooping rate-limit vlan 19
Max IGMP messages incoming rate : 200 pps
Vlan       Incoming IGMP rate (in pps)
--------+--------------------------------
19       200
Router#
```

Related Commands

Command	Description
ip igmp snooping rate	Sets the rate limit for IGMP snooping packets.

show ip igmp snooping statistics

To display IGMPv3 statistics, use the **show ip igmp snooping statistics** command.

show ip igmp snooping statistics [{**interface** *interface* [*interface-number*]} | {**port-channel** *number*} | {**vlan** *vlan-id*}]

Syntax Description

interface *interface*	(Optional) Displays IGMP statistics for the specified interface type; possible valid values are **ethernet**, **fastethernet**, and **gigabitethernet**.
interface-number	(Optional) Multicast-related statistics for the specified module and port; see the "Usage Guidelines" section for valid values.
port-channel *number*	(Optional) Displays multicast-related statistics for the specified port-channel; valid values are from 1 to 282.
vlan *vlan-id*	(Optional) Displays multicast-related statistics for the specified VLAN; valid values for *vlan-id* are from 1 to 4094.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The **show ip igmp snooping statistics** command displays the following statistics:

- List of ports that are members of a group
- Filter mode
- Reporter-address behind the port
- Additional information (such as the last-join and last-leave collected since the previous time that a **clear ip igmp snooping statistics** command was issued)

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The **port-channel** *number* values from 257 to 282 are supported on the CSM and the FWSM only.

The #hosts behind the VLAN is displayed only if you define the max-hosts policy on the specified VLAN and enable the log policy for the specified VLAN.

Examples

This example shows how to display IGMPv3 statistics:

```
Router# show ip igmp snooping statistics interface FastEthernet5/1

IGMP Snooping statistics
Service-policy: Policy1policy tied with this interface
#Channels: 3
#hosts : 3
Query Rx: 2901 GS Query Rx: 0 V3 Query Tot Rx: 0
Join Rx: 8686 Leave Rx: 0 V3 Report Rx: 2300
Join Rx from router ports: 8684 Leave Rx from router ports: 0
Total Rx: 11587
Channel/Group        Interface    Reporter   Uptime    Last-Join    Last-Leave
10.7.20.1,239.1.1.1  F5/1         10.5.20.1  00:12:00  1:10:00      -
10.7.30.1,239.1.1.1 F5/1         10.5.30.1  00:50:10  1:10:02      0:30:02
10.7.40.1,239.1.1.1 F5/1         10.5.40.1  00:10:10  1:10:03      -
Router#
```

Table 2-49 describes the fields that are shown in the example.

Table 2-49 show ip igmp snooping statistics Field Descriptions

Field	Description
Service-policy: Policy1	Policy tied to this interface.
#Channels: 3	Number of channels behind the specified interface.
#hosts	Number of hosts behind the specified interface. This field is displayed only if max-hosts policy is used.

Related Commands

Command	Description
clear ip igmp snooping statistics	Clears the IGMP snooping statistics.

show ip igmp udlr

To display UDLR information for the connected multicast groups on the interfaces that have a UDL helper address configured, use the **show ip igmp udlr** command.

show ip igmp udlr [*group-name* | *group-address* | *interface-type interface-number*]

Syntax Description

group-name	(Optional) Name of the multicast group.
group-address	(Optional) Address of the multicast group.
interface-type interface-number	(Optional) Interface type and number.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command displays which groups are being forwarded and received over the UDL.

On the upstream router, this command shows which interface is a UDL interface and which IP multicast groups are being forwarded out that interface. The UDL Reporter is the IP address of the downstream interface on the receiving router. If there is more than one downstream router, this field shows which downstream router forwarded the IGMP host report to the upstream router over the ground-based network. This report is forwarded over the UDL so that all downstream routers know which groups have already been requested by other downstream routers, and additional IGMP host reports are suppressed.

On the downstream router, this command (in the Interface field) shows which local interface received an IGMP host report (from a connected host for a specific group). The UDL Reporter is the IP address of the router that had forwarded the IGMP host report to the upstream router over the ground-based network. The UDL Interfaces column shows the interface on which IP multicast packets are being received.

Examples

This example shows the output of the **show ip igmp udlr** command on an upstream router:

```
Router# show ip igmp udlr

IGMP UDLR Status, UDL Interfaces: Serial0
Group Address    Interface           UDL Reporter     Reporter Expires
224.2.127.254    Serial0             10.0.0.2         00:02:12
224.0.1.40       Serial0             10.0.0.2         00:02:11
225.7.7.7        Serial0             10.0.0.2         00:02:15
Router#
```

This example shows the output of the **show ip igmp udlr** command on a downstream router:

```
Router# show ip igmp udlr

IGMP UDLR Status, UDL Interfaces: Serial0
Group Address     Interface            UDL Reporter     Reporter Expires
224.2.127.254     Serial0              10.0.0.2         00:02:49
224.0.1.40        Serial0              10.0.0.2         00:02:48
225.7.7.7         Serial0              10.0.0.2         00:02:52
Router#
```

Table 2-50 describes the fields shown in the output of the **show ip igmp udlr** command.

Table 2-50 show ip igmp udlr Field Descriptions

Field	Description
Group Address	All group's helper addresses on the interface.
Interface	Interface type and number to which the group is connected.
UDL Reporter	IP address of the router on the UDL network that is IGMP helping for the group.
Reporter Expires	How soon the UDL Reporter will become inactive, in hours:minutes:seconds. This can occur under the following conditions: • The UDL Reporter has become nonoperational. • The link or network to the reporter has become nonoperational. • The group member attached to the UDL Reporter has left the group.

show ip interface

To display the usability status of interfaces that are configured for IP, use the **show ip interface** command.

show ip interface [*type number*]

Syntax Description

type	(Optional) Interface type.
number	(Optional) Interface number.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The Cisco IOS software automatically enters a directly connected route in the routing table if the interface is usable. A usable interface is one through which the software can send and receive packets. If the software determines that an interface is not usable, it removes the directly connected routing entry from the routing table. Removing the entry allows the software to use dynamic routing protocols to determine backup routes to the network, if any.

If the interface can provide two-way communication, the line protocol is marked “up.” If the interface hardware is usable, the interface is marked “up.”

If you specify an optional interface type, you see only information on that specific interface.

If you specify no optional arguments, you see information on all the interfaces.

When an asynchronous interface is encapsulated with PPP or Serial Line Internet Protocol (SLIP), IP fast switching is enabled. The **show ip interface** command on an asynchronous interface that is encapsulated with PPP or SLIP displays a message indicating that IP fast switching is enabled.

Examples

This example shows how to display the usability status for a specific VLAN:

```
Router# show ip interface vlan 1
Vlan1 is up, line protocol is up
  Internet address is 10.6.58.4/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Fast switching turbo vector
  IP Normal CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
  Sampled Netflow is disabled
  IP multicast multilayer switching is disabled
  Netflow Data Export (hardware) is enabled
Router#
```

Table 2-51 describes the fields that are shown in the example.

Table 2-51 show ip interface Field Descriptions

Field	Description
Ethernet0 is up	If the interface hardware is usable, the interface is marked “up.” For an interface to be usable, both the interface hardware and line protocol must be up.
line protocol is up	If the interface can provide two-way communication, the line protocol is marked “up.” For an interface to be usable, both the interface hardware and line protocol must be up.
Internet address and subnet mask	IP address and subnet mask of the interface.
Broadcast address	Broadcast address.
Address determined by...	Status of how the IP address of the interface was determined.
MTU	MTU value that is set on the interface.
Helper address	Helper address, if one has been set.
Secondary address	Secondary address, if one has been set.
Directed broadcast forwarding	Status of directed broadcast forwarding.
Multicast groups joined	Multicast groups to which this interface belongs.
Outgoing access list	Status of whether the interface has an outgoing access list set.
Inbound access list	Status of whether the interface has an incoming access list set.

Table 2-51 show ip interface Field Descriptions (continued)

Field	Description
Proxy ARP	Status of whether Proxy Address Resolution Protocol (ARP) is enabled for the interface.
Security level	IP Security Option (IPSO) security level set for this interface.
Split horizon	Status of the split horizon.
ICMP redirects	Status of the redirect messages on this interface.
ICMP unreachables	Status of the unreachable messages on this interface.
ICMP mask replies	Status of the mask replies on this interface.
IP fast switching	Status of whether fast switching has been enabled for this interface. Fast switching is typically enabled on serial interfaces, such as this one.
IP SSE switching	Status of the IP silicon switching engine (SSE).
Router Discovery	Status of the discovery process for this interface. It is typically disabled on serial interfaces.
IP output packet accounting	Status of IP accounting for this interface and the threshold (maximum number of entries).
TCP/IP header compression	Status of compression.
Probe proxy name	Status of whether the HP Probe proxy name replies are generated.
WCCP Redirect outbound is enabled	Status of whether packets that are received on an interface are redirected to a cache engine.
WCCP Redirect exclude is disabled	Status of whether packets that are targeted for an interface are excluded from being redirected to a cache engine.
Netflow Data Export (hardware) is enabled	NDE hardware flow status on the interface.

show ip mcache

To display the contents of the IP fast-switching cache, use the **show ip mcache** command.

show ip mcache [**vrf** *vrf-name*] [*group-address* | *group-name*] [*source-address* | *source-name*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
group-address | *group-name*	(Optional) Fast-switching cache for the single group.
source-address | *source-name*	(Optional) If the source address or name is also specified, displays a single multicast cache entry.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The *group-address* | *group-name* can be either a Class D IP address or a DNS name.

The *source-address* | *source-name* can be either a unicast IP address or a DNS name.

Examples

This example shows how to display the contents of the IP fast-switching cache. This entry shows a specific source (wrn-source 226.62.246.73) sending to the World Radio Network group (224.2.143.24):

```
Router> show ip mcache wrn wrn-source

IP Multicast Fast-Switching Cache
(226.62.246.73/32, 224.2.143.24), Fddi0, Last used: 00:00:00
  Ethernet0       MAC Header: 01005E028F1800000C1883D30800
  Ethernet1       MAC Header: 01005E028F1800000C1883D60800
  Ethernet2       MAC Header: 01005E028F1800000C1883D40800
  Ethernet3       MAC Header: 01005E028F1800000C1883D70800
```

Table 2-52 describes the fields shown in the display.

Table 2-52 show ip mcache Field Descriptions

Field	Description
226.62.246.73	Source address.
224.2.143.24	Destination address.
Fddi0	Incoming or expected interface on which the packet should be received.

Table 2-52 show ip mcache Field Descriptions (continued)

Field	Description
Last used:	Latest time that the entry was accessed for a packet that was successfully fast switched. "Semi-fast" indicates that the first part of the outgoing interface list is fast switched and the rest of the list is process level switched.
Ethernet0 MAC Header:	Outgoing interface list and respective MAC header that is used when rewriting the packet for output. If the interface is a tunnel, the MAC header shows the real next-hop MAC header and, in parentheses, the real interface name.

show ip mds interface

To display MDS information for all the interfaces on the module, use the **show ip mds interface** command.

show ip mds interface [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to display MDS information for all the interfaces on the module:

```
Router# show ip mds interface

Interface                SW-Index  HW-Index  HW IDB      FS Vector   VRF
Ethernet1/0/0            2         1         0x60C2DB40  0x602FB7A4 default
Ethernet1/0/1            3         2         0x60C32280  0x603D52B8 default
Ethernet1/0/2            4         3         0x60C35E40  0x602FB7A4 default
Ethernet1/0/3            5         4         0x60C39E60  0x603D52B8 default
Ethernet1/0/4            6         5         0x60C3D780  0x602FB7A4 default
Ethernet1/0/5            7         6         0x60C41140  0x602FB7A4 default
Ethernet1/0/6            8         7         0x60C453A0  0x602FB7A4 default
Ethernet1/0/7            9         8         0x60C48DC0  0x602FB7A4 default
POS2/0/0                 10        9         0x0                    default
POS3/0/0                 11        10        0x0                    default
Virtual-Access1          13        11        0x0                    default
Loopback0                14        12        0x0                    default
Tunnel0                  15        23        0x61C2E480  0x603D52B8  vrf1
Tunnel1                  16        24        0x61C267E0  0x603D52B8  vrf2
Ethernet1/0/3.1          17        4         0x60C39E60  0x603D52B8  vrf1
Ethernet1/0/3.2          18        4         0x60C39E60  0x603D52B8  vrf2
```

Table 2-53 describes the fields shown in the display.

Table 2-53 show ip mds interface Field Descriptions

Field	Description
Interface	Specified interface.
SW-Index	Software index.
HW-Index	Hardware index.

Table 2-53 show ip mds interface Field Descriptions (continued)

Field	Description
HW IDB	Hardware interface description block.
VRF	VPN routing/forwarding instance.

show ip mpacket

To display the contents of the circular cache-header buffer, use the **show ip mpacket** command.

show ip mpacket [**vrf** *vrf-name*] [*group-address* | *group-name*] [*source-address* | *source-name*] [**detail**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
group-address | *group-name*	(Optional) Cache headers matching the specified group address or group name.
source-address | *source-name*	(Optional) Cache headers matching the specified source address or source name.
detail	(Optional) In addition to the summary information, displays the rest of the IP header fields on an additional line, plus the first 8 bytes after the IP header (usually the UDP port numbers).

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is applicable only when the **ip multicast cache-headers** command is in effect.

Each time that this command is entered, a new buffer is allocated. The summary display (when the **detail** keyword is omitted) shows the IP packet identifier, time-to-live (TTL) value, source and destination IP addresses, and a local time stamp when the packet was received.

The two arguments and one keyword can be used in the same command in any combination.

Examples

This example shows how to display the contents of the circular cache-header buffer:

```
Router # show ip mpacket smallgroup

IP Multicast Header Cache - entry count:6, next index: 7
Key: id/ttl timestamp (name) source group

D782/117 206416.908 (ABC-xy.company.com) 192.168.228.10 224.5.6.7
7302/113 206417.908 (school.edu) 147.12.2.17 224.5.6.7
6CB2/114 206417.412 (MSSRS.company.com) 154.2.19.40 224.5.6.7
D782/117 206417.868 (ABC-xy.company.com) 192.168.228.10 224.5.6.7
E2E9/123 206418.488 (Newman.com) 211.1.8.10 224.5.6.7
1CA7/127 206418.544 (teller.company.com) 192.168.6.10 224.5.6.7
```

Table 2-54 describes the fields shown in the display.

Table 2-54 show ip mpacket Field Descriptions

Field	Description
entry count	Number of packets cached (one packet for each line in the display). The cache has lines numbered from 0 to 1024.
next index	Index for the next element in the cache.
id	Identification number of the IP packet.
ttl	Current TTL of the packet.
timestamp	Time-stamp sequence number of the packet.
(name)	DNS name of the source sending to the group. Name appears in parentheses.
source	IP address of the source sending to the group.
group	Multicast group address to which the packet is sent. In this example, the group address is the group name smallgroup.

Related Commands

Command	Description
ip multicast cache-headers	Allocates a circular buffer to store IP multicast packet headers that the router receives.

show ip mroute

To display the information about the IP-multicast routing table, use the **show ip mroute** command.

show ip mroute [**vrf** *vrf-name*] [{*interface interface-number*} | {**null** *interface-number*} | {**port-channel** *number*} | {**vlan** *vlan-id*} | {{*host-name* | *host-address*} [*source*]} | {**active** [*kbps* | {*interface-type num*}]} | {**count** | **pruned** | **static** | **summary**}]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
interface	(Optional) Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **atm**, and **ge-wan**.
interface-number	(Optional) Module and port number; see the "Usage Guidelines" section for valid values.
null *interface-number*	(Optional) Specifies the null interface; the valid value is **0**.
port-channel *number*	(Optional) Specifies the channel interface; valid values are a maximum of 64 values ranging from 1 to 282.
vlan *vlan-id*	(Optional) Specifies the VLAN; valid values are from 1 to 4094.
host-name | *host-address*	(Optional) Name or IP address as defined in the DNS hosts table.
source	(Optional) IP address or name of a multicast source.
active	(Optional) Displays the rate that active sources are sending to multicast groups.
kbps	(Optional) Minimum rate at which active sources are sending to multicast groups; active sources sending at this rate or greater are displayed. Valid values are from 1 to 4294967295 kbps.
count	(Optional) Displays the route and packet count information.
pruned	(Optional) Displays the pruned routes.
static	(Optional) Displays the static multicast routes.
summary	(Optional) Displays a one-line, abbreviated summary of each entry in the IP-multicast routing table.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

If you omit all optional arguments and keywords, the **show ip mroute** command displays all entries in the IP-multicast routing table.

The **show ip mroute active** *kbps* command displays all sources sending at a rate greater than or equal to *kbps*.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The **port-channel** *number* values are from 257 to 282 are supported on the CSM and the FWSM only.

The multicast routing table is populated by creating source, group (S,G) entries from star, group (*,G) entries. The star refers to all source addresses, the "S" refers to a single source address, and the "G" is the destination multicast group address. In creating (S,G) entries, the software uses the best path to that destination group that is found in the unicast routing table (through RPF).

Examples

This example shows how to display all entries in the IP-multicast routing table:

```
Router# show ip mroute 224.1.1.1
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel
       Y - Joined MDT-data group, y - Sending to MDT-data group, s - SSM
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 224.1.1.1), 00:00:07/00:02:59, RP 2.0.0.1, flags: BC
  Bidir-Upstream: Null, RPF nbr 0.0.0.0, RPF-MFD
  Outgoing interface list:
    Vlan202, Forward/Sparse-Dense, 00:00:07/00:02:59, H
Router#
```

This example shows how to display the rate that active sources are sending to multicast groups and to display only active sources sending at greater than the default rate:

```
Router# show ip mroute active

Active IP Multicast Sources - sending >= 4 kbps

Group: 224.2.127.254, (sdr.cisco.com)
   Source: 146.137.28.69 (mbone.ipd.anl.gov)
     Rate: 1 pps/4 kbps(1sec), 4 kbps(last 1 secs), 4 kbps(life avg)

Group: 224.2.201.241, ACM 97
   Source: 130.129.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 9 pps/93 kbps(1sec), 145 kbps(last 20 secs), 85 kbps(life avg)

Group: 224.2.207.215, ACM 97
   Source: 130.129.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 3 pps/31 kbps(1sec), 63 kbps(last 19 secs), 65 kbps(life avg)
Router#
```

This example shows how to display the information about the route and packet count:

```
Router# show ip mroute count
IP Multicast Statistics
56 routes using 28552 bytes of memory
13 groups, 3.30 average sources per group
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second

Other counts:Total/RPF failed/Other drops(OIF-null, rate-limit etc)

Group:224.2.136.89, Source count:1, Group pkt count:29051
  Source:132.206.72.28/32, Forwarding:29051/-278/1186/0, Other:85724/8/56665
Router#
```

This example shows how to display summary information:

```
Router# show ip mroute summary
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, s - SSM Group, C - Connected, L - Local,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT, M - MSDP created entry, X - Proxy Join Timer Running
       A - Advertised via MSDP, U - URD, I - Received Source Specific Host
           Report
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

Router#
```

Table 2-55 describes the fields that are shown in the example.

Table 2-55 show ip mroute Field Descriptions

Field	Description
Flags:	Information about the entry.
D - Dense	Entry is operating in dense mode.
S - Sparse	Entry is operating in sparse mode.
s - SSM Group	Entry is a member of an SSM group.
C - Connected	Member of the multicast group is present on the directly connected interface.
L - Local	Router is a member of the multicast group.
P - Pruned	Route has been pruned. This information is retained in case a downstream member wants to join the source.
R - Rp-bit set	Status of whether the (S,G) entry is pointing toward the route processor. This field shows a prune state along the shared tree for a particular source.
F - Register flag	Status of whether the software is registering for a multicast source.
T - SPT-bit set	Status of whether the packets have been received on the shortest-path tree.

Table 2-55 show ip mroute Field Descriptions (continued)

Field	Description
J - Join SPT	For (*, G) entries, indicates that the rate of traffic flowing down the shared tree is exceeding the SPT-Threshold that is set for the group. (The default SPT-Threshold setting is 0 kbps.) When the J - Join SPT flag is set, the next (S,G) packet that is received down the shared tree triggers an (S,G) join in the direction of the source causing the router to join the source tree. For (S,G) entries, indicates that the entry was created because the SPT-Threshold for the group was exceeded. When the J - Join SPT flag is set for (S,G) entries, the router monitors the traffic rate on the source tree and attempts to switch back to the shared tree for this source if the traffic rate on the source tree falls below the group's SPT-Threshold for more than 1 minute. The router measures the traffic rate on the shared tree and compares the measured rate to the group's SPT-Threshold once every second. If the traffic rate exceeds the SPT-Threshold, the J - Join SPT flag is set on the (*, G) entry until the next measurement of the traffic rate. The flag is cleared when the next packet arrives on the shared tree and a new measurement interval is started. If the default SPT-Threshold value of 0 Kbps is used for the group, the J - Join SPT flag is always set on (*, G) entries and is never cleared. When the default SPT-Threshold value is used, the router immediately switches to the shortest-path tree when traffic from a new source is received.
Bidir-Upstream: Null, RPF nbr 0.0.0.0, RPF-MFD	Interface that is used to reach the PIM route processor. Set to Null if the router is the PIM route processor or if no route exists to the PIM route processor.
Outgoing interface flags:	Information about the outgoing entry.
H - Hardware switched	Entry is hardware switched.
Timers:	Uptime/Expires.
Interface state:	Interface, Next-Hop or VCD, State/Mode.
(*, 224.0.255.1) (198.92.37.100/32, 224.0.255.1)	Entry in the IP-multicast routing table. The entry consists of the IP address of the source router followed by the IP address of the multicast group. An asterisk (*) in place of the source router indicates all sources. Entries in the first format are referred to as (*,G) or "star comma G" entries. Entries in the second format are referred to as (S,G) or "S comma G" entries. (*,G) entries are used to build (S,G) entries.
uptime	Hours, minutes, and seconds that the entry has been in the IP-multicast routing table.
expires	Hours, minutes, and seconds until the entry is removed from the IP-multicast routing table on the outgoing interface.

Table 2-55 show ip mroute Field Descriptions (continued)

Field	Description
RP	Address of the route processor. For routers and access servers operating in sparse mode, this address is always 0.0.0.0.
flags:	Information about the entry.
Incoming interface:	Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.
RPF neighbor	IP address of the upstream router to the source. Tunneling indicates that this router is sending data that is encapsulated in register packets to the route processor. The hexadecimal number in parentheses indicates to which route processor it is registering. Each bit indicates a different route processor if multiple route processors per group are used.
Dvmrp or Mroute	Status of whether the RPF information is obtained from the DVMRP routing table or the static mroute configuration.
Outgoing interface list:	Interfaces through which packets are forwarded. When you enable the **ip pim nbma-mode** command on the interface, the IP address of the PIM neighbor is also displayed.
Ethernet0	Name and number of the outgoing interface.
Next hop or VCD	Next hop specifies the downstream neighbor's IP address. VCD specifies the virtual-circuit descriptor number. VCD0 indicates that the group is using the static-map virtual circuit.
Forward/Dense	Status of whether the packets are forwarded on the interface if there are no restrictions due to access lists or the TTL threshold. Following the slash (/), the mode in which the interface is operating (dense or sparse).
Forward/Sparse	Sparse mode interface is in forward mode.
time/time (uptime/expiration time)	Per interface, the duration in hours, minutes, and seconds that the entry has been in the IP-multicast routing table. Specifies that following the slash (/), the duration in hours, minutes, and seconds until the entry is removed from the IP-multicast routing table.

Related Commands

Command	Description
ip multicast-routing	Enables IP multicast routing.
ip pim	Enables PIM on an interface.

show ip mroute bidirectional

To display Bidir information from the IP-multicast routing table, use the **show ip mroute bidirectional** command.

show ip mroute bidirectional [{*interface interface-number*} | {**null** *interface-number*} | {**port-channel** *number*} | {**vlan** *vlan-id*} | {{*host-name* | *host-address*} [*source*]} | {**active** [*kbps* | {*interface-type num*}]} | {**count** | **pruned** | **static** | **summary**}]

Syntax Description

interface	(Optional) Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **atm**, and **ge-wan**.
interface-number	Module and port number; see the "Usage Guidelines" section for valid values.
null *interface-number*	Specifies the null interface; the valid value is **0**.
port-channel *number*	Specifies the channel interface; valid values are a maximum of 64 values ranging from 1 to 282.
vlan *vlan-id*	Specifies the VLAN; valid values are from 1 to 4094.
host-name | *host-address*	(Optional) Name or IP address as defined in the DNS hosts table.
source	(Optional) IP address or name of a multicast source.
active	(Optional) Displays the rate that active sources are sending to multicast groups.
kbps	(Optional) Minimum rate at which active sources are sending to multicast groups; active sources sending at this rate or greater are displayed. Valid values are from 1 to 4294967295 kbps.
count	(Optional) Displays the route and packet count.
pruned	(Optional) Displays the pruned routes.
static	(Optional) Displays the static multicast routes.
summary	(Optional) Displays a one-line, abbreviated summary of each entry in the IP-multicast routing table.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

If you omit all optional arguments and keywords, the **mroute bidirectional** command displays all entries in the IP-multicast routing table.

Examples

This example shows how to display the information in the IP-multicast routing table that is related to bidirectional PIM:

```
Router# show ip mroute bidirectional
(*, 225.1.3.0), 00:00:02/00:02:57, RP 3.3.3.3, flags:BC
Bidir-Upstream:GigabitEthernet2/1, RPF nbr 10.53.1.7, RPF-MFD
Outgoing interface list:
GigabitEthernet2/1, Bidir-Upstream/Sparse-Dense, 00:00:02/00:00:00,H
Vlan30, Forward/Sparse-Dense, 00:00:02/00:02:57, H
(*, 225.1.2.0), 00:00:04/00:02:55, RP 3.3.3.3, flags:BC
Bidir-Upstream:GigabitEthernet2/1, RPF nbr 10.53.1.7, RPF-MFD
Outgoing interface list:
GigabitEthernet2/1, Bidir-Upstream/Sparse-Dense, 00:00:04/00:00:00,H
Vlan30, Forward/Sparse-Dense, 00:00:04/00:02:55, H
(*, 225.1.4.1), 00:00:00/00:02:59, RP 3.3.3.3, flags:BC
Bidir-Upstream:GigabitEthernet2/1, RPF nbr 10.53.1.7, RPF-MFD
Outgoing interface list:
GigabitEthernet2/1, Bidir-Upstream/Sparse-Dense, 00:00:00/00:00:00,H
Vlan30, Forward/Sparse-Dense, 00:00:00/00:02:59, H
Router#
```

show ip msdp count

To display the number of sources and groups that originated in MSDP source-active messages and the number of source-active messages from an MSDP peer in the source-active cache, use the **show ip msdp count** command.

show ip msdp [**vrf** *vrf-name*] **count** [*as-number*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
as-number	(Optional) Number of sources and groups that originated in source-active messages from the specified autonomous system number.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

You must enter the **ip msdp cache-sa-state** command for this command to obtain any output from the **show ip msdp** command.

Examples

This example shows how to display the number of sources and groups that originated in MSDP source-active messages and the number of source-active messages from an MSDP peer in the source-active cache:

```
Router# show ip msdp count

SA State per Peer Counters, <Peer>: <# SA learned>
 224.135.250.116: 24
 172.16.240.253: 3964
 172.16.253.19: 10
 172.16.170.110: 11

SA State per ASN Counters, <asn>: <# sources>/<# groups>
 Total entries: 4009
 ?: 192/98, 9: 1/1, 14: 107/57, 17: 7/5
 18: 4/3, 25: 23/17, 26: 39/27, 27: 2/2
 32: 19/7, 38: 2/1, 52: 4/4, 57: 1/1
 68: 4/4, 73: 12/8, 81: 19/1, 87: 9/6
 .
 .
 .
```

Table 2-56 describes the fields shown in the display.

Table 2-56 show ip msdp count Field Descriptions

Field	Description
224.135.250.116: 24	MSDP peer with IP address 224.135.250.116: 24 source-active messages from the MSDP peer in the source-active cache.
Total entries	Total number of source-active entries in the source-active cache.
9: 1/1	Autonomous system 9: 1 source/1 group.

Related Commands

Command	Description
ip msdp cache-sa-state	Creates a source-active state on the router.

show ip msdp peer

To display detailed information about the MSDP peer, use the **show ip msdp peer** command.

show ip msdp [**vrf** *vrf-name*] **peer** [*peer-address* | *peer-name*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
peer-address | *peer-name*	(Optional) DNS name or IP address of the MSDP peer for which information is displayed.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to display detailed information about the MSDP peer:

```
Router# show ip msdp peer 224.135.250.116

MSDP Peer 224.135.250.116 (rtp5-rp1.cisco.com), AS 109 (configured AS)
Description:
 Connection status:
   State: Up, Resets: 9, Connection source: Loopback2 (228.69.199.17)
   Uptime(Downtime): 1d10h, Messages sent/received: 436765/429062
   Output messages discarded: 0
   Connection and counters cleared 1w2d     ago
 SA Filtering:
   Input (S,G) filter: none, route-map: none
   Input RP filter: none, route-map: none
   Output (S,G) filter: none, route-map: none
   Output RP filter: none, route-map: none
 SA-Requests:
   Input filter: none
   Sending SA-Requests to peer: disabled
 Peer ttl threshold: 0
 SAs learned from this peer: 32, SAs limit: 500
 Input queue size: 0, Output queue size: 0
```

Table 2-57 describes the fields shown in the display.

Table 2-57 show ip msdp peer Field Descriptions

Field	Description
MSDP Peer	IP address of the MSDP peer.
AS	Autonomous system to which the MSDP peer belongs.
State:	State of the MSDP peer.
Connection source:	Interface used to obtain the IP address for the TCP local connection address.
Uptime(Downtime):	Days and hours that the MSDP peer is up or down. If the time is less than 24 hours, it is shown in hours:minutes:seconds.
Messages sent/received:	Number of source-active messages sent to the MSDP peer/number of source-active messages received from the MSDP peer.
SA Filtering:	Information regarding access list filtering of source-active input and output if any.
SA-Requests:	Information regarding access list filtering of source-active requests if any.
SAs learned from this peer:	Number of source-active messages from the MSDP peer in the source-active cache.
SAs limit:	Source-active message limit for this MSDP peer.

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.

show ip msdp sa-cache

To display the (S,G) state that is learned from MSDP peers, use the **show ip msdp sa-cache** command.

show ip msdp [**vrf** *vrf-name*] **sa-cache** [*group-address* | *source-address* | *group-name* | *source-name*] [*group-address* | *source-address* | *group-name* | *source-name*] [*as-number*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
group-address | *source-address* | *group-name* | *source-name*	(Optional) Group address, source address, group name, or source name of the group or source about which (S,G) information is displayed.
as-number	(Optional) Only state originated by the autonomous system number specified is displayed.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The state is cached only if you enter the **ip msdp cache-sa-state** command.

If you specify two addresses or names, an (S,G) entry corresponding to those addresses is displayed. If you specify one group address only, all sources for that group are displayed.

If no options are specified, the entire source-active cache is displayed.

Examples

This example shows how to display the (S,G) state that is learned from MSDP peers:

```
Router# show ip msdp sa-cache

MSDP Source-Active Cache - 2398 entries
(172.16.41.33, 238.105.148.0), RP 172.16.3.111, MBGP/AS 704, 2d10h/00:05:33
(172.16.112.8, 224.2.0.1), RP 192.168.200.65, MBGP/AS 10888, 00:03:21/00:02:38
(172.16.10.13, 227.37.32.1), RP 192.168.3.92, MBGP/AS 704, 05:22:20/00:03:32
(172.16.66.18, 233.0.0.1), RP 192.168.3.111, MBGP/AS 704, 2d10h/00:05:35
(172.16.66.148, 233.0.0.1), RP 192.168.3.111, MBGP/AS 704, 2d10h/00:05:35
(172.16.10.13, 227.37.32.2), RP 192.168.3.92, MBGP/AS 704, 00:44:30/00:01:31
(172.16.70.203, 224.2.236.2), RP 192.168.253.7, MBGP/AS 3582, 02:34:16/00:05:49
(172.18.42.104, 236.195.56.2), RP 192.168.3.92, MBGP/AS 704, 04:21:13/00:05:22
(172.16.10.13, 227.37.32.3), RP 192.168.3.92, MBGP/AS 704, 00:44:30/00:02:31
(172.18.15.43, 224.0.92.3), RP 192.168.200.65, MBGP/AS 10888, 6d09h/00:05:35
(172.18.15.111, 224.0.92.3), RP 192.168.200.65, MBGP/AS 10888, 16:18:08/00:05:35
(172.18.21.45, 224.0.92.3), RP 192.168.200.65, MBGP/AS 10888, 16:18:08/00:05:35
(172.18.15.75, 224.0.92.3), RP 192.168.200.65, MBGP/AS 10888, 08:40:52/00:05:35
```

```
(172.18.15.100, 224.0.92.3), RP 192.168.200.65, MBGP/AS 10888, 08:40:52/00:05:35
(172.16.10.13, 227.37.32.6), RP 192.168.3.92, MBGP/AS 704, 00:45:30/00:05:31
(172.18.41.33, 224.247.228.10), RP 192.168.3.111, MBGP/AS 704, 2d10h/00:05:35
(172.18.222.210, 224.2.224.13), RP 192.168.3.92, MBGP/AS 704, 01:51:53/00:05:22
(172.18.41.33, 229.231.124.13), RP 192.168.3.111, MBGP/AS 704, 2d10h/00:05:33
(172.18.32.138, 224.2.200.23), RP 192.168.253.7, MBGP/AS 3582, 21:33:40/00:05:49
(172.18.75.244, 224.2.200.23), RP 192.168.253.7, MBGP/AS 3582, 21:33:40/00:05:49
```

Table 2-58 describes the fields shown in the display.

Table 2-58 show ip msdp sa-cache Field Descriptions

Field	Description
(172.16.41.33, 238.105.148.0)	First address (source) that is sending to the second address (group).
RP 172.16.3.111	Rendezvous point address in the originating domain where the source-active messages started.
MBGP/AS 704	Rendezvous point that is in autonomous system 704 according to multiprotocol BGP.
2d10h/00:05:33	Route that has been cached for 2 days and 10 hours. If no source-active message is received in 5 minutes and 33 seconds, the route is removed from the source-active cache.

Related Commands

Command	Description
clear ip msdp sa-cache	Clears MSDP source active cache entries.
ip msdp cache-sa-state	Creates a source-active state on the router.

show ip msdp summary

To display the MSDP peer status, use the **show ip msdp summary** command.

show ip msdp [**vrf** *vrf-name*] **summary**

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to display the MSDP peer status:

```
Router# show ip msdp summary

MSDP Peer Status Summary
Peer Address     AS    State    Uptime/  Reset SA    Peer Name
                                Downtime Count Count
224.135.250.116  109   Up       1d10h    9     111   rtp5-rp1
*172.20.240.253 1239  Up       14:24:00 5     4010  sl-rp-stk
172.16.253.19    109   Up       12:36:17 5     10    shinjuku-rp1
172.16.170.110   109   Up       1d11h    9     12    ams-rp1
```

Table 2-59 describes the fields shown in the display.

Table 2-59 show ip msdp summary Field Descriptions

Field	Description
Peer Address	IP address of the MSDP peer.
AS	Autonomous system to which the MSDP peer belongs.
State	State of the MSDP peer.
Uptime/Downtime	Days and hours that the MSDP peer is up or down per the state that is shown in the previous column. If the time is less than 24 hours, it is shown in hours:minutes:seconds.
SA Count	Number of source-active messages from this MSDP peer in the source-active cache.
Peer Name	Name of the MSDP peer.

show ip nhrp

To display information about the NHRP cache, use the **show ip nhrp** command.

show ip nhrp [**summary** | **dynamic** | **static** | **incomplete**] [{*interface-type interface-number*} | *ip-address*] [**detail** | **brief**]

Syntax Description

summary	(Optional) Displays a summary of NHRP cache purge information.
dynamic	(Optional) Displays the dynamic (learned) IP-to-NBMA cache entries only.
static	(Optional) Displays the static IP-to-NBMA address cache entries only (configured using the **ip nhrp map** command).
incomplete	(Optional) Displays information about an incomplete cache.
interface-type interface-number	(Optional) NHRP cache information for the specified interface type only; see Table 2-60 for types, number ranges, and descriptions.
ip-address	(Optional) NHRP cache information for the specified IP address only.
detail	(Optional) Displays detailed information about the NHRP cache.
brief	(Optional) Displays basic information about the NHRP cache.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Table 2-60 lists the valid types, number ranges, and descriptions for the *type* and *number* optional arguments.

Note The valid types can vary according to the platform and interfaces on the platform.

Table 2-60 Valid Types, Number Ranges, and Interface Descriptions

Valid Types	Number Ranges	Interface Descriptions
async	1	Async
ctunnel	0 to 2147483647	C-Tunnel
dialer	0 to 20049	Dialer
fastethernet	0 to 6	Fast Ethernet IEEE 802.3
GigabitEthernet	0 to 6	Gigabit Ethernet IEEE 802.3

Table 2-60 Valid Types, Number Ranges, and Interface Descriptions (continued)

Valid Types	Number Ranges	Interface Descriptions
loopback	0 to 2147483647	Loopback
mfr	0 to 2147483647	Multilink Frame Relay bundle
multilink	0 to 2147483647	Multilink-group
null	0	Null
port-channel	1 to 282	EtherChannel of interfaces
pos-channel	1 to 4094	PoS channel of interfaces
tunnel	0 to 2147483647	Tunnel interfaces
vif	1	PGM multicast host
tunnel	0 to 2147483647	Tunnel
virtual-template	1 to 1000	Virtual template
virtual-tokenring	0 to 2147483647	Virtual Token Ring
xtagatm	0 to 2147483647	Extended tag ATM

Examples

This example shows how to display information about the NHRP cache:

```
Router# show ip nhrp

10.0.0.2 255.255.255.255, ATM0/0 created 0:00:43 expire 1:59:16
 Type: dynamic Flags: authoritative
 NBMA address: 11.1111.1111.1111.1111.1111.1111.1111.1111.1111.11
10.0.0.1 255.255.255.255, Tunnel0 created 0:10:03 expire 1:49:56
 Type: static Flags: authoritative
 NBMA address: 11.1.1.2
```

Table 2-61 describes the fields shown in the display.

Table 2-61 show ip nhrp Field Descriptions

Field	Description
10.0.0.2 255.255.255.255	IP address and its network mask in the IP-to-NBMA address cache. The mask is currently always 255.255.255.255 because aggregation of NBMA information through NHRP is not supported.
ATM0/0 created 0:00:43	Interface type and number (in this case, ATM slot and port numbers) and when it was created (hours:minutes:seconds).
expire 1:59:16	Time in which the positive and negative authoritative NBMA address will expire (hours:minutes:seconds). This value is based on the **ip nhrp holdtime** command.
Type	• dynamic—NBMA address was obtained from the NHRP Request packet. • static—NBMA address was statically configured.

Table 2-61 show ip nhrp Field Descriptions (continued)

Field	Description
Flags	• authoritative—Indicates that the NHRP information was obtained from the next-hop server or router that maintains the NBMA-to-IP address mapping for a particular destination. • implicit—Indicates that the information was learned not from an NHRP request generated from the local router, but from an NHRP packet being forwarded or from an NHRP request being received by the local router. • negative—For negative caching; indicates that the requested NBMA mapping could not be obtained.
NBMA address	Nonbroadcast multiaccess address. The address format is appropriate for the type of network being used (for example, ATM, Ethernet, SMDS, or multipoint tunnel).

This example shows how to display basic information about the dynamic (learned) IP-to-NBMA cache entries only for a specific IP address:

```
Router# show ip nhrp dynamic 255.255.255.255 brief
   Target      Via               NBMA            Mode    Intfc   Claimed
```

Related Commands

Command	Description
ip nhrp holdtime	Changes the number of seconds that NHRP NBMA addresses are advertised as valid in authoritative NHRP responses.
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an MBMA network.

show ip pim bsr-router

To display the BSR information, use the **show ip pim bsr-router** command.

show ip pim vrf *vrf-name* **bsr-router**

Syntax Description

vrf *vrf-name*	Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The output includes elected BSR information and information about the locally configured candidate rendezvous-point advertisement.

Examples

This example shows how to display the BSR information:

```
Router# show ip pim bsr-router

PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 172.16.143.28
  Uptime: 04:37:59, BSR Priority: 4, Hash mask length: 30
  Next bootstrap message in 00:00:03 seconds

Next Cand_RP_advertisement in 00:00:03 seconds.
  RP: 172.16.143.28(Ethernet0), Group acl: 6
```

Table 2-62 describes the fields shown in the display.

Table 2-62 show ip pim bsr Field Descriptions

Field	Description
BSR address	IP address of the bootstrap router.
Uptime	Length of time that this router has been up, in hours, minutes, and seconds.
BSR Priority	Priority as configured in the **ip pim bsr-candidate** command.
Hash mask length	Length of a mask (32 bits maximum) that is to be ANDed with the group address before the hash function is called. This value is configured in the **ip pim bsr-candidate** command.

Table 2-62 show ip pim bsr Field Descriptions (continued)

Field	Description
Next bootstrap message in	Time in hours, minutes, and seconds in which the next bootstrap message is due from this BSR.
Next Cand_RP_advertisement in	Time in hours, minutes, and seconds in which the next candidate rendezvous-point advertisement will be sent.
RP	List of IP addresses of rendezvous points.
Group acl	Standard IP access list number that defines the group prefixes that are advertised in association with the rendezvous-point address. This value is configured in the **ip pim bsr-candidate** command.

Related Commands

Command	Description
ip pim bsr-candidate	Configures the router to announce its candidacy as a BSR.
ip pim rp-candidate	Configures the router to advertise itself as a PIM Version 2 rendezvous-point candidate to the BSR.
show ip pim rp-hash	Displays which rendezvous point is being selected for a specified group.

show ip pim interface df

To display information about the designated forwarder interface, use the **show ip pim interface df** command.

show ip pim vrf *vrf-name* **interface df** [*rp-addr*]

Syntax Description

vrf *vrf-name*	Specifies the name that is assigned to the multicast VRF instance.
rp-addr	(Optional) Hostname or IP address of the designated forwarder.

Command Default

If you do not specify *rp-addr*, all designated forwarders are displayed.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to display the information about the DF interface:

```
Router# show ip pim interface df 10.18.1.31
Interface                RP               DF Winner        Metric     Uptime
Vlan70                   10.18.1.31       10.70.1.55       0          14:16:24
FastEthernet5/5          10.18.1.31       10.16.1.30       0          14:16:24
FastEthernet5/6          10.18.1.31       10.18.1.31       0          14:16:24
Router#
```

show ip pim mdt bgp

To display the detailed BGP advertisement of the route distinguisher for the MDT default group, use the **show ip pim mdt bgp** command.

show ip pim vrf *vrf-name* **mdt bgp**

Syntax Description

vrf *vrf-name*	Specifies the name that is assigned to the multicast VRF instance.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to display the detailed BGP advertisement of the route distinguisher for the MDT default group:

```
Router# show ip pim mdt bgp

MDT-default group 232.2.1.4
 rid:1.1.1.1 next_hop:1.1.1.1
```

Table 2-63 describes the fields shown in the display.

Table 2-63 show ip pim mdt bgp Field Descriptions

Field	Description
MDT-default group	MDT default groups that have been advertised to this router.
rid:10.1.1.1	BGP router ID of the advertising router.
next_hop:10.1.1.1	BGP next-hop address that was contained in the advertisement.

show ip pim mdt history

To display the information on data MDTs that have been reused, use the **show ip pim mdt history** command.

show ip pim vrf *vrf-name* **mdt history interval** *minutes*

Syntax Description

vrf *vrf-name*	Specifies the name that is assigned to the multicast VRF instance.
interval *minutes*	Specifies the length of time, in minutes, for which the interval can be configured; valid values are from 1 to 71582 minutes (the maximum is 71582 minutes or 7 weeks).

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The **show ip pim mdt history** command displays the data MDTs that have been reused during the past configured interval.

Examples

This example shows how to display the information on data MDTs that have been reused:

```
Router# show ip pim vrf blue mdt history interval 20

   MDT-data send history for VRF - blue for the past 20 minutes

MDT-data group        Number of reuse
     10.9.9.8           3
     10.9.9.9           2
```

Table 2-64 describes the fields shown in the display.

Table 2-64 show ip pim mdt history Field Descriptions

Field	Description
MDT-data group	MDT data group for which information is being shown.
Number of reuse	Number of data MDTs that have been reused in this group.

show ip pim mdt receive

To display the data MDT advertisements that are received by a specified router, use the **show ip pim mdt receive** command.

show ip pim vrf *vrf-name* **mdt receive** [**detail**]

Syntax Description

vrf *vrf-name*	Specifies the name that is assigned to the multicast VRF instance.
detail	(Optional) Provides a detailed description of the data MDT advertisements that are received.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

When a router wants to switch over from the default MDT to a data MDT, it advertises the VRF source, the group pair, and the global multicast address over which the traffic will be sent. If the remote router wants to receive this data, then the remote router joins this global address multicast group.

Examples

This example shows how to display the data MDT advertisements that are received by a specified router:

```
Router# show ip pim vrf vpn8 mdt receive detail

Joined MDT-data groups for VRF:vpn8
group:232.2.8.0 source:10.0.0.100 ref_count:13
(10.101.8.10, 225.1.8.1), 1d13h/00:03:28/00:02:26, OIF count:1, flags:TY
(10.102.8.10, 225.1.8.1), 1d13h/00:03:28/00:02:27, OIF count:1, flags:TY
```

Table 2-65 describes the fields shown in the display.

Table 2-65 show ip pim mdt receive Field Descriptions

Field	Description
group:172.16.8.0	Group that caused the data MDT to be built.
source:10.0.0.100	VRF source that caused the data MDT to be built.
ref_count:13	Number of source and group pairs that are reusing this data MDT.

Table 2-65 show ip pim mdt receive Field Descriptions (continued)

Field	Description
OIF count:1	Number of interfaces out of which this multicast data is being forwarded.
flags:	Information about the entry: A - Candidate MSDP advertisement B - Bidir group D - Dense C - Connected F - Register flag I - Received source-specific host report J - Join SPT L - Local M - MSDP-created entry P - Pruned R - RP bit set S - Sparse s - SSM group T - SPT bit set X - Proxy join timer running U -URD Y - Joined MDT data group y - Sending to MDT data group Z - Multicast tunnel

show ip pim mdt send

To display the data MDT advertisements that a specified router has made, use the **show ip pim mdt send** command.

show ip pim vrf *vrf-name* **mdt send**

Syntax Description

vrf *vrf-name*	Specifies the name that is assigned to the multicast VRF instance.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Use this command to show the data MDT advertisements that a specified router has made.

Examples

This example shows how to display the data MDT advertisements that a specified router has made:

```
Router# show ip pim mdt send

MDT-data send list for VRF:vpn8
  (source, group)                     MDT-data group      ref_count
  (10.100.8.10, 225.1.8.1)            232.2.8.0           1
  (10.100.8.10, 225.1.8.2)            232.2.8.1           1
  (10.100.8.10, 225.1.8.3)            232.2.8.2           1
  (10.100.8.10, 225.1.8.4)            232.2.8.3           1
  (10.100.8.10, 225.1.8.5)            232.2.8.4           1
  (10.100.8.10, 225.1.8.6)            232.2.8.5           1
  (10.100.8.10, 225.1.8.7)            232.2.8.6           1
  (10.100.8.10, 225.1.8.8)            232.2.8.7           1
  (10.100.8.10, 225.1.8.9)            232.2.8.8           1
  (10.100.8.10, 225.1.8.10)           232.2.8.9           1
```

Table 2-66 describes the fields shown in the display.

Table 2-66 show ip pim mdt send Field Descriptions

Field	Description
source, group	Source and group addresses that this router has switched over to data MDTs.
MDT-data group	Multicast address over which these data MDTs are being sent.
ref_count	Number of source and group pairs that are reusing this data MDT.

show ip pim neighbor

To display the list that the PIM neighbors discovered, use the **show ip pim neighbor** command.

show ip pim vrf *vrf-name* **neighbor** [*interface-type interface-number*]

Syntax Description

vrf *vrf-name*	Specifies the name that is assigned to the multicast VRF instance.
interface-type	(Optional) Interface type.
interface-number	Interface number.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Use this command to determine which routers on the LAN are configured for PIM.

Examples

This example shows how to display the list that the PIM neighbors discovered:

```
Router# show ip pim neighbor

PIM Neighbor Table
Neighbor Address  Interface          Uptime    Expires   Mode
192.168.37.2       Ethernet0          17:38:16  0:01:25   Dense
192.168.37.33      Ethernet0          17:33:20  0:01:05   Dense (DR)
192.168.36.131     Ethernet1          17:33:20  0:01:08   Dense (DR)
192.168.36.130     Ethernet1          18:56:06  0:01:04   Dense
10.1.22.9         Tunnel0            19:14:59  0:01:09   Dense
```

Table 2-67 describes the fields shown in the display.

Table 2-67 show ip pim neighbor Field Descriptions

Field	Description
Neighbor Address	IP address of the PIM neighbor.
Interface	Interface type and number on which the neighbor is reachable.
Uptime	Time in hours, minutes, and seconds that the entry has been in the PIM neighbor table.
Expires	Time in hours, minutes, and seconds until the entry will be removed from the IP multicast routing table.

Table 2-67 show ip pim neighbor Field Descriptions (continued)

Field	Description
Mode	Mode in which the interface is operating.
(DR)	Status of whether this neighbor is a designated router on the LAN.

Related Commands

Command	Description
ip pim state-refresh disable	Disables the processing and forwarding of PIM dense-mode refresh-control messages on a PIM router.
ip pim state-refresh origination-interval	Configures the origination of and the interval for PIM dense-mode state-refresh control messages on a PIM router.
show ip pim interface df	Displays information about the designated forwarder interface.

show ip pim rp-hash

To display which rendezvous point is being selected for a specified group, use the **show ip pim rp-hash** command.

show ip pim vrf *vrf-name* **rp-hash** {*group-address* | *group-name*}

Syntax Description

vrf *vrf-name*	Specifies the name that is assigned to the multicast VRF instance.
group-address | *group-name*	Rendezvous-point information for the specified group address or name as defined in the DNS hosts table.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command displays which rendezvous point was selected for the group specified. It also shows whether this rendezvous point was selected by Auto-RP or the PIM Version 2 bootstrap mechanism.

Examples

This example shows how to display which rendezvous point is being selected for a specified group:

```
Router# show ip pim rp-hash 239.1.1.1

RP 172.16.24.12 (mt1-47a.cisco.com), v2
    Info source: 172.16.24.12 (mt1-47a.cisco.com), via bootstrap
         Uptime: 05:15:33, expires: 00:02:01
```

Table 2-68 describes the fields shown in the display.

Table 2-68 show ip pim rp-hash Field Descriptions

Field	Description
RP 172.16.24.12 (mt1-47a.cisco.com), v2	Address of the rendezvous point for the group specified (239.1.1.1). The DNS name of the rendezvous point within the parentheses. If the address of the rendezvous point is not registered in the DNS, a question mark (?) is displayed. PIM Version 2 is configured.
Info source: 172.16.24.12 (mt1-47a.cisco.com), via bootstrap	System from which the router learned this rendezvous-point information and the DNS name of the source. The rendezvous point was selected by the bootstrap mechanism. In this case, the BSR is also the rendezvous point.
Uptime	Length of time (in hours, minutes, and seconds) that the router has known about this rendezvous point.
expires	Time (in hours, minutes, and seconds) after which the information about this rendezvous point expires. If the router does not receive any refresh messages in this time, it discards information about this rendezvous point.

show ip pim rp mapping

To display the mappings for the PIM group to the active rendezvous points, use the **show ip pim rp mapping** command.

show ip pim vrf *vrf-name* **rp mapping** [*rp-address*]

Syntax Description

vrf *vrf-name*	Specifies the name that is assigned to the multicast VRF instance.
rp-address	(Optional) Rendezvous-point IP address.

Command Default

If you do not specify an *rp-address*, the mappings for all the active rendezvous points are displayed.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to display the mappings for the PIM group to the active rendezvous points:

```
Router# show ip pim rp mapping
PIM Group-to-RP Mappings
This system is an RP-mapping agent
Group(s) 224.1.0.0/16
RP 6.6.6.6 (?), v2v1
Info source: 6.6.6.6 (?), elected via Auto-RP ---> learned via Auto-RP
and the elected RP.
Uptime: 22:36:49, expires: 00:02:04
Group(s) 225.2.2.0/24
RP 9.9.9.9 (?), v2v1, bidir
Info source: 9.9.9.9 (?), elected via Auto-RP
Uptime: 22:36:20, expires: 00:02:37
Group(s) 226.2.2.0/24
RP 2.2.2.2 (?), v2v1, bidir
Info source: 2.2.2.2 (?), elected via Auto-RP
Uptime: 22:36:24, expires: 00:02:29
Group(s) 227.2.2.0/24
RP 9.9.9.9 (?), v2v1, bidir
Info source: 9.9.9.9 (?), elected via Auto-RP
Uptime: 22:36:21, expires: 00:02:35
Router#
```

Table 2-69 describes the fields that are shown in the example.

Table 2-69 show ip pim rp mapping Field Descriptions

Field	Description
Info source	ACL number.
Static	Group-to-mapping information from the static rendezvous-point configuration.
Bidir Mode	Status of whether the rendezvous point is operating in bidirectional mode.
RP	Address of the rendezvous point for that group.
(?)	Status that shows no Domain Name System (DNS) name has been specified.

show ip pim snooping

To display the information about IP PIM snooping, use the **show ip pim snooping** command.

show ip pim snooping

show ip pim snooping vlan *vlan-id* [**neighbor** | **mac-group** | **statistics** | **mroute** [{*src-ip* | *group-ip*}]]

Syntax Description

vlan *vlan-id*	Displays information for a specific VLAN; valid values are from 1 to 4094.
neighbor	(Optional) Displays information about the neighbor database.
mac-group	(Optional) Displays information about the GDA database in Layer 2.
statistics	(Optional) Displays information about the VLAN statistics.
mroute	(Optional) Displays information about the mroute database.
src-ip	(Optional) Source IP address.
group-ip	(Optional) Group IP address.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to display the information about the global status:

```
Router# show ip pim snooping
Global runtime mode: Enabled
Global admin mode  : Enabled
Number of user enabled VLANs: 1
User enabled VLANs: 10
Router#
```

This example shows how to display the information about a specific VLAN:

```
Router# show ip pim snooping vlan 10
3 neighbors (0 DR priority incapable, 0 Bi-dir incapable)
6 mroutes, 3 mac entries
DR is 10.10.10.4
RP DF Set
Router#
```

This example shows how to display the information about the neighbor database for a specific VLAN:

```
Router# show ip pim snooping vlan 10 neighbor
IP Address       Mac address     Port Uptime/Expires    Flags
10.10.10.2       000a.f330.344a  3/13 00:09:57/00:01:22
10.10.10.1       000a.f330.334a  3/12 00:09:44/00:01:21
10.10.10.4       000a.f330.3c00 15/01 00:09:57/00:01:22 DR
Number of Neighbors = 3
Router#
```

This example shows how to display the information about the GDA database for a specific VLAN in Layer 2:

```
Router# show ip pim snooping vlan 10 mac-group
Mac address    Group address   Uptime/Expires    Outgoing Ports
0100.5e01.6465 224.1.100.101   00:20:26/00:02:43 3/12 3/13 15/1
0100.5e01.6464 224.1.100.100   00:20:28/00:02:41 3/12 3/13 15/1
0100.5e00.0128 224.0.1.40      00:20:27/00:02:47 3/12 3/13 15/1
Number of mac-groups = 3
Router#
```

This example shows how to display the detailed statistics for a specific VLAN:

```
Router# show ip pim snooping vlan 10 statistics
PIMv2 statistics for vlan 10:
Hello                                        : 811
Join/Prunes                                  : 1332
RP DF Election                               : 0
Asserts                                      : 133
Other types                                  : 0

Hello option holdtime [1]                    : 811
Hello option Generation ID[20]               : 544
Hello option DR priority[19]                 : 544
Hello option Bi-dir capable[22]              : 0
Hello option Fast Hold[65005]                : 0
Hello option Lan Prune Delay[2]              : 0
Hello option Tag switching [17]              : 0
Hello option PIM-DM State Refresh[21]        : 544
Hello option Deprecated Cisco DR priority[18]   : 0
Error - Hello length too short               : 0
Error - Hello hold option missing            : 0
Error - Hello option length                  : 0
Error - Hello option unknown                 : 0

Error - Join/Prune Address Family            : 0
Error - Join/Prune Parser malloc failure     : 0
Error - Join/Prune Unknown up/down neighbor  : 0
Error - Join/Prune Malformed packet discards    : 0

Error - RPDF election Address Family         : 0
Error - RPDF Unknown up/down neighbor        : 0

Error - Generic packet input error           : 0
Router#
```

This example shows how to display the information about the mroute database for all mrouters in a specific VLAN:

```
Router# show ip pim snooping vlan 10 mroute
Number of Mroutes = 6
Flags: J/P - (*,G) Join/Prune, j/p - (S,G) Join/Prune
       SGR-P - (S,G,R) Prune
```

```
(*, 224.1.100.101), 00:16:14/00:02:58
  10.10.10.1->10.10.10.2, 00:16:14/00:02:58, J
  Downstream ports: 3/12
  Upstream   ports: 3/13
  Outgoing   ports: 3/12 3/13

(*, 224.1.100.100), 00:16:16/00:02:56
  10.10.10.1->10.10.10.2, 00:16:16/00:02:56, J
  Downstream ports: 3/12
  Upstream   ports: 3/13
  Outgoing   ports: 3/12 3/13

(10.10.10.2, 224.0.1.40), 00:16:10/00:03:03
  10.10.10.1->10.10.10.2, 00:16:10/00:03:03, SGR-P
  Downstream ports:
  Upstream   ports: 3/13
  Outgoing   ports: 3/13

(*, 224.0.1.40), 00:16:16/00:03:02
  10.10.10.1->10.10.10.2, 00:16:16/00:03:02, J
  Downstream ports: 3/12
  Upstream   ports: 3/13
  Outgoing   ports: 3/12 3/13

(*, 224.10.10.10), 00:02:23/00:01:06
  Downstream ports:
  Upstream   ports:
  Outgoing   ports: 3/12 3/13

(123.123.123.123, 224.10.10.10), 00:02:23/00:01:06
  10.10.10.1->10.10.10.2, 00:02:23/00:01:06, j
  Downstream ports: 3/12
  Upstream   ports: 3/13
  Outgoing   ports: 3/12 3/13
Router#
```

This example shows how to display the information about the PIM mroute for a specific source address:

```
Router# show ip pim snooping vlan 10 mroute 224.1.100.100
(*, 224.1.100.100), 00:16:36/00:02:36
  10.10.10.1->10.10.10.2, 00:16:36/00:02:36, J
  Downstream ports: 3/12
  Upstream   ports: 3/13
  Outgoing   ports: 3/12 3/13
Router#
```

This example shows how to display the information about the PIM mroute for a specific source and group address:

```
Router# show ip pim snooping vlan 10 mroute 123.123.123.123 224.10.10.10
(123.123.123.123, 224.10.10.10), 00:03:04/00:00:25
  10.10.10.1->10.10.10.2, 00:03:04/00:00:25, j
  Downstream ports: 3/12
  Upstream   ports: 3/13
  Outgoing   ports: 3/12 3/13
Router#
```

Related Commands

Command	Description
ip pim snooping (global configuration mode)	Enables PIM snooping globally.
ip pim snooping (interface configuration mode)	Enables PIM snooping on an interface.

show ip rpf events

To display the triggered RPF statistics, use the **show ip rpf events** command.

show ip rpf [**vrf** *vrf-name*] **events**

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to display the triggered RPF statistics:

```
Router#  show ip rpf events
Last 15 triggered multicast RPF check events
RPF backoff delay: 500 msec
RPF maximum delay: 5 sec
DATE/TIME BACKOFF PROTOCOL EVENT RPF CHANGES
Jan 1 00:00:55.643 500 msec EIGRP Route UP 0
Jan 1 00:00:07.283 1000 sec Connected Route UP 0
Jan 1 00:00:06.283 500 msec Connected Route UP 0
Router#
```

Related Commands

Command	Description
ip multicast rpf backoff	Sets the PIM-backoff interval.
ip multicast rpf interval	Sets the RPF consistency-check interval.

show ip wccp

To display the WCCP statistics, use the **show ip wccp** command.

show ip wccp [{*service-number* | **web-cache**} [**detail** | **view**]]

Syntax Description

service-number	(Optional) Identification number of the cache engine service group being controlled by a router; valid values are from 0 to 99.
web-cache	(Optional) Directs the router to display statistics for the web-cache service.
detail	(Optional) Displays information for the router and all cache engines in the currently configured cluster.
view	(Optional) Displays which other members of a particular service group have or have not been detected.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Use the **show ip wccp** *service-number* command to provide the “Total Packets Redirected” count. The “Total Packets Redirected” count is the number of flows, or sessions, that are redirected.

Use the **show ip wccp** *service-number* **detail** command to provide the “Packets Redirected” count. The “Packets Redirected” count is the number of flows, or sessions, that are redirected.

Use the **show ip wccp web-cache detail** command to provide an indication of how many flows, rather than packets, are using Layer 2 redirection.

For cache-engine clusters using Cisco cache engines, the reverse proxy *service-number* is indicated by a value of 99.

Use the **clear ip wccp** command to reset the counter for the “Packets Redirected” information.

For additional information on the IP WCCP commands, refer to the “Configuring Web Cache Services Using WCCP” section in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Examples

This example shows how to display the connected cache engine using Layer 2 redirection:

```
Router# show ip wccp web-cache detail
WCCP Cache-Engine information:
        IP Address:           10.11.1.1
        Protocol Version:     2.0
        State:                Usable
        Redirection:          L2
        Initial Hash Info:    FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

```
                       FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
Assigned Hash Info:   FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                       FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
Hash Allotment:       256 (100.00%)
Packets Redirected:   10273
Connect Time:         17:05:44
```

Table 2-70 describes the fields that are shown in the example.

Table 2-70 show ip wccp web-cache detail Command Output Fields

Field	Description
WCCP Cache-Engine information	Header for the area that contains fields for the IP address and version of WCCP that is associated with the router that is connected to the cache engine in the service group.
IP Address	IP address of the router that is connected to the cache engine in the service group.
Protocol Version	Version of WCCP that is used by the router in the service group.
WCCP Cache-Engine information	Fields for information on cache engines.
IP Address	IP address of the cache engine in the service group.
Protocol Version	Version of WCCP that is used by the cache engine in the service group.
State	Status of whether the cache engine is operating properly and can be contacted by a router and other cache engines in the service group.
Initial Hash Info	Initial state of the hash-bucket assignment.
Assigned Hash Info	Current state of the hash-bucket assignment.
Hash Allotment	Percentage of buckets that is assigned to the current cache engine. Both a value and a percent figure are displayed.
Packets Redirected	Number of flows or sessions that have been redirected to the cache engine.
Connect Time	Amount of time that it takes for the cache engine to connect to the router.

Related Commands

Command	Description
clear ip wccp	Removes WCCP statistics (counts) maintained on the router for a particular service.
ip wccp	Directs a router to enable or disable the support for a cache engine service group.
ip wccp redirect	Enables packet redirection on an outbound or inbound interface using WCCP.
ip wccp web-cache accelerated	Enables the hardware acceleration for WCCP version 1.
show ip interface	Displays the usability status of interfaces that are configured for IP.

show ipv6 mfib

To display the forwarding entries and interfaces in the IPv6 MFIB, use the **show ipv6 mfib** command.

show ipv6 mfib [{*group-ip-addr***/***prefix-length* | *group-name* | *group-address* [*source-name* | *source-address*]} | {**active** *kbps*} | **count** | **interface** | **status** | **summary** | **verbose**]

show ipv6 mfib [**link-local** [**active** [*kbps*] | **count** | **verbose**]]

Syntax Description

*group-ip-addr***/***prefix-length*	(Optional) Group IPv6 address/prefix length for the IPv6 network assigned to the interface.
group-name	(Optional) Multicast group name.
group-address	(Optional) Group IPv6 address.
source-name	(Optional) Source name.
source-address	(Optional) Source IP address.
active *kbps*	(Optional) Displays the rate at which active sources are sending to multicast groups; valid values are from 0 to 4294967295 kilobits per second.
count	(Optional) Displays information about the route and packet count.
interface	(Optional) Displays information about the interface settings and status.
status	(Optional) Displays information about the general settings and status.
summary	(Optional) Displays information about the summary statistics.
verbose	(Optional) Displays additional information such as the MAC encapsulation header and platform-specific information.
link-local	(Optional) Displays the link-local groups.

Command Default

prefix-length is **128**.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Use the **show ipv6 mfib** command to display MFIB entries, forwarding interfaces, and their traffic statistics. This command can be enabled on virtual IP (VIP) if the router is operating in distributed mode.

Use the **show ipv6 mfib active** command to display MFIB entries actively used to forward packets. In many cases, it is useful to provide the optional *kbps* argument to display the set of entries that are forwarding an amount of traffic larger or equal to the amount set by the *kbps* argument.

Use the **show ipv6 mfib count** command to display the average packet size and data rate in kilobits per seconds.

The *prefix-length* is the length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

A forwarding entry in the MFIB has flags that determine the default forwarding and signaling behavior to use for packets matching the entry. The entry also has per-interface flags that further specify the forwarding behavior for packets received or forwarded on specific interfaces. Table 2-71 describes the MFIB forwarding entries and interface flags.

Table 2-71 MFIB Forwarding Entries and Interface Flags

Flag	Description
F	Forward—Data is forwarded out of this interface.
A	Accept—Data received on this interface is accepted for forwarding.
IC	Internal copy—Deliver a copy of the packets received or forwarded on this interface to the router.
NS	Negate signal—Reverse the default entry signaling behavior for packets received on this interface.
DP	Do not preserve—When signaling the reception of a packet on this interface, do not preserve a copy of it (discard it instead).
SP	Signal present—The reception of a packet on this interface was just signaled.
S	Signal—By default, signal the reception of packets matching this entry.
C	Perform directly connected check for packets matching this entry. Signal the reception if packets were originated by a directly connected source.

Examples

This example shows how to display information for a specific group IPv6 address:

```
Router# show ipv6 mfib ff35::1:1
IP Multicast Forwarding Information Base
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: Distributed FS Pkt Count/FS Pkt Count/PS Pkt Count
(1600::2,FF35::1:1) Flags:
   RP Forwarding: 7188/100/48/37, Other: 203619/203619/0
   LC Forwarding: 0/0/0/0, Other: 0/0/0
   Vlan25 Flags: A
   Vlan11 Flags: F NS
     Pkts: 0/7188/0
```

Table 2-72 describes the fields shown in the display.

Table 2-72 show ipv6 mfib Field Descriptions

Field	Description
Entry flags	Information about the entry.
Forwarding Counts	Statistics on the packets that are received and forwarded to at least one interface.
Pkt Count/	Total number of packets received and forwarded since the creation of the multicast forwarding state to which this counter applies.
Pkts per second/	Number of packets received and forwarded per second.
Avg Pkt Size/	Total number of bytes divided by the total number of packets for this multicast forwarding state. There is no direct display for the total number of bytes. You can calculate the total number of bytes by multiplying the average packet size by the packet count.
Kbits per second	Bytes per second divided by packets per second, and divided by 1000.
Other counts:	Statistics on the received packets. These counters include statistics about the packets received and forwarded and packets received but not forwarded.
Interface Flags:	Information about the interface. See Table 2-71 for further information on interface flags.
Interface Counts:	Interface statistics.

This example shows forwarding entries and interfaces in the MFIB with a group address of FF03:1::1 and a source address of 5002:1::2 specified:

```
Router# show ipv6 mfib FF03:1::1 5002:1::2

IP Multicast Forwarding Information Base
Entry Flags:C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:Total/RPF failed/Other drops
Interface Flags:A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts:FS Pkt Count/PS Pkt Count
(5002:1::2,FF03:1::1) Flags:
   Forwarding:71505/0/50/0, Other:42/0/42
   GigabitEthernet5/0 Flags:A
   GigabitEthernet5/0.19 Flags:F NS
     Pkts:239/24
   GigabitEthernet5/0.20 Flags:F NS
     Pkts:239/24
.
.
.
   GigabitEthernet5/0.16 Flags:F NS
     Pkts:71628/24
```

This example shows forwarding entries and interfaces in the MFIB with a group address of FF03:1::1 and a default prefix of 128:

```
Router# show ipv6 mfib FF03:1::1/128

IP Multicast Forwarding Information Base
Entry Flags:C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:Total/RPF failed/Other drops
Interface Flags:A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts:FS Pkt Count/PS Pkt Count
(*,FF03:1::1) Flags:C
   Forwarding:0/0/0/0, Other:0/0/0
   Tunnel1 Flags:A NS
   GigabitEthernet5/0.25 Flags:F NS
     Pkts:0/0
.
.
.
   GigabitEthernet5/0.16 Flags:F NS
     Pkts:0/0
```

This example displays statistics on the rate at which active IP multicast sources are sending information. The router is switching traffic from 2001::1:1:200 to FF05::1:

```
Router# show ipv6 mfib active

Active IPv6 Multicast Sources - sending >= 4 kbps
Group: FF05::1
  Source: 2001::1:1:200
    Rate: 20 pps/16 kbps(1sec), 0 kbps(last 128 sec)
```

Table 2-73 describes the fields shown in the display.

Table 2-73 show ipv6 mfib active Field Descriptions

Field	Description
Group:	Summary information about counters for (*, G) and the range of (S,G) states for one particular group G. The following RP-tree: and Source: output fields contain information about the individual states belonging to this group. **Note** For PIM-SSM range groups, the Group: displays are statistical. All SSM range (S,G) states are individual, unrelated SSM channels.
Rate...kbps	Bytes per second divided by packets per second and divided by 1000. On an IP multicast fast-switching platform, the number of packets per second is the number of packets during the last second. Other platforms may use a different approach to calculate this number. Refer to the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY* for more information.

This example displays statistics from the MFIB about the group and source. The router is switching traffic from 2001::1:1:200 to FF05::1:

```
Router# show ipv6 mfib count

IP Multicast Statistics
54 routes, 7 groups, 0.14 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Group: FF00::/8
  RP-tree:    Forwarding: 0/0/0/0, Other: 0/0/0
Group: FF00::/15
  RP-tree:    Forwarding: 0/0/0/0, Other: 0/0/0
```

```
Group: FF05::1
  RP-tree:    Forwarding: 2/0/100/0, Other: 0/0/0
  Source: 10::1:1:200,   Forwarding: 367/10/100/7, Other: 0/0/0
  Tot. shown: Source count: 1, pkt count: 369
Group: FF10::/15
  RP-tree:    Forwarding: 0/0/0/0, Other: 0/0/0
Group: FF20::/15
  RP-tree:    Forwarding: 0/0/0/0, Other: 0/0/0
```

Table 2-74 describes the fields shown in the display.

Table 2-74 show ipv6 mfib count Field Descriptions

Field	Description
Forwarding Counts	Statistics on the packets that are received and forwarded to at least one interface.
Pkt Count/	Total number of packets received and forwarded since the multicast forwarding state to which this counter applies was created.
Pkts per second/	Number of packets received and forwarded per second.
Avg Pkt Size/	Total number of bytes divided by the total number of packets for this multicast forwarding state. There is no direct display for the total number of bytes. You can calculate the total number of bytes by multiplying the average packet size by the packet count.
Kilobits per second	Bytes per second, divided by packets per second, and divided by 1000.
Other counts:	Statistics on the received packets. These counters include statistics about the packets received and forwarded and packets received but not forwarded.
Total/	Total number of packets received.
RPF failed/	Number of packets not forwarded due to a failed RPF or acceptance check (when bidirectional PIM is configured).
Other drops (OIF-null, rate-limit etc)	Number of packets not forwarded for reasons other than an RPF or acceptance check (such as the outgoing interface [OIF] list was empty or because the packets were discarded because of a configuration that was enabled).
Group:	Summary information about counters for (*,G) and the range of (S,G) states for one particular group G. The following RP-tree: and Source: output fields contain information about the individual states belonging to this group. **Note** For Source Specific Multicast (PIM-SSM) range groups, the Group: displays are statistical. All SSM range (S,G) states are individual, unrelated SSM channels.
RP-tree:	Counters for the (*,G) state of this group G. These counters are displayed only for groups that have a forwarding mode that do not forward packets on the shared tree. These (*,G) groups are bidirectional PIM and PIM sparse mode (PIM-SM) groups. There are no RP-tree displays for PIM SSM range groups.

This example shows forwarding entries and interfaces in the MFIB and additional information such as the MAC encapsulation header and platform-specific information:

```
Router# show ipv6 mfib ff33::1:1 verbose
IP Multicast Forwarding Information Base
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, K - Keepalive
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
```

```
Platform per slot HW-Forwarding Counts: Pkt Count/Byte Count
Platform flags: HF - Forwarding entry,HB - Bridge entry,HD - NonRPF Drop entry,
                NP - Not platform switchable,RPL - RPF-ltl linkage,
                MCG - Metset change,ERR - S/w Error Flag,RTY - In RetryQ,
                LP - L3 pending,MP - Met pending,AP - ACL pending
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: Distributed FS Pkt Count/FS Pkt Count/PS Pkt Count
(10::2,FF33::1:1) Flags: K
   RP Forwarding: 0/0/0/0, Other: 0/0/0
   LC Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwd:   0/0/0/0, Other: NA/NA/NA
   Slot 6: HW Forwarding: 0/0, Platform Flags:  HF RPL
   Slot 1: HW Forwarding: 0/0, Platform Flags:  HF RPL
   Vlan10 Flags: A
   Vlan30 Flags: F NS
     Pkts: 0/0/0 MAC: 33330001000100D0FFFE180086DD
Router#
```

Table 2-75 describes the fields shown in the display.

Table 2-75 show ipv6 mfib verbose Field Descriptions

Field	Description
Platform flags	Information about the platform.
Platform per slot HW-Forwarding Counts	Total number of packets per bytes forwarded.

Table 2-76 describes the MFIB platform flags.

Table 2-76 MFIB Platform Flags

Flag	Description
H	Entry is installed in hardware
HF	Forwarding entry
HB	Bridge entry
HD	NonRPF Drop entry
NP	Software switched
RPL	RPF-ltl linkage
MCG	Metset change
ERR	S/w Error Flag
RTY	In RetryQ
LP	Layer 3 pending
MP	Met pending
AP	ACL pending

show ipv6 mld snooping

To display MLDv2 snooping information, use the **show ipv6 mld snooping** command.

show ipv6 mld snooping {{**explicit-tracking** *vlan*} | {**mrouter** [**vlan** *vlan*]} | {**report-suppression vlan** *vlan*} | {**statistics vlan** *vlan*}}

Syntax Description

explicit-tracking vlan *vlan*	Displays the status of explicit host tracking.
mrouter	Displays the multicast router interfaces on an optional VLAN.
vlan *vlan*	(Optional) Specifies the VLAN number on the multicast router interfaces.
report-suppression vlan *vlan*	Displays the status of the report suppression.
statistics vlan *vlan*	Displays IGMP snooping information on a VLAN.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

You can also use the **show ip igmp snooping** commands to display information about IGMP snooping.

You can enter the **show ipv6 mld snooping mrouter** command without arguments to display all the multicast router interfaces.

Examples

This example shows how to display explicit tracking information on VLAN 25:

```
Router# show ipv6 mld snooping explicit-tracking vlan 25
Source/Group                    Interface    Reporter        Filter_mode
------------------------------------------------------------------------
10.1.1.1/226.2.2.2              Vl25:1/2     16.27.2.3       INCLUDE
10.2.2.2/226.2.2.2              Vl25:1/2     16.27.2.3       INCLUDE
Router#
```

This example shows how to display the multicast router interfaces in VLAN 1:

```
Router# show ipv6 mld snooping mrouter vlan 1
vlan            ports
-----+----------------------------------------
  1          Gi1/1,Gi2/1,Fa3/48,Router
Router#
```

This example shows the IGMP snooping statistics information for VLAN 25:

```
Router# show ipv6 mld snooping statistics interface vlan 25

Snooping staticstics for Vlan25
#channels:2
#hosts   :1

Source/Group            Interface       Reporter      Uptime        Last-Join    Last-Leave
10.1.1.1/226.2.2.2      Gi1/2:Vl25      16.27.2.3     00:01:47      00:00:50       -
10.2.2.2/226.2.2.2      Gi1/2:Vl25      16.27.2.3     00:01:47      00:00:50       -
Router#
```

Related Commands

Command	Description
ipv6 mld snooping	Enables MLDv2 snooping globally.
ipv6 mld snooping explicit-tracking	Enables explicit host tracking.
ipv6 mld snooping querier	Enables the MLDv2 snooping querier.
ipv6 mld snooping report-suppression	Enables report suppression on a VLAN.

show l2protocol-tunnel

To display the protocols that are tunneled on an interface or on all interfaces, use the **show l2protocol-tunnel** command.

show l2protocol-tunnel [{**interface** *interface mod/port*} | {**vlan** *vlan-id*} | **summary**]

Syntax Description

interface *interface*	(Optional) Specifies the interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **atm**, and **ge-wan**.
mod/port	Module and port number.
vlan *vlan-id*	Specifies the VLAN; valid values are from 1 to 4094.
summary	(Optional) Displays a summary of a tunneled port.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The **show l2protocol-tunnel** command displays only the ports that have protocol tunneling enabled.

The **show l2protocol-tunnel summary** command displays the ports that have protocol tunneling enabled, regardless of whether the port is down or currently configured as a trunk.

Examples

This example shows how to display the protocols that are tunneled on all interfaces:

```
Router# show l2protocol-tunnel
COS for Encapsulated Packets: 5
Drop Threshold for Encapsulated Packets: 3000
Port    Protocol Shutdown    Drop    Encapsulation Decapsulation     Drop
                 Threshold Threshold    Counter       Counter       Counter
------- -------- --------- --------- ------------- ------------- -------------
Fa3/38  cdp      ----      3000      5             0             0
        stp      ----      3000      2653          0             0
                 ---       ----      ----          ----          ----
Router#
```

This example shows how to display a summary of Layer 2-protocol tunnel ports:

```
Router# show l2protocol-tunnel summary
COS for Encapsulated Packets:5
Drop Threshold for Encapsulated Packets:0

Port    Protocol    Shutdown         Drop             Status
                    Threshold        Threshold
                    (cdp/stp/vtp)    (cdp/stp/vtp)
```

```
------- ----------- ---------------- ---------------- ----------
Fa9/1   --- stp --- ----/----/----   ----/----/----   down
Fa9/9   cdp stp vtp ----/----/----   ----/----/----   up
Fa9/47  --- --- --- ----/----/----   1500/1500/1500   down(trunk)
Fa9/48  cdp stp vtp ----/----/----   ----/----/----   down(trunk)
Router>
```

Related Commands

Command	Description
l2protocol-tunnel	Enables the protocol tunneling on an interface and specifies the type of protocol to be tunneled.
l2protocol-tunnel drop-threshold	Specifies the maximum number of packets that can be processed for the specified protocol on that interface before being dropped.
l2protocol-tunnel global drop-threshold	Enables rate limiting at the software level.
l2protocol-tunnel shutdown-threshold	Specifies the maximum number of packets that can be processed for the specified protocol on that interface in 1 second.

show l3-mgr

To display the information about the Layer 3 manager, use the **show l3-mgr** command.

show l3-mgr status

show l3-mgr {**interface** {{*interface interface-number*} | {**null** *interface-number*} | {**port-channel** *number*} | {**vlan** *vlan-id*} | **status**}}

Syntax Description

status	Displays information about the global variable.
interface	Displays information about the Layer 3 manager.
interface	Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **atm**, and **ge-wan**.
interface-number	Module and port number; see the "Usage Guidelines" section for valid values.
null *interface-number*	Specifies the null interface; the valid value is **0**.
port-channel *number*	Specifies the channel interface; valid values are a maximum of 64 values ranging from 1 to 282.
vlan *vlan-id*	Specifies the VLAN; valid values are from 1 to 4094.
status	Displays status information about the Layer 3 manager.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The **port-channel** *number* values from 257 to 282 are supported on the CSM and the FWSM only.

Examples

This example shows how to display the status of the Layer 3 manager:

```
Router# show l3-mgr status
l3_mgr_state:         2
l3_mgr_req_q.count:   0
l3_mgr_req_q.head:    0
```

```
l3_mgr_req_q.tail:    0
l3_mgr_max_queue_count:  1060
l3_mgr_shrunk_count:  0
l3_mgr_req_q.ip_inv_count:    303
l3_mgr_req_q.ipx_inv_count:   0
l3_mgr_outpak_count:  18871
l3_mgr_inpak_count:   18871

l3_mgr_max_pending_pak: 4
l3_mgr_pending_pak_count: 0

nde enable statue:    0
current nde addr:     0.0.0.0

Router#
```

This example shows how to display the information about the Layer 3 manager for a specific interface:

```
Router# show l3-mgr interface fastethernet 5/40
vlan:                0
ip_enabled:        1
ipx_enabled:       1
bg_state:          0 0 0 0
hsrp_enabled:      0
hsrp_mac:          0000.0000.0000
state:             0
up:                0
Router#
```

show lacp

To display LACP information, use the **show lacp** command.

show lacp [*channel-group*] {**counters** | **internal** | **neighbors** | **sys-id**}

Syntax Description

channel-group	(Optional) Number of the channel group; valid values are from 1 to 282.
counters	Displays information about the LACP statistics.
internal	Displays LACP internal information.
neighbors	Displays information about the LACP neighbor.
sys-id	Displays the LACP system identification.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

If you do not specify a *channel-group*, all channel groups are displayed.

The *channel-group* values from 257 to 282 are supported on the CSM and the FWSM only.

You can enter the optional *channel-group* to specify a channel group for all keywords, except the **sys-id** keyword.

Examples

This example shows how to display the LACP statistics for a specific channel group:

```
Router# show lacp 1 counters
              LACPDUs         Marker       LACPDUs
Port       Sent   Recv     Sent   Recv     Pkts Err
---------------------------------------------------
Channel group: 1
  Fa4/1    8      15       0      0         3    0
  Fa4/2    14     18       0      0         3    0
  Fa4/3    14     18       0      0         0
  Fa4/4    13     18       0      0         0
```

The output displays the following information:

- The LACPDUs Sent and Recv columns display the LACPDUs that are sent and received on each specific interface.
- The LACPDUs Pkts and Err columns display the marker-protocol packets.

This example shows how to display internal information for the interfaces that belong to a specific channel:

```
Router# show lacp 1 internal
Flags:  S - Device sends PDUs at slow rate. F - Device sends PDUs at fast rate.
        A - Device is in Active mode.       P - Device is in Passive mode.

Channel group 1
                            LACPDUs     LACP Port    Admin   Oper    Port     Port
Port      Flags    State    Interval    Priority     Key     Key     Number   State
Fa4/1     saC      bndl     30s         32768        100     100     0xc1     0x75
Fa4/2     saC      bndl     30s         32768        100     100     0xc2     0x75
Fa4/3     saC      bndl     30s         32768        100     100     0xc3     0x75
Fa4/4     saC      bndl     30s         32768        100     100     0xc4     0x75
Router#
```

Table 2-77 describes the fields that are shown in the example.

Table 2-77 show lacp internal Command Output Fields

Field	Description
State	State of the specific port at the current moment is displayed; allowed values are as follows: • *bndl*—Port is attached to an aggregator and bundled with other ports. • *susp*—Port is in a suspended state; it is not attached to any aggregator. • *indep*—Port is in an independent state (not bundled but able to switch data traffic. In this case, LACP is not running on the partner port). • *hot-sby*—Port is in a hot-standby state. • *down*—Port is down.
LACPDUs Interval	Interval setting.
LACP Port Priority	Port-priority setting.
Admin Key	Administrative key.
Oper Key	Operator key.
Port Number	Port number.
Port State	State variables for the port that are encoded as individual bits within a single octet with the following meaning [1]: • **bit0**: *LACP_Activity* • **bit1**: *LACP_Timeout* • **bit2**: *Aggregation* • **bit3**: *Synchronization* • **bit4**: *Collecting* • **bit5**: *Distributing* • **bit6**: *Defaulted* • **bit7**: *Expired*

This example shows how to display the information about the LACP neighbors for a specific port channel:

```
Router# show lacp 1 neighbors
Flags:  S - Device sends PDUs at slow rate. F - Device sends PDUs at fast rate.
        A - Device is in Active mode.       P - Device is in Passive mode.

Channel group 1 neighbors
          Partner                 Partner
Port      System ID               Port Number     Age     Flags
Fa4/1     8000,00b0.c23e.d84e     0x81            29s     P
Fa4/2     8000,00b0.c23e.d84e     0x82            0s      P
Fa4/3     8000,00b0.c23e.d84e     0x83            0s      P
Fa4/4     8000,00b0.c23e.d84e     0x84            0s      P

          Port          Admin     Oper      Port
          Priority      Key       Key       State
Fa4/1     32768         200       200       0x81
Fa4/2     32768         200       200       0x81
Fa4/3     32768         200       200       0x81
Fa4/4     32768         200       200       0x81
Router#
```

If no PDUs have been received, the default administrative information is displayed in braces.

This example shows how to display the LACP system identification:

```
Router> show lacp sys-id
8000,AC-12-34-56-78-90
```

The system identification is made up of the system priority and the system MAC address. The first 2 bytes are the system priority, and the last 6 bytes are the globally administered individual MAC address that is associated to the system.

Related Commands

Command	Description
clear lacp counters	Clears the statistics for all interfaces belonging to a specific channel group.
lacp port-priority	Sets the priority for the physical interfaces.
lacp system-priority	Sets the priority of the system.

show logging ip access-list

To display information about the logging IP access list, use the **show logging ip access-list** command.

show logging ip access-list {**cache** | **config**}

Syntax Description

cache	Displays information about all the entries in the OAL cache.
config	Displays information about the logging IP access-list configuration.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

OAL is supported on IPv4 unicast traffic only.

Examples

This example shows how to display all the entries in the OAL cache:

```
Router# show logging ip access-list cache
Matched flows:
id prot src_ip dst_ip sport dport status count
total lastlog
-------------------------------------------------------------------------------------
1 17 20.2.1.82 21.2.12.2 111 63 Permit 0
3906 2d02h
2 17 20.2.1.82 21.2.12.2 1135 63 Permit 0
3906 2d02h
3 17 20.2.1.82 21.2.12.2 2159 63 Permit 0
3906 2d02h
4 17 20.2.1.82 21.2.12.2 3183 63 Permit 0
3906 2d02h
5 17 20.2.1.82 21.2.12.2 4207 63 Permit 0
3906 2d02h
6 17 20.2.1.82 21.2.12.2 5231 63 Deny 0
3906 2d02h
7 17 20.2.1.82 21.2.12.2 6255 63 Deny 0
3906 2d02h
8 17 20.2.1.82 21.2.12.2 7279 63 Permit 0
3906 2d02h
9 17 20.2.1.82 21.2.12.2 8303 63 Permit 0
3906 2d02h
10 17 20.2.1.82 21.2.12.2 9327 63 Permit 0
3905 2d02h
11 17 20.2.1.82 21.2.12.2 10351 63 Permit 0
3905 2d02h
```

```
12 17 20.2.1.82 21.2.12.2 11375 63 Permit 0
3905 2d02h
13 17 20.2.1.82 21.2.12.2 12399 63 Deny 0
3905 2d02h
14 17 20.2.1.82 21.2.12.2 13423 63 Permit 0
3905 2d02h
15 17 20.2.1.82 21.2.12.2 14447 63 Deny 0
3905 2d02h
16 17 20.2.1.82 21.2.12.2 15471 63 Permit 0
3905 2d02h
17 17 20.2.1.82 21.2.12.2 16495 63 Permit 0
3905 2d02h
18 17 20.2.1.82 21.2.12.2 17519 63 Permit 0
3905 2d02h
19 17 20.2.1.82 21.2.12.2 18543 63 Permit 0
3905 2d02h
20 17 20.2.1.82 21.2.12.2 19567 63 Permit 0
3905 2d02h

Number of entries: 20
Number of messages logged: 112
Number of packets logged: 11200
Number of packets received for logging: 11200
Router#
```

This example shows how to display information about the logging IP access-list configuration:

```
Router# show logging ip access-list config
Logging ip access-list configuration
 Maximum number of cached entries: 8192
 Logging rate limiter: 0
 Log-update interval: 300
 Log-update threshold: 0
 Configured on input direction:
        Vlan2
        Vlan1
 Configured on output direction:
        Vlan2
Router#
```

Related Commands

Command	Description
clear logging ip access-list cache	Clears all the entries from the OAL cache and sends them to the syslog.
logging ip access-list cache (global configuration mode)	Configures the OAL parameters.
logging ip access-list cache (interface configuration mode)	Enables an OAL-logging cache on an interface that is based on direction.

show mac-address-table

To display the information about the MAC-address table, use the **show mac-address-table** command.

show mac-address-table

show mac-address-table {**address** *mac-addr*} [**all** | {**interface** *interface interface-number*} | {**vlan** *vlan-id*}]

show mac-address-table aging-time [**vlan** *vlan-id*]

show mac-address-table count [**vlan** *vlan-id*]

show mac-address-table dynamic [{**address** *mac-addr*} | {**interface** *interface interface-number*} | {**vlan** *vlan-id*}]

show mac-address-table {**interface** *interface interface-number*}

show mac-address-table limit [**vlan** *vlan-id* | {**interface** *interface*}]

show mac-address-table multicast [**count** | {{**igmp-snooping** | **mld-snooping**} [**count**]} | {**user** [**count**]} | {**vlan** *vlan-id*}]

show mac-address-table notification {**mac-move** | **threshold**}

show mac-address-table static [{**address** *mac-addr*} | **detail** | {**interface** *interface interface-number*} | {**vlan** *vlan-id*}]

show mac-address-table synchronize statistics

show mac-address-table unicast-flood

show mac-address-table vlan *vlan-id*

Syntax Description

address *mac-addr*	Displays information about the MAC-address table for a specific MAC address; see the “Usage Guidelines” section for format guidelines.
all	(Optional) Displays every instance of the specified MAC address in the forwarding table.
interface *interface*	(Optional) Displays information about a specific interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **atm**, and **ge-wan**.
interface-number	Module and port number; see the “Usage Guidelines” section for valid values.
vlan *vlan-id*	(Optional) Displays information for a specific VLAN only; valid values are from 1 to 4094.
aging-time	Displays information about the MAC-address aging time.
count	Displays the number of entries that are currently in the MAC-address table.
dynamic	Displays information about the dynamic MAC-address table entries only.

limit	Displays MAC-usage information.
multicast	Displays information about the multicast MAC-address table entries only.
igmp-snooping	Displays the addresses learned by IGMP snooping.
mld-snooping	Displays the addresses learned by MLDv2 snooping.
user	Displays the manually entered (static) addresses.
notification mac-move	Displays the MAC-move notification status.
notification threshold	Displays the CAM-table utilization notification status.
static	Displays information about the static MAC-address table entries only.
synchronize statistics	Displays information about the statistics collected on the switch processor.
unicast-flood	Displays unicast-flood information.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

If you do not specify a module number, the output of the **show mac-address-table** command displays information about the supervisor engine. To display information about the MAC-address table of the switch processor, you must enter the **all** keyword.

The *mac-addr* is a 48-bit MAC address and the valid format is H.H.H.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

Valid values for *mac-group-address* are from 1 to 9.

The optional **count** keyword displays the number of multicast entries.

The optional **multicast** keyword displays the multicast MAC addresses (groups) in a VLAN or displays all statically installed or IGMP snooping-learned entries in the Layer 2 table.

The information that is displayed in the **show mac-address-table unicast-flood** command output is as follows:

- Up to 50 flood entries, shared across all the VLANs that are not configured to use the filter mode, can be recorded.

- The output field displays are defined as follows:
  - ALERT—Information is updated approximately every 3 seconds.
  - SHUTDOWN—Information is updated approximately every 3 seconds.

Note The information displayed on the destination MAC addresses is deleted as soon as the floods stop after the port shuts down.

  - Information is updated each time that you install the filter. The information lasts until you remove the filter.

The **show mac-address-table protocol** {**assigned** | **ip** | **ipx** | **other**} syntax is not supported on Catalyst 6500 series switches that are configured with a Supervisor Engine 720.

The keyword definitions for the *protocol* argument are as follows:

- **assigned** specifies assigned protocol entries.
- **ip** specifies IP protocol.
- **ipx** specifies IPX protocols.
- **other** specifies other protocol entries.

The dynamic entries that are displayed in the Learn field are always set to Yes.

The **show mac-address-table limit** command output displays the following information:

- The current number of MAC addresses.
- The maximum number of MAC entries that are allowed.
- The percentage of usage.

The **show mac-address-table synchronize statistics** command output displays the following information:

- Number of messages processed at each time interval.
- Number of active entries sent for synchronization.
- Number of entries updated, created, ignored, or failed.

Examples

Note In a distributed EARL switch, the asterisk (*) indicates a MAC address that is learned on a port that is associated with this EARL.

This example shows how to display the information about the MAC-address table for a specific MAC address (the Catalyst 6500 series switch is configured with a Supervisor Engine 2):

```
Router# show mac-address-table address 001.6441.60ca
Codes: * - primary entry

  vlan   mac address     type    learn qos             ports
------+----------------+--------+-----+---+--------------------------
Supervisor:
*  ---  0001.6441.60ca    static  No    --  Router
Router#
```

This example shows how to display MAC-address table information for a specific MAC address (the Catalyst 6500 series switch is configured with a Supervisor Engine 720):

```
Router# show mac-address-table address 0100.5e00.0128
Legend: * - primary entry
        age - seconds since last seen
        n/a - not available

  vlan   mac address     type    learn     age              ports
------+----------------+--------+-----+----------+--------------------------
Supervisor:
*   44  0100.5e00.0128    static  Yes          -   Fa6/44,Router
*    1  0100.5e00.0128    static  Yes          -   Router
Module 9:
*   44  0100.5e00.0128    static  Yes          -   Fa6/44,Router
*    1  0100.5e00.0128    static  Yes          -   Router
Router#
```

This example shows how to display the currently configured aging time for all VLANs:

```
Router# show mac-address-table aging-time
Vlan    Aging Time
----    ----------
*100     300
200     1000

Router#
```

This example shows how to display the entry count for a specific slot:

```
Router# show mac-address-table count slot 1
MAC Entries on slot 1 :
Dynamic Address Count:                4
Static Address (User-defined) Count:  25
Total MAC Addresses In Use:           29
Total MAC Addresses Available:        131072
Router#
```

This example shows how to display all the dynamic MAC-address entries:

```
Router# show mac-address-table dynamic
Legend: * - primary entry
age - seconds since last seen
n/a - not applicable
vlan     mac address      type   learn    age              ports
------+----------------+--------+-----+----------+--------------------------
* 10   0010.0000.0000   dynamic  Yes   n/a        Gi4/1
* 3    0010.0000.0000   dynamic  Yes   0          Gi4/2
* 1    0002.fcbc.ac64   dynamic  Yes   265        Gi8/1
* 1    0009.12e9.adc0   static   No    -          Router
Router#
```

This example shows how to display the information about the MAC-address table for a specific interface (the Catalyst 6500 series switch is configured with a Supervisor Engine 720):

```
Router# show mac-address-table interface fastethernet 6/45
Legend: * - primary entry
        age - seconds since last seen
        n/a - not available

  vlan   mac address     type    learn     age              ports
------+----------------+--------+-----+----------+--------------------------
*   45  00e0.f74c.842d   dynamic  Yes          5   Fa6/45
Router#
```

Note A leading asterisk (*) indicates entries from a MAC address that was learned from a packet coming from an outside device to a specific module.

This example shows how to display the MAC-move notification status:

```
Router# show mac-address-table notification mac-move
MAC Move Notification: Enabled
Router#
```

This example shows how to display the CAM-table utilization-notification status:

```
Router# show mac-address-table notification threshold
Status limit Interval
-------------+-----------+-------------
enabled 1 120
Router#
```

This example shows how to display unicast-flood information:

```
Router# show mac-address-table unicast-flood
Unicast Flood Protection status: enabled

Configuration:
vlan Kfps action timeout
------+----------+-----------------+----------
2 2 alert none

Mac filters:
No. vlan souce mac addr. installed
on time left (mm:ss)

-----+------+-----------------+------------------------------+------------------

Flood details:
Vlan souce mac addr. destination mac addr.

------+----------------+-------------------------------------------------
2 0000.0000.cafe 0000.0000.bad0, 0000.0000.babe,
0000.0000.bac0
0000.0000.bac2, 0000.0000.bac4,
0000.0000.bac6
0000.0000.bac8
2 0000.0000.caff 0000.0000.bad1, 0000.0000.babf,
0000.0000.bac1
0000.0000.bac3, 0000.0000.bac5,
0000.0000.bac7
0000.0000.bac9
Router#
```

This example shows how to display all the static MAC-address entries (this Catalyst 6500 series switch is configured with a Supervisor Engine 2):

```
Router# show mac-address-table static
Codes: * - primary entry

  vlan   mac address     type    learn qos             ports
------+----------------+--------+-----+---+--------------------------
*  ---  0001.6441.60ca    static  No    --  Router

Router#
```

This example shows how to display the information about the MAC-address table for a specific VLAN:

```
Router# show mac-address-table vlan 100
vlan   mac address     type    protocol  qos             ports
-----+---------------+--------+---------+---+--------------------------------
 100  0050.3e8d.6400  static   assigned  --  Router
 100  0050.7312.0cff  dynamic        ip  --  Fa5/9
 100  0080.1c93.8040  dynamic        ip  --  Fa5/9
 100  0050.3e8d.6400  static        ipx  --  Router
 100  0050.3e8d.6400  static      other  --  Router
 100  0100.0cdd.dddd  static      other  --  Fa5/9,Router,Switch
 100  00d0.5870.a4ff  dynamic        ip  --  Fa5/9
 100  00e0.4fac.b400  dynamic        ip  --  Fa5/9
 100  0100.5e00.0001  static         ip  --  Fa5/9,Switch
 100  0050.3e8d.6400  static         ip  --  Router
Router#
```

This example shows how to display the information about the MAC-address table for MLDv2 snooping:

```
Router# show mac-address-table multicast mld-snooping
vlan mac address type learn qos ports
-----+---------------+--------+-----+---+---------------------------------
--- 3333.0000.0001 static Yes - Switch,Stby-Switch
--- 3333.0000.000d static Yes - Fa2/1,Fa4/1,Router,Switch
--- 3333.0000.0016 static Yes - Switch,Stby-Switch
Router#
```

Related Commands

Command	Description
mac-address-table aging-time	Configures the aging time for entries in the Layer 2 table.
mac-address-table limit	Enables MAC limiting.
mac-address-table notification mac-move	Enables MAC-move notification.
mac-address-table static	Adds static entries to the MAC-address table or configures a static MAC address with IGMP snooping disabled for that address.
mac-address-table synchronize	Synchronizes the Layer 2 MAC address table entries across the PFC.

show mac-address-table learning

To display the MAC-address learning state, use the **show mac-address-table learning** command.

show mac-address-table learning [{**vlan** *vlan-id*} | {**interface** *interface slot*/*port*}] [**module** *num*]

Syntax Description

vlan *vlan-id*	(Optional) Displays information about the MAC-address learning state for the specified switch port VLAN; valid values are from 1 to 4094.
interface *interface slot*/*port*	(Optional) Displays information about the MAC-address learning state for the specified routed interface type, the slot number, and the port number.
module *num*	(Optional) Displays information about the MAC-address learning state for the specified module number.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The **module** *num* keyword and argument can be used to specify supervisor engines only.

The **interface** *interface slot*/*port* keyword and arguments can be used on routed interfaces only. The **interface** *interface slot*/*port* keyword and arguments cannot be used to configure learning on switch-port interfaces.

If you specify the **vlan** *vlan-id*, the state of the MAC-address learning of the specified VLAN, including router interfaces, on all modules, is displayed.

If you specify the **vlan** *vlan-id* and the **module** *num*, the state of the MAC-address learning of a specified VLAN on a specified module is displayed.

If you specify the **interface** *interface slot*/*port* keyword and arguments, the state of the MAC-address learning of the specified interface on all modules is displayed.

If you specify the **interface** *interface slot*/*port* keyword and arguments, the state of the MAC-address learning of the specified interface on the specified module is displayed.

If you enter the **show mac-address-table learning** command with no arguments or keywords, the status of MAC learning on all the existing VLANs on all the supervisor engines configured on a Catalyst 6500 series switch is displayed.

Examples

This example shows how to display the MAC-address learning status on all the existing VLANs on all the supervisor engines:

```
Router# show mac-address-table learning

VLAN/Interface          Mod1   Mod4   Mod7
--------------------    ---------------------
1                       yes    yes    yes
100                     yes    yes    yes
150                     yes    yes    yes
200                     yes    yes    yes
250                     yes    yes    yes
1006                     no     no     no
1007                     no     no     no
1008                     no     no     no
1009                     no     no     no
1010                     no     no     no
1011                     no     no     no
1012                     no     no     no
1013                     no     no     no
1014                     no     no     no
GigabitEthernet6/1       no     no     no
GigabitEthernet6/2       no     no     no
GigabitEthernet6/4       no     no     no
FastEthernet3/4          no     no     no
FastEthernet3/5          no     no     no
GigabitEthernet4/1       no     no     no
GigabitEthernet4/2       no     no     no
GigabitEthernet7/1       no     no     no
GigabitEthernet7/2       no     no     no

Router#
```

Table 2-78 describes the fields that are shown in the example.

Table 2-78 show mac-address-table learning Field Descriptions

Field	Description
VLAN/Interface[1]	VLAN ID or interface type, module, and port number.
Mod#	Module number of a supervisor engine.
yes	MAC-address learning is enabled.
no	MAC-address learning is disabled.

[1] The interfaces displayed are routed interfaces that have internal VLANs assigned to them.

This example shows how to display the status of MAC-address learning on all the existing VLANs on a single supervisor engine:

```
Router# show mac-address-table learning module 4

VLAN/Interface          Mod4
--------------------    -----
1                       yes
100                     yes
150                     yes
200                     yes
250                     yes
1006                     no
1007                     no
1008                     no
1009                     no
1010                     no
1011                     no
1012                     no
1013                     no
1014                     no
GigabitEthernet6/1       no
GigabitEthernet6/2       no
GigabitEthernet6/4       no
FastEthernet3/4          no
FastEthernet3/5          no
GigabitEthernet4/1       no
GigabitEthernet4/2       no
GigabitEthernet7/1       no
GigabitEthernet7/2       no

Router#
```

This example shows how to display the status of MAC-address learning for a specific VLAN on all the supervisor engines:

```
Router# show mac-address-table learning vlan 100

VLAN    Mod1   Mod4   Mod7
----    ---------------------
100      no     no     yes
Router
```

This example shows how to display the status of MAC-address learning for a specific VLAN on a specific supervisor engine:

```
Router# show mac-address-table learning vlan 100 module 7

VLAN    Mod7
----    -----
100     yes
Router
```

This example shows how to display the status of MAC-address learning for a specific supervisor engine:

```
Router# show mac-address-table learning interface FastEthernet 3/4

Interface       Mod1   Mod4   Mod7
---------       ---------------------
Fa3/4            no     yes    no
Router
```

This example shows how to display the status of MAC-address learning for a specific interface on a specific specific supervisor engine:

```
Router# show mac-address-table learning interface FastEthernet 3/4 module 1

Interface       Mod1
---------       -----
Fa3/4            no
Router
```

Related Commands

Command	Description
mac-address-table learning	Enables MAC-address learning.

show memory dead

To display statistics of memory allocated by processes that are now terminated, use the **show memory dead** command.

show memory dead [**totals**]

Syntax Description

totals	(Optional) Displays memory totals for processes that have been terminated.

Command Default

This command has no default settings.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The **show memory dead** command displays information about processes that have been terminated. Terminated processes accounts for memory allocated under another process.

Examples

This example shows the sample output from the **show memory dead** command:

```
Router# show memory dead

                Head   Total(b)    Used(b)    Free(b)    Lowest(b)   Largest(b)
       I/O    600000    2097152     461024    1636128      1635224      1635960

          Processor memory

 Address  Bytes Prev.    Next     Ref  PrevF   NextF   Alloc PC  What
1D8310       60 1D82C8   1D8378     1                  3281FFE   Router Init
2CA964       36 2CA914   2CA9B4     1                  3281FFE   Router Init
2CAA04      112 2CA9B4   2CAAA0     1                  3A42144   OSPF Stub LSA RBTree
2CAAA0       68 2CAA04   2CAB10     1                  3A420D4   Router Init
2ED714       52 2ED668   2ED774     1                  3381C84   Router Init
2F12AC       44 2F124C   2F1304     1                  3A50234   Router Init
2F1304       24 2F12AC   2F1348     1                  3A420D4   Router Init
2F1348       68 2F1304   2F13B8     1                  3381C84   Router Init
300C28      340 300A14   300DA8     1                  3381B42   Router Init
```

Table 2-79 describes the significant fields shown in the display.

Table 2-79 show memory dead Field Descriptions

Field	Description
Head	Hexadecimal address of the head of the memory allocation chain.
Total(b)	Sum of used bytes plus free bytes.
Used(b)	Amount of memory in use.
Free(b)	Amount of memory not in use (in bytes).
Lowest(b)	Smallest amount of free memory since last boot (in bytes).
Largest(b)	Size of the largest available free block (in bytes).
Address	Hexadecimal address of the block (in bytes).
Bytes	Size of the block (in bytes).
Prev.	Address of the preceding block.
Next	Address of the following block.
Ref	Reference count for that memory block, indicating how many different processes are using that block of memory.
PrevF	Address of the preceding free block (if free).
NextF	Address of the following free block (if free).
Alloc PC	Address of the system call that allocated the block.
What	Name of the process that owns the block, or “(fragment)” if the block is a fragment, or “(coalesced)” if the block was coalesced from adjacent free blocks.

show mls asic

To display the ASIC version, use the **show mls asic** command.

show mls asic

Syntax Description

This command has no keywords or arguments.

Command Default

This command has no default settings.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to display the ASIC versions:

```
Router# show mls asic
Earl in Module 2
 Tycho - ver:1 Cisco-id:1C8 Vendor-id:49
Router#
```