

show controllers vsi control-interface

To display information about an ATM interface configured with the **tag-control-protocol vsi** command to control an external switch (or if an interface is not specified, to display information about all Virtual Switch Interface [VSI] control interfaces), use the **show controllers vsi control-interface** command in user EXEC or privileged EXEC mode.

```
show controllers vsi control-interface [interface]
```

Syntax Description

<i>interface</i>	(Optional) Specifies the interface number.
------------------	--

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Examples

The following is sample output from the **show controllers vsi control-interface** command:

```
Router# show controllers vsi control-interface
```

```
Interface:          ATM2/0          Connections:          14
```

The display shows the number of cross-connects currently on the switch that were established by the MPLS LSC through the VSI over the control interface.

Related Commands

Command	Description
tag-control-protocol vsi	Configures the use of VSI on a control port.

show controllers vsi descriptor

To display information about a switch interface discovered by the Multiprotocol Label Switching (MPLS) Label Switch Controller (LSC) through a Virtual Switch Interface (VSI), or if no descriptor is specified, about all such discovered interfaces, use the **show controllers vsi descriptor** command in user EXEC or privileged EXEC mode.

show controllers vsi descriptor [*descriptor*]

Syntax Description

<i>descriptor</i>	(Optional) Physical descriptor. For the Cisco BPX switch, the physical descriptor has the following form: <i>slot.port.0</i>
-------------------	--

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Specify an interface by its (switch-supplied) physical descriptor.

Per-interface information includes the following:

- Interface name
- Physical descriptor
- Interface status
- Physical interface state (supplied by the switch)
- Acceptable VPI and VCI ranges
- Maximum cell rate
- Available cell rate (forward/backward)
- Available channels

Similar information is displayed when you enter the **show controllers xtagatm** privileged EXEC command. However, you must specify a Cisco IOS interface name instead of a physical descriptor.

Examples

The following is sample output from the **show controllers vsi descriptor** command:

```
Router# show controllers vsi descriptor 12.2.0

Phys desc: 12.2.0
Log intf:  0x000C0200 (0.12.2.0)
Interface: XTagATM0
IF status: up                               IFC state: ACTIVE
Min VPI:   1                                Maximum cell rate: 10000
Max VPI:   259                              Available channels: 2000
```

show controllers vsi descriptor

```

Min VCI:    32                Available cell rate (forward): 10000
Max VCI:    65535            Available cell rate (backward): 10000

```

Table 12 describes the significant fields in the display.

Table 12 *show controllers vsi descriptor Field Descriptions*

Field	Description
Phys desc	Physical descriptor. A string learned from the switch that identifies the interface.
Log intf	Logical interface ID. This 32-bit entity, learned from the switch, uniquely identifies the interface.
Interface	The (Cisco IOS) interface name.
IF status	Overall interface status. Can be “up,” “down,” or “administratively down.”
Min VPI	Minimum virtual path identifier. Indicates the low end of the VPI range configured on the switch.
Max VPI	Maximum virtual path identifier. Indicates the high end of the VPI range configured on the switch.
Min VCI	Minimum virtual channel identifier. Indicates the low end of the VCI range configured on the switch.
Max VCI	Maximum virtual channel identifier. Indicates the high end of the VCI range configured on, or determined by, the switch.
IFC state	Operational state of the interface, according to the switch. Can be one of the following: <ul style="list-style-type: none"> FAILED_EXT (that is, an external alarm) FAILED_INT (indicates the inability of the MPLS LSC to communicate with the VSI slave controlling the interface, or another internal failure) REMOVED (administratively removed from the switch)
Maximum cell rate	Maximum cell rate for the interface, which has been configured on the switch (in cells per second).
Available channels	Indicates the number of channels (endpoints) that are currently free to be used for cross-connects.
Available cell rate (forward)	Cell rate that is currently available in the forward (that is, ingress) direction for new cross-connects on the interface.
Available cell rate (backward)	Cell rate that is currently available in the backward (that is, egress) direction for new cross-connects on the interface.

Related Commands

Command	Description
show controllers xtagatm	Displays information about an extended MPLS ATM interface.

show controllers vsi session

To display information about all sessions with Virtual Switch Interface (VSI) slaves, use the **show controllers vsi session** command in user EXEC or privileged EXEC mode.

show controllers vsi session [*session-number* [**interface** *interface*]]



Note

A session consists of an exchange of VSI messages between the VSI master (the LSC) and a VSI slave (an entity on the switch). There can be multiple VSI slaves for a switch. On the BPX, each port or trunk card assumes the role of a VSI slave.

Syntax Description

<i>session-number</i>	(Optional) Specifies the session number.
interface <i>interface</i>	(Optional) Specifies the VSI control interface.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

If a session number and an interface are specified, detailed information on the individual session is presented. If the session number is specified, but the interface is omitted, detailed information on all sessions with that number is presented. (Only one session can contain a given number, because multiple control interfaces are not supported.)

Examples

The following is sample output from the **show controllers vsi session** command:

Router# **show controllers vsi session**

Interface	Session	VCD	VPI/VCI	Switch/Slave Ids	Session State
ATM0/0	0	1	0/40	0/1	ESTABLISHED
ATM0/0	1	2	0/41	0/2	ESTABLISHED
ATM0/0	2	3	0/42	0/3	DISCOVERY
ATM0/0	3	4	0/43	0/4	RESYNC-STARTING
ATM0/0	4	5	0/44	0/5	RESYNC-STOPPING
ATM0/0	5	6	0/45	0/6	RESYNC-UNDERWAY
ATM0/0	6	7	0/46	0/7	UNKNOWN
ATM0/0	7	8	0/47	0/8	UNKNOWN
ATM0/0	8	9	0/48	0/9	CLOSING
ATM0/0	9	10	0/49	0/10	ESTABLISHED
ATM0/0	10	11	0/50	0/11	ESTABLISHED
ATM0/0	11	12	0/51	0/12	ESTABLISHED

Table 13 describes the significant fields in the display.

Table 13 show controllers vsi session Field Descriptions

Field	Description
Interface	Control interface name.
Session	Session number (from 0 to $\langle n-1 \rangle$), where n is the number of sessions on the control interface.
VCD	Virtual circuit descriptor (virtual circuit number). Identifies the VC carrying the VSI protocol between the master and the slave for this session.
VPI/VCI	Virtual path identifier or virtual channel identifier (for the VC used for this session).
Switch/Slave Ids	Switch and slave identifiers supplied by the switch.
Session State	Indicates the status of the session between the master and the slave. <ul style="list-style-type: none"> ESTABLISHED is the fully operational steady state. UNKNOWN indicates that the slave is not responding. <p>Other possible states include the following:</p> <ul style="list-style-type: none"> CONFIGURING RESYNC_STARTING RESYNC_UNDERWAY RESYNC_ENDING DISCOVERY SHUTDOWN_STARTING SHUTDOWN_ENDING INACTIVE

In the following example, session number 9 is specified with the **show controllers vsi session** command:

```
Router# show controllers vsi session 9

Interface:          ATM1/0          Session number:      9
VCD:                10              VPI/VCI:            0/49
Switch type:        BPX              Switch id:           0
Controller id:      1                Slave id:            10
Keepalive timer:    15              Powerup session id: 0x0000000A
Cfg/act retry timer: 8/8            Active session id:  0x0000000A
Max retries:        10              Ctrl port log intf: 0x000A0100
Trap window:        50              Max/actual cmd wndw: 21/21
Trap filter:        all              Max checksums:      19
Current VSI version: 1              Min/max VSI version: 1/1
Messages sent:      2502            Inter-slave timer:  4.000
Messages received: 2502            Messages outstanding: 0
```

Table 14 describes the significant fields in the display.

Table 14 *show controllers vsi session Field Descriptions*

Field	Description
Interface	Name of the control interface on which this session is configured.
Session number	A number from 0 to <n-1>, where <i>n</i> is the number of slaves. Configured on the MPLS LSC with the <i>slaves</i> option of the tag-control-protocol vsi command.
VCD	Virtual circuit descriptor (virtual circuit number). Identifies the VC that carries VSI protocol messages for this session.
VPI/VCI	Virtual path identifier or virtual channel identifier for the VC used for this session.
Switch type	Switch device (for example, the BPX).
Switch id	Switch identifier (supplied by the switch).
Controller id	Controller identifier. Configured on the LSC, and on the switch, with the id option of the tag-control-protocol vsi command.
Slave id	Slave identifier (supplied by the switch).
Keepalive timer	VSI master keepalive timeout period (in seconds). Configured on the MPLS LSC through the keepalive option of the tag-control-protocol vsi command. If no valid message is received by the MPLS LSC within this time period, it sends a keepalive message to the slave.
Powerup session id	Session ID (supplied by the slave) used at powerup time.
Cfg/act retry timer	Configured and actual message retry timeout period (in seconds). If no response is received for a command sent by the master within the actual retry timeout period, the message is resent. This applies to most message transmissions. The configured retry timeout value is specified through the retry option of the tag-control-protocol vsi command. The actual retry timeout value is the larger of the configured value and the minimum retry timeout value permitted by the switch.
Active session id	Session ID (supplied by the slave) for the currently active session.
Max retries	Maximum number of times that a particular command transmission will be retried by the master. That is, a message may be sent up to <max_retries+1> times. Configured on the MPLS LSC through the retry option of the tag-control-protocol vsi command.
Ctrl port log intf	Logical interface identifier for the control port, as supplied by the switch.
Trap window	Maximum number of outstanding trap messages permitted by the master. This is advertised, but not enforced, by the LSC.
Max/actual cmd wndw	Maximum command window is the maximum number of outstanding (that is, unacknowledged) commands that may be sent by the master before waiting for acknowledgments. This number is communicated to the master by the slave. The command window is the maximum number of outstanding commands that are permitted by the master, before it waits for acknowledgments. This is always less than the maximum command window.

Table 14 *show controllers vsi session Field Descriptions (continued)*

Field	Description
Trap filter	This is always “all” for the LSC, indicating that it wants to receive all traps from the slave. This is communicated to the slave by the master.
Max checksums	Maximum number of checksum blocks supported by the slave.
Current VSI version	VSI protocol version currently in use by the master for this session.
Min/max VSI version	Minimum and maximum VSI versions supported by the slave, as last reported by the slave. If both are zero, the slave has not yet responded to the master.
Messages sent	Number of commands sent to the slave.
Inter-slave timer	Timeout value associated by the slave for messages it sends to other slaves. On a VSI-controlled switch with a distributed slave implementation (such as the BPX), VSI messages may be sent between slaves to complete their processing. For the MPLS LSC VSI implementation to function properly, the value of its retry timer is forced to be at least two times the value of the interslave timer. (See “Cfg/act retry timer” in this table.)
Messages received	Number of responses and traps received by the master from the slave for this session.
Messages outstanding	Current number of outstanding messages (that is, commands sent by the master for which responses have not yet been received).

Related Commands

Command	Description
tag-control-protocol vsi	Configures the use of VSI on a control port.

show controllers vsi status

To display a one-line summary of each Virtual Switch Interface (VSI)-controlled interface, use the **show controllers vsi status** command in user EXEC or privileged EXEC mode.

show controllers vsi status

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines If an interface is discovered by the LSC, but no extended Multiprotocol Label Switching (MPLS) ATM interface is associated with it through the **extended-port** command, then the interface name is marked <unknown>, and interface status is marked n/a.

Examples The following is sample output from the **show controllers vsi status** command:

```
Router# show controllers vsi status
```

```
Interface Name           IF Status   IFC State   Physical Descriptor
switch control port     n/a        ACTIVE      12.1.0
XTagATM0                 up          ACTIVE      12.2.0
XTagATM1                 up          ACTIVE      12.3.0
<unknown>                n/a        FAILED-EXT  12.4.0
```

Table 15 describes the significant fields in the display.

Table 15 *show controllers vsi status Field Descriptions*

Field	Description
Interface Name	The (Cisco IOS) interface name.
IF Status	Overall interface status. Can be “up,” “down,” or “administratively down.”
IFC State	The operational state of the interface, according to the switch. Can be one of the following: <ul style="list-style-type: none"> FAILED_EXT (that is, an external alarm) FAILED_INT (indicates the inability of the MPLS LSC to communicate with the VSI slave controlling the interface, or another internal failure) REMOVED (administratively removed from the switch)
Physical Descriptor	A string learned from the switch that identifies the interface.

show controllers vsi traffic

To display traffic information about Virtual Switch Interface (VSI)-controlled interfaces, VSI sessions, or virtual circuits (VCs) on VSI-controlled interfaces, use the **show controllers vsi traffic** command in user EXEC or privileged EXEC mode.

```
show controllers vsi traffic {descriptor descriptor | session session-number | vc [descriptor
descriptor [vpi vci]]}
```

Syntax Description

descriptor <i>descriptor</i>	Specifies the interface.
session <i>session-number</i>	Specifies a session number.
<i>vpi</i>	Virtual path identifier (0 to 4095).
<i>vci</i>	Virtual circuit identifier (0 to 65535).

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(4)T	The VPI range of values was extended to 4095.

Usage Guidelines

If none of the keywords is specified, traffic for all interfaces is displayed. You can specify a single interface by its (switch-supplied) physical descriptor. For the BPX switch, the physical descriptor has the form

slot.port. 0

If a session number is specified, the output displays VSI protocol traffic by message type. The VC traffic display is also displayed by the **show xmplsatm vc cross-connect traffic descriptor** command.

Examples

The following is sample output from the **show controllers vsi traffic** command:

```
Router# show controllers vsi traffic

Phys desc: 10.1.0
Interface: switch control port
IF status: n/a
Rx cells: 304250           Rx cells discarded: 0
Tx cells: 361186           Tx cells discarded: 0
Rx header errors: 4294967254 Rx invalid addresses (per card): 80360
Last invalid address: 0/53

Phys desc: 10.2.0
Interface: XTagATM0
IF status: up
Rx cells: 202637           Rx cells discarded: 0
Tx cells: 194979           Tx cells discarded: 0
Rx header errors: 4294967258 Rx invalid addresses (per card): 80385
```

```

Last invalid address: 0/32

Phys desc: 10.3.0
Interface: XTagATM1
IF status: up
Rx cells: 182295           Rx cells discarded: 0
Tx cells: 136369           Tx cells discarded: 0
Rx header errors: 4294967262 Rx invalid addresses (per card): 80372
Last invalid address: 0/32

```

Table 16 describes the significant fields shown in the display.

Table 16 *show controllers vsi traffic Field Descriptions*

Field	Description
Phys desc	Physical descriptor of the interface.
Interface	The Cisco (IOS) interface name.
Rx cells	Number of cells received on the interface.
Tx cells	Number of cells transmitted on the interface.
Rx cells discarded	Number of cells received on the interface that were discarded due to traffic management.
Tx cells discarded	Number of cells that could not be transmitted on the interface due to traffic management and which were therefore discarded.
Rx header errors	Number of cells that were discarded due to ATM header errors.
Rx invalid addresses	Number of cells received with an invalid address (that is, an unexpected VPI/VCI combination). With the Cisco BPX switch, this count is of all such cells received on all interfaces in the port group of this interface.
Last invalid address	Number of cells received on this interface with ATM cell header errors.

The following sample output is displayed when you enter the **show controllers vsi traffic session 9** command:

```
Router# show controllers vsi traffic session 9
          Sent                               Received
Sw Get Cnfg Cmd:      3656      Sw Get Cnfg Rsp:      3656
Sw Cnfg Trap Rsp:    0          Sw Cnfg Trap:         0
Sw Set Cnfg Cmd:      1          Sw Set Cnfg Rsp:     1
Sw Start Resync Cmd:  1          Sw Start Resync Rsp: 1
Sw End Resync Cmd:   1          Sw End Resync Rsp:   1
Ifc Getmore Cnfg Cmd: 1          Ifc Getmore Cnfg Rsp: 1
Ifc Cnfg Trap Rsp:   4          Ifc Cnfg Trap:       4
Ifc Get Stats Cmd:   8          Ifc Get Stats Rsp:   8
Conn Cmt Cmd:        73         Conn Cmt Rsp:        73
Conn Del Cmd:        50         Conn Del Rsp:        0
Conn Get Stats Cmd:  0          Conn Get Stats Rsp:  0
Conn Cnfg Trap Rsp:  0          Conn Cnfg Trap:     0
Conn Bulk Clr Stats Cmd: 0      Conn Bulk Clr Stats Rsp: 0
Gen Err Rsp:         0          Gen Err Rsp:         0
unused:              0          unused:              0
unknown:             0          unknown:             0
TOTAL:               3795      TOTAL:               3795
```

Table 17 describes the significant fields shown in the display.

Table 17 show controllers vsi traffic session Field Descriptions

Field	Description
Sw Get Cnfg Cmd	Number of VSI “get switch configuration command” messages sent.
Sw Cnfg Trap Rsp	Number of VSI “switch configuration asynchronous trap response” messages sent.
Sw Set Cnfg Cmd	Number of VSI “set switch configuration command” messages sent.
Sw Start Resync Cmd	Number of VSI “set resynchronization start command” messages sent.
Sw End Resync Cmd	Number of VSI “set resynchronization end command” messages sent.
Ifc Getmore Cnfg Cmd	Number of VSI “get more interfaces configuration command” messages sent.
Ifc Cnfg Trap Rsp	Number of VSI “interface configuration asynchronous trap response” messages sent.
Ifc Get Stats Cmd	Number of VSI “get interface statistics command” messages sent.
Conn Cmt Cmd	Number of VSI “set connection committed command” messages sent.
Conn Del Cmd	Number of VSI “delete connection command” messages sent.
Conn Get Stats Cmd	Number of VSI “get connection statistics command” messages sent.
Conn Cnfg Trap Rsp	Number of VSI “connection configuration asynchronous trap response” messages sent.
Conn Bulk Clr Stats Cmd	Number of VSI “bulk clear connection statistics command” messages sent.
Gen Err Rsp	Number of VSI “generic error response” messages sent or received.
Sw Get Cnfg Rsp	Number of VSI “get connection configuration command response” messages received.
Sw Cnfg Trap	Number of VSI “switch configuration asynchronous trap” messages received.

Table 17 *show controllers vsi traffic session Field Descriptions (continued)*

Field	Description
Sw Set Cnfg Rsp	Number of VSI “set switch configuration response” messages received.
Sw Start Resync Rsp	Number of VSI “set resynchronization start response” messages received.
Sw End Resync Rsp	Number of VSI “set resynchronization end response” messages received.
Ifc Getmore Cnfg Rsp	Number of VSI “get more interfaces configuration response” messages received.
Ifc Cnfg Trap	Number of VSI “interface configuration asynchronous trap” messages received.
Ifc Get Stats Rsp	Number of VSI “get interface statistics response” messages received.
Conn Cmt Rsp	Number of VSI “set connection committed response” messages received.
Conn Del Rsp	Number of VSI “delete connection response” messages received.
Conn Get Stats Rsp	Number of VSI “get connection statistics response” messages received.
Conn Cnfg Trap	Number of VSI “connection configuration asynchronous trap” messages received.
Conn Bulk Clr Stats Rsp	Number of VSI “bulk clear connection statistics response” messages received.
unused, unknown	<p>“Unused” messages are those whose function codes are recognized as being part of the VSI protocol, but which are not used by the MPLS LSC and, consequently, are not expected to be received or sent.</p> <p>“Unknown” messages have function codes that the MPLS LSC does not recognize as part of the VSI protocol.</p>
TOTAL	Total number of VSI messages sent or received.

show controllers xtagatm

To display information about an extended Multiprotocol Label Switching (MPLS) ATM interface controlled through the Virtual Switch Interface (VSI) protocol (or, if an interface is not specified, to display information about all extended MPLS ATM interfaces controlled through the VSI protocol), use the **show controllers xtagatm** command in user EXEC or privileged EXEC mode.

show controllers xtagatm *if-number*

Syntax Description

<i>if-number</i>	Specifies the interface number.
------------------	---------------------------------

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Per-interface information includes the following:

- Interface name
- Physical descriptor
- Interface status
- Physical interface state (supplied by the switch)
- Acceptable VPI and VCI ranges
- Maximum cell rate
- Available cell rate (forward/backward)
- Available channels

Similar information appears if you enter the **show controllers vsi descriptor** command. However, you must specify an interface by its (switch-supplied) physical descriptor, instead of its Cisco IOS interface name. For the Cisco BPX switch, the physical descriptor has the form *slot.port.0*.

Examples

In this example, the sample output is from the **show controllers xtagatm** command specifying interface 0:

```
Router# show controllers xtagatm 0

Interface XTagATM0 is up
Hardware is Tag-Controlled ATM Port (on BPX switch BPX-VSI1)
Control interface ATM1/0 is up
Physical descriptor is 10.2.0
Logical interface 0x000A0200 (0.10.2.0)
Oper state ACTIVE, admin state UP
VPI range 1-255, VCI range 32-65535
VPI is not translated at end of link
```

```

Tag control VC need not be strictly in VPI/VCI range
Available channels: ingress 30, egress 30
Maximum cell rate: ingress 300000, egress 300000
Available cell rate: ingress 300000, egress 300000
Endpoints in use: ingress 7, egress 8, ingress/egress 1
Rx cells 134747
rx cells discarded 0, rx header errors 0
rx invalid addresses (per card): 52994
last invalid address 0/32
Tx cells 132564
tx cells discarded: 0

```

Table 18 describes the significant fields in the display.

Table 18 *show controllers xtagatm Field Descriptions*

Field	Description
Interface XTagATM0 is up	Indicates the overall status of the interface. May be “up,” “down,” or “administratively down.”
Hardware is Tag-Controlled ATM Port	<p>Indicates the hardware type.</p> <p>If the XTagATM was successfully associated with a switch port, a description of the form (on <switch_type> switch <name>) follows this field, where <switch_type> indicates the type of switch (for example, BPX), and the name is an identifying string learned from the switch.</p> <p>If the XTagATM interface was not bound to a switch interface (with the extended-port interface configuration command), then the label “Not bound to a control interface and switch port” appears.</p> <p>If the interface has been bound, but the target switch interface has not been discovered by the LSC, then the label “Bound to undiscovered switch port (id <number>)” appears, where <number> is the logical interface ID in hexadecimal notation.</p>
Control interface ATM1/0 is up	Indicates that the XTagATM interface was bound (with the extended-port interface configuration command) to the VSI master whose control interface is ATM1/0 and that this control interface is up.
Physical descriptor is...	A string identifying the interface that was learned from the switch.
Logical interface	This 32-bit entity, learned from the switch, uniquely identifies the interface. It appears in both hexadecimal and dotted quad notation.
Oper state	<p>Operational state of the interface, according to the switch. Can be one of the following:</p> <ul style="list-style-type: none"> ACTIVE FAILED_EXT (that is, an external alarm) FAILED_INT (indicates the inability of the MPLS LSC to communicate with the VSI slave controlling the interface, or another internal failure) REMOVED (administratively removed from the switch)
admin state	Administrative state of the interface, according to the switch—either “Up” or “Down.”
VPI range 1 to 255	Indicates the allowable VPI range for the interface that was configured on the switch.

Table 18 *show controllers xtagatm Field Descriptions (continued)*

Field	Description
VCI range 32 to 65535	Indicates the allowable VCI range for the interface that was configured on, or determined by, the switch.
LSC control VC need not be strictly in VPI or VCI range	Indicates that the label control VC does not need to be within the range specified by VPI range, but may be on VPI 0 instead.
Available channels	Indicates the number of channels (endpoints) that are currently free to be used for cross-connects.
Maximum cell rate	Maximum cell rate for the interface, which was configured on the switch.
Available cell rate	Cell rate that is currently available for new cross-connects on the interface.
Endpoints in use	Number of endpoints (channels) in use on the interface, broken down by anticipated traffic flow, as follows: <ul style="list-style-type: none"> • Ingress—Endpoints carry traffic into the switch • Egress—Endpoints carry traffic away from the switch • Ingress/egress—Endpoints carry traffic in both directions
Rx cells	Number of cells received on the interface.
rx cells discarded	Number of cells received on the interface that were discarded due to traffic management actions (rx header errors).
rx header errors	Number of cells received on the interface with cell header errors.
rx invalid addresses (per card)	Number of cells received with invalid addresses (that is, unexpected VPI or VCI.). On the BPX, this counter is maintained per port group (not per interface).
last invalid address	Address of the last cell received on the interface with an invalid address (for example, 0/32).
Tx cells	Number of cells sent from the interface.
tx cells discarded	Number of cells intended for transmission from the interface that were discarded due to traffic management actions.

Related Commands

Command	Description
show controllers vsi descriptor	Displays information about a switch interface discovered by the MPLS LSC through the VSI.

show interface stats

To display numbers of packets that were process switched, fast switched, and distributed switched, use the **show interface stats** command in user EXEC or privileged EXEC mode.

show interface *type number* **stats**

Syntax Description	<i>type number</i>	Interface type and number about which to display statistics.
---------------------------	--------------------	--

Command Modes	User EXEC Privileged EXEC
----------------------	------------------------------

Command History	Release	Modification
	11.0	This command was introduced.

Usage Guidelines Use this command on the RP.



Note

When fast switching is configured on the outbound interface, and RSP optimum, RSP flow, and VIP DFS switching modes are all specified on the incoming interface, the interface on which RSP optimum, RSP flow, and VIP DFS switching modes is not enabled can still show packets switched out via those switching paths when packets are received from other interfaces with RSP optimum, RSP flow, and VIP DES switching modes enabled.

Examples The following is sample output from the **show interface stats** command:

```
Router# show interface fddi 3/0/0 stats

Fddi3/0/0
  Switching path   Pkts In   Chars In   Pkts Out   Chars Out
    Processor      3459994  1770812197  4141096   1982257456
    Route cache    10372326  3693920448   439872    103743545
  Distributed cache 19257912  1286172104  86887377  1184358085
    Total          33090232  2455937453  91468345  3270359086
```

[Table 19](#) describes the significant fields in the display.

Table 19 *show interface stats* Field Descriptions

Field	Description
Fddi3/0/0	Interface for which information is shown.
Switching path	Column heading for the various switching paths below it.
Pkts In	Number of packets received in each switching mechanism.
Chars In	Number of characters received in each switching mechanism.

Table 19 *show interface stats Field Descriptions (continued)*

Field	Description
Pkts Out	Number of packets sent out each switching mechanism.
Chars Out	Number of characters sent out each switching mechanism.

show interface xtagatm

To display information about an extended Multiprotocol Label Switching (MPLS) ATM interface, use the **show interface xtagatm** command in user EXEC or privileged EXEC mode.

show interface xtagatm *if-number*

Syntax Description

<i>if-number</i>	Specifies the MPLS ATM interface number.
------------------	--

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3T	Sample command output was added for when an interface is down.

Usage Guidelines

Extended MPLS ATM interfaces are virtual interfaces that are created on first reference like tunnel interfaces. Extended MPLS ATM interfaces are similar to ATM interfaces except that the former only supports LC-ATM encapsulation.

Examples

The following is sample command output when an interface is down:

Router# **show interface xt92**

```

XTagATM92 is down, line protocol is down
Hardware is Tag-Controlled Switch Port
Interface is unnumbered. Using address of Loopback1 (15.15.15.15)
MTU 4470 bytes, BW 4240 Kbit, DLY 80 used,
reliability 186/255, txload 1/255, rxload 1/255
Encapsulation ATM, loopback not set
Keepalive set (10 sec) [00:00:08/4]
Encapsulation(s): AAL5
Control interface: not configured
0 terminating VCs
Switch port traffic:
  ? cells input, ? cells output
Last input 00:00:10, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
Terminating traffic:
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
 138 packets input, 9193 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 i
00:05:46: %SYS-5-CONFIG_I: Configured from console by consolegnored, 0 abort
142 packets output, 19686 bytes, 0 underruns

```

show interface xtagatm

```
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
```

The following is sample command output when an interface is up:

Router# show interface xt92

```
XTagATM92 is up, line protocol is up
Hardware is Tag-Controlled Switch Port
Interface is unnumbered. Using address of Loopback1 (15.15.15.15)
MTU 4470 bytes, BW 4240 Kbit, DLY 80 used,
reliability 174/255, txload 1/255, rxload 1/255
Encapsulation ATM, loopback not set
Keepalive set (10 sec)
Encapsulation(s): AAL5
Control interface: ATM3/0, switch port: bpx 9.2
3 terminating VCs, 7 switch cross-connects
Switch port traffic:
275 cells input, 273 cells output
Last input 00:00:00, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
Terminating traffic:
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
127 packets input, 8537 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
131 packets output, 18350 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
```

Table 20 describes the significant fields shown in the displays.

Table 20 *show interface xtagatm Field Descriptions*

Field	Description
XTagATM0 is up XTagATM0 is down	Interface is currently active (up) or inactive (down).
line protocol is up line protocol is down	Displays the line protocol as up or down.
Hardware is Tag-Controlled Switch Port	Specifies the hardware type.
Interface is unnumbered	Specifies that this is an unnumbered interface.
MTU	Maximum transmission unit of the extended MPLS ATM interface.
BW	Bandwidth of the interface (in kBps).
DLY	Delay of the interface in microseconds.
reliability	Reliability of the interface as a fraction of 255 (255/255 is 100% reliability), calculated as an exponential average over 5 minutes.
Encapsulation ATM	Encapsulation method.
loopback not set	Indicates that loopback is not set.

Table 20 *show interface xtagatm Field Descriptions (continued)*

Field	Description
Keepalive set (10 sec) [00:00:08/4]	Indicates why the Xtag line is down. Valid values are: 1—Internal usage. 2—Administratively down. 3—Internal usage. 4—No extended port is configured. 5—Some cross-connects from an old session have been left operational. 6—No extended port or a wrong extended port was configured. 7—No control port was configured. 8—Internal usage. 9—Internal usage. 10—Internal usage. 11—Internal usage. 12—External port. The XTag is mapped to an invalid port on the switch. 13—External port. The XTag is mapped to a port that is down. 14—External port is mapped to the control panel on the switch. 15—OAM is being used to track the link state. The neighbor may be down or it is not responding to the OAM calls.
Encapsulation(s)	Identifies the ATM adaptation layer.
Control interface	Identifies the control port switch port with which the extended MPLS ATM interface has been associated through the extended-port interface configuration command.
<i>n</i> terminating VCs	Number of terminating VCs with an endpoint on this extended MPLS ATM interface. Packets are sent or received by the MPLS LSC on a terminating VC, or are forwarded between an LSC-controlled switch port and a router interface.
7 switch cross-connects	Number of switch cross-connects on the external switch with an endpoint on the switch port that corresponds to this interface. This includes cross-connects to terminating VCs that carry data to and from the LSC, and cross-connects that bypass the MPLS LSC and switch cells directly to other ports.
Switch port traffic	Number of cells received and sent on all cross-connects associated with this interface.
Terminating traffic	Indicates that counters below this line apply only to packets sent or received on terminating VCs.
5-minute input rate, 5-minute output rate	Average number of bits and packets sent per second in the last 5 minutes.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.

Table 20 *show interface xtagatm Field Descriptions (continued)*

Field	Description
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernet systems and bursts of noise on serial lines are often responsible for no input buffer events.
broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the medium's minimum packet size.
giants	Number of packets that are discarded because they exceed the medium's maximum packet size.
input errors	Total number of no buffer, runts, giants, CRCs, frame, overrun, ignored and abort counts. Other input-related errors can also increment the count, so that this sum may not balance with other counts.
CRC	<p>Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received.</p> <p>On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus. A high number of CRCs is usually the result of traffic collisions or a station sending bad data.</p> <p>On a serial link, CRCs usually indicate noise, gain hits, or other transmission problems on the data link.</p>
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different from the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be incremented.
abort	Illegal sequence of one bits on the interface. This usually indicates a clocking problem between the interface and the data-link equipment.
packets output	Total number of messages sent by the system.
bytes	Total number of bytes, including data and MAC encapsulation, sent by the system.
underruns	Number of times that the sender has been running faster than the router can handle data. This condition may never be reported on some interfaces.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.

Table 20 *show interface xtagatm Field Descriptions (continued)*

Field	Description
collisions	Number of messages re-sent due to an Ethernet collision. This is usually the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only one time in output packets.
interface resets	Number of times an interface has been completely reset. Resets occur if packets queued for transmission were not sent within several seconds. On a serial line, this can be caused by a malfunctioning modem that is not supplying the transmit clock signal, or by a cable problem. If the system notices that the carrier detect line of a serial interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.

Related Commands

Command	Description
interface xtagatm	Enters configuration mode for an extended MPLS ATM (XTagATM) interface.

show interfaces switching

To display the number of packets sent and received on an interface classified by the switching path, use the **show interfaces switching** command in user EXEC and privileged EXEC mode.

show interfaces [*type number*] **switching**

Syntax Description

<i>type number</i>	Interface type and number about which to display packet switching path information.
--------------------	---

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3	This command was introduced.

Usage Guidelines

Use the **show interfaces switching** command to show which path the router uses and how the traffic is switched. This command is also useful for troubleshooting CPU utilization.

Statistics for packets in, bytes in, packets out, and bytes out are displayed for the available protocols. The statistics are arranged by process, cache misses, fast-path and autonomous path. All values displayed by the **show interfaces switching** command are absolute. The **clear interface counters** command has no effect on these values.

You must enter at least seven characters of the **switching** keyword (**switchi**) when you use the **show interfaces switching** command.

Examples

The following shows sample output from the **show interfaces switching** command:

```
Router# show interface switching

FastEthernet0/0
  Throttle count      0
  Drops              RP      0      SP      0
  SPD Flushes        Fast      0      SSE     0
  SPD Aggress        Fast      0
  SPD Priority        Inputs    0      Drops   0

  Protocol IP
  Switching path     Pkts In  Chars In  Pkts Out  Chars Out
  Process            24      8208     0          0
  Cache misses
  Fast               0        0        0          0
  Auton/SSE          0        0        0          0

  Protocol DECnet
  Switching path     Pkts In  Chars In  Pkts Out  Chars Out
  Process            0        0        0          0
  Cache misses
  Fast               0        0        0          0
```

```

Auton/SSE          0          0          0          0
.....
.....

Protocol IPv6
Switching path    Pkts In    Chars In    Pkts Out    Chars Out
  Process          0          0          0          0
Cache misses      0          -          -          -
  Fast             0          0          0          0
Auton/SSE         0          0          0          0

Protocol Other
Switching path    Pkts In    Chars In    Pkts Out    Chars Out
  Process          2          120         3          180
Cache misses      0          -          -          -
  Fast             0          0          0          0
Auton/SSE         0          0          0          0

```

NOTE: all counts are cumulative and reset only after a reload.

Interface POS4/0 is disabled

The following shows sample output from the **show interfaces switching** command for the interface FastEthernet 0/0:

Router> **show interfaces FastEthernet 0/0 switching**

```

FastEthernet0/0
  Throttle count      0
    Drops              RP          SP          0
  SPD Flushes         Fast      218         SSE          0
  SPD Aggress         Fast          0
  SPD Priority         Inputs      0          Drops          0

Protocol IP
Switching path    Pkts In    Chars In    Pkts Out    Chars Out
  Process          239      23422      237      23226
Cache misses      0          -          -          -
  Fast             0          0          0          0
Auton/SSE         0          0          0          0

Protocol ARP
Switching path    Pkts In    Chars In    Pkts Out    Chars Out
  Process          4          240         3          180
Cache misses      0          -          -          -
  Fast             0          0          0          0
Auton/SSE         0          0          0          0

Protocol CDP
Switching path    Pkts In    Chars In    Pkts Out    Chars Out
  Process          8          2632        15      5477
Cache misses      0          -          -          -
  Fast             0          0          0          0
Auton/SSE         0          0          0          0

```

NOTE: all counts are cumulative and reset only after a reload.

Table 21 describes the significant fields shown in the display.

Table 21 *show interfaces switching Field Descriptions*

Field	Description
Throttle count	Number of times input packet processing was throttled on this interface.
Drops	RP—Number of packets dropped for input congestion. SP—Number of packets flushed by external throttling.
SPD Flushes	Fast—Number of packets flushed by selective packet discard on RP. SSE—Number of packets flushed by external selective packet discard.
SPD Aggress	Fast—Input packets dropped by aggressive selective packet discard.
SPD Priority	Inputs—Number of priority packets received. Drops—Number of priority packets dropped.
Protocol	Name of the protocol for which packet switching information is displayed.
Switching Path	Indicates the traffic switching path.
Pkts In	Number of incoming packets.
Char In	Number of incoming bytes.
Pkts Out	Number of outgoing packets.
Char Out	Number of outgoing bytes.
Process	Process switching. With this type of switching, an incoming packet is associated with a destination network or subnet entry in the routing table located in main memory. Process switching is a scheduled process that is performed by the system processor.
Cache misses	Packets that were forwarded through the process level (for which there was no entry in fast switching cache).
Fast	Fast switching. With this type of switching, an incoming packet matches an entry in the fast-switching cache located in main memory. Fast switching is done via asynchronous interrupts, which are handled in real time. Fast switching allows higher throughput by switching a packet using a cache created by previous packets.
Auton	Autonomous switching. With this type of switching, an incoming packet matches an entry in the autonomous-switching cache located on the interface processor. Autonomous switching provides faster packet switching by allowing the ciscoBus controller to switch packets independently without having to interrupt the system processor. It is available only on Cisco 7000 series routers and in AGS+ systems with high-speed network controller cards.
SSE	Silicon switching engine switching. With this type of switching, an incoming packet matches an entry in the silicon-switching cache located in the silicon switching engine (SSE) of the Silicon Switch Processor (SSP) module. This module is available only on Cisco 7000 series routers. Silicon switching provides very fast, dedicated packet switching by allowing the SSE to switch packets independently without having to interrupt the system processor.

Related Commands

Command	Description
show interface stats	Displays numbers of packets that were process switched, fast switched, and distributed switched.

show ip bgp labels

To display information about Multiprotocol Label Switching (MPLS) labels from the External Border Gateway Protocol (EBGP) route table, use the **show ip bgp labels** command in user EXEC or privileged EXEC mode.

show ip bgp labels

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Use this command to display EBGP labels associated with a carrier supporting carrier customer edge (CSC-CE) router.

This command displays labels for BGP routes in the default table only. To display labels in the VRF tables, use the **show ip bgp vpv4 {all | vrf vrf-name}** command with the optional **labels** keyword.

Examples

The following example shows output for a CSC-CE router using BGP as a label distribution protocol:

```
Router# show ip bgp labels

Network          Next Hop          In Label/Out Label
3.3.0.0/16        0.0.0.0           imp-null/exp-null
15.15.15.15/32   15.15.15.15      18/exp-null
16.16.16.16/32   0.0.0.0           imp-null/exp-null
17.17.17.17/32   34.0.0.1         20/exp-null
18.18.18.18/32   43.0.0.1         24/31
18.18.18.18/32   38.0.0.1         24/33
19.19.19.19/32   43.0.0.1         25/32
19.19.19.19/32   38.0.0.1         25/34
20.20.20.20/32   43.0.0.1         21/30
20.20.20.20/32   38.0.0.1         21/32
33.0.0.0          15.15.15.15      19/exp-null
34.0.0.0          0.0.0.0           imp-null/exp-null
35.0.0.0          43.0.0.1         22/29
35.0.0.0          38.0.0.1         22/31
38.0.0.0          0.0.0.0           imp-null/exp-null
38.0.0.1/32       38.0.0.1         17/29
38.0.0.1/32       0.0.0.0           17/exp-null
40.0.0.0          38.0.0.1         26/35
40.0.0.0          43.0.0.1         26/34
42.0.0.0          43.0.0.1         23/28
```

■ show ip bgp labels

```

42.0.0.0          38.0.0.1          23/30
43.0.0.0          0.0.0.0           imp-null/exp-null
43.0.0.1/32       0.0.0.0           16/exp-null

```

Table 22 describes the significant fields shown in the display.

Table 22 *show ip bgp labels Field Descriptions*

Field	Description
Network	Displays the network address from the EGBP table.
Next Hop	Specifies the EGBP next hop address.
In Label	Displays the label (if any) assigned by this router.
Out Label	Displays the label assigned by the BGP next hop router.

Related Commands

Command	Description
show ip bgp vpnv4	Displays VPN address information from the BGP table.

show ip bgp vpnv4

To display Virtual Private Network (VPN) address information from the Border Gateway Protocol (BGP) table, use the **show ip bgp vpnv4** command in user EXEC or privileged EXEC mode.

```
show ip bgp vpnv4 {all | rd route-distinguisher | vrf vrf-name} [rib-failure] [ip-prefix/length
longer-prefixes] [output-modifiers]] [network-address [mask] [longer-prefixes]
[output-modifiers]] [cidr-only] [community] [community-list] [dampened-paths] [filter-list]
[flap-statistics] [inconsistent-as] [neighbors] [paths [line]] [peer-group] [quote-regexp]
[regexp] [summary] [labels]
```

Syntax	Description
all	Displays the complete VPNv4 database.
rd <i>route-distinguisher</i>	Displays Network Layer Reachability Information (NLRI) prefixes that have a matching route distinguisher.
vrf <i>vrf-name</i>	Displays NLRI prefixes associated with the named VPN routing and forwarding instance (VRF).
rib-failure	(Optional) Displays BGP routes that failed to install in the VRF table.
<i>ip-prefix/length</i>	(Optional) The IP prefix address (in dotted decimal format) and the length of the mask (0 to 32). The slash mark must be included.
longer-prefixes	(Optional) Displays the entry, if any, that exactly matches the specified prefix parameter and all entries that match the prefix in a “longest-match” sense. That is, prefixes for which the specified prefix is an initial substring.
<i>output-modifiers</i>	(Optional) For a list of associated keywords and arguments, use context-sensitive help.
<i>network-address</i>	(Optional) The IP address of a network in the BGP routing table.
<i>mask</i>	(Optional) The mask of the network address, in dotted decimal format.
cidr-only	(Optional) Displays only routes that have nonnatural net masks.
community	(Optional) Displays routes matching this community.
community-list	(Optional) Displays routes matching this community list.
dampened-paths	(Optional) Displays paths suppressed on account of dampening (BGP route from peer is up and down).
filter-list	(Optional) Displays routes conforming to the filter list.
flap-statistics	(Optional) Displays flap statistics of routes.
inconsistent-as	(Optional) Displays only routes that have inconsistent autonomous systems of origin.
neighbors	(Optional) Displays details about TCP and BGP neighbor connections.
paths	(Optional) Displays path information.
<i>line</i>	(Optional) A regular expression to match the BGP autonomous system paths.
peer-group	(Optional) Displays information about peer groups.
quote-regexp	(Optional) Displays routes matching the autonomous system path regular expression.

show ip bgp vpnv4

regex	(Optional) Displays routes matching the autonomous system path regular expression.
summary	(Optional) Displays BGP neighbor status.
labels	(Optional) Displays incoming and outgoing BGP labels for each NLRI prefix.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(2)T	The output of the show ip bgp vpnv4 all ip-prefix command was enhanced to display attributes including multipaths and a best path to the specified network.
12.0(21)ST	The keyword tags was replaced with the keyword labels to conform to the MPLS IETF guidelines. This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	The keyword rib-failure was added for VRFs.

Usage Guidelines

Use this command to display VPNv4 information from the BGP database. The **show ip bgp vpnv4 all** command displays all available VPNv4 information. The **show ip bgp vpnv4 summary** command displays BGP neighbor status.

Examples

The following example shows output for all available VPNv4 information in a BGP routing table:

```
Router# show ip bgp vpnv4 all
```

```
BGP table version is 18, local router ID is 14.14.14.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```

      Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 1:101 (default for vrf vpn1)
*>i6.6.6.6/32         223.0.0.21             11    100      0 ?
*> 7.7.7.7/32         150.150.0.2            11                32768 ?
*>i69.69.0.0/30       223.0.0.21             0     100      0 ?
*> 150.150.0.0/24     0.0.0.0                0                32768 ?
*> 222.0.0.1/32       150.150.0.2            11                32768 ?
*>i222.0.0.3/32       223.0.0.21             11    100      0 ?
*> 222.0.0.10/32     0.0.0.0                0                32768 ?
*>i222.0.0.30/32     223.0.0.21             0     100      0 ?

```

Table 23 describes the significant fields shown in the display.

Table 23 show ip bgp vpnv4 Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the address of the BGP next hop.
Metric	Displays the BGP metric.
LocPrf	Displays the local preference.
Weight	Displays the BGP weight.
Path	Displays the BGP path per route.

The following example shows how to display a table of labels for NLRI prefixes that have a route distinguisher value of 100:1.

```
Router# show ip bgp vpnv4 rd 100:1 labels

Network          Next Hop          In label/Out label
Route Distinguisher: 100:1 (vrf1)
 2.0.0.0          10.20.0.60        34/nolabel
10.0.0.0          10.20.0.60        35/nolabel
12.0.0.0          10.20.0.60        26/nolabel
                  10.20.0.60        26/nolabel
13.0.0.0          10.15.0.15        nolabel/26
```

Table 24 describes the significant fields shown in the display.

Table 24 show ip bgp vpnv4 rd labels Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Specifies the BGP next hop address.
In label	Displays the label (if any) assigned by this router.
Out label	Displays the label assigned by the BGP next hop router.

The following example shows VPNv4 routing entries for the VRF named vpn1:

```
Router# show ip bgp vpnv4 vrf vpn1

BGP table version is 18, local router ID is 14.14.14.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 1:101 (default for vrf vpn1)
*>i6.6.6.6/32     223.0.0.21        11    100    0 ?
*> 7.7.7.7/32     150.150.0.2       11                32768 ?
*>i69.69.0.0/30   223.0.0.21        0     100    0 ?
*> 150.150.0.0/24 0.0.0.0           0                32768 ?
*> 222.0.0.1/32   150.150.0.2       11                32768 ?
*>i222.0.0.3/32   223.0.0.21        11    100    0 ?
```

Table 25 describes the significant fields shown in the display.

Table 25 *show ip bgp vpnv4 vrf Field Descriptions*

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the address of the BGP next hop.
Metric	Displays the BGP metric.
LocPrf	Displays the local preference.
Weight	Displays the BGP weight.
Path	Displays the BGP path per route.

The following example shows attributes for network 10.22.22.0 that includes multipaths and a best path:

```
Router# show ip bgp vpnv4 all 10.22.22.0

BGP routing table entry for 100:1:10.22.22.0/24, version 50
Paths: (6 available, best #1)
Multipath:iBGP
  Advertised to non peer-group peers:
  200.1.12.12
  22
    1.22.7.8 (metric 11) from 1.11.3.4 (100.0.0.8)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath, best
      Extended Community:RT:100:1
      Originator:100.0.0.8, Cluster list:100.1.1.44
  22
    1.22.1.9 (metric 11) from 1.11.1.2 (100.0.0.9)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath
      Extended Community:RT:100:1
      Originator:100.0.0.9, Cluster list:100.1.1.22
  22
    1.22.6.10 (metric 11) from 1.11.6.7 (100.0.0.10)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath
      Extended Community:RT:100:1
      Originator:100.0.0.10, Cluster list:100.0.0.7
  22
    1.22.4.10 (metric 11) from 1.11.4.5 (100.0.0.10)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath
      Extended Community:RT:100:1
      Originator:100.0.0.10, Cluster list:100.0.0.5
  22
    1.22.5.10 (metric 11) from 1.11.5.6 (100.0.0.10)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath
      Extended Community:RT:100:1
      Originator:100.0.0.10, Cluster list:100.0.0.6
```

Table 26 describes the significant fields shown in the display.

Table 26 show ip bgp vpnv4 all 10.22.22.0 Field Descriptions

Field	Description
BGP routing table ... version	Internal version number of the table. This number is incremented whenever the table changes.
Paths:	Number of autonomous system paths to the specified network. If multiple paths exist, one of the multipaths is designated the best path.
Multipath:	Indicates the maximum paths configured (iBGP or eBGP).
Advertised to non peer-group peers: 200.1.12.12 22	IP address of the BGP peers that the specified route is advertised to.
1.22.7.8 (metric 11) from 1.11.3.4 (100.0.0.8)	Indicates the next hop address and the address of the gateway that sent the update.
Origin	Indicates the origin of the entry. It can be one of the following values: IGP—Entry originated from Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. incomplete—Entry originated from other than an IGP or Exterior Gateway Protocol (EGP) and was advertised with the redistribute router configuration command. EGP—Entry originated from an EGP.
metric	If shown, the value of the interautonomous system metric.
localpref	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
valid	Indicates that the route is usable and has a valid set of attributes.
internal/external	The field is <i>internal</i> if the path is learned via iBGP. The field is <i>external</i> if the path is learned via eBGP.
multipath	One of multiple paths to the specified network.
best	If multiple paths exist, one of the multipaths is designated the best path and advertised the neighbors.
Extended Community:RT:100:1	Route Target value associated with the specified route.
Originator:	The router ID of the route originating router when route reflector is used.
Cluster list:	The router ID of all the route reflectors that the specified route has passed through.

The following example shows routes that BGP could not install in the VRF table:

```
Router# show ip bgp vpnv4 vrf foo rib-failure
```

```
Network          Next Hop          RIB-failure    RIB-NH Matches
Route Distinguisher: 2:2 (default for vrf bar)
10.1.1.2/32      100.100.100.100  Higher admin distance    No
111.111.111.112/32 9.9.9.9          Higher admin distance    Yes
```

Table 27 describes the significant fields shown in the display.

Table 27 *show ip bgp Field Descriptions*

Field	Description
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
RIB-failure	Cause of RIB failure. Higher admin distance means that a route with a better (lower) administrative distance such as a static route already exists in the IP routing table.
RIB-NH Matches	Route status that applies only when Higher admin distance appears in the RIB-failure column and bgp suppress-inactive is configured for the address family being used. There are three choices: <ul style="list-style-type: none"> • Yes—Means that the route in the RIB has the same nexthop as the BGP route or nexthop recurses down to the same adjacency as the BGP nexthop. • No—Means that the nexthop in the RIB recurses down differently from the nexthop of the BGP route. • n/a—Means that bgp suppress-inactive is not configured for the address family being used.

Related Commands

Command	Description
show ip bgp rib-failure	Displays BGP routes that failed to install in the RIB table.
show ip vrf	Displays the set of defined VRFs and associated interfaces.

show ip cache

To display the routing table cache used to fast switch IP traffic, use the **show ip cache** command in user EXEC or privileged EXEC mode.

```
show ip cache [prefix mask] [type number]
```

Syntax Description	prefix	(Optional) Displays only the entries in the cache that match the prefix and mask combination.
	mask	(Optional) Displays only the entries in the cache that match the prefix and mask combination.
	type	(Optional) Displays only the entries in the cache that match the interface type and number combination.
	number	(Optional) Displays only the entries in the cache that match the interface type and number combination.

Command Modes	User EXEC Privileged EXEC
---------------	------------------------------

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines The **show ip cache** display shows MAC headers up to 92 bytes.

Examples The following is sample output from the **show ip cache** command:

```
Router# show ip cache

IP routing cache version 4490, 141 entries, 20772 bytes, 0 hash overflows
Minimum invalidation interval 2 seconds, maximum interval 5 seconds,
  quiet interval 3 seconds, threshold 0 requests
Invalidation rate 0 in last 7 seconds, 0 in last 3 seconds
Last full cache invalidation occurred 0:06:31 ago

Prefix/Length      Age      Interface      MAC Header
131.108.1.1/32     0:01:09  Ethernet0/0    AA000400013400000C0357430800
131.108.1.7/32     0:04:32  Ethernet0/0    00000C01281200000C0357430800
131.108.1.12/32    0:02:53  Ethernet0/0    00000C029FD000000C0357430800
131.108.2.13/32    0:06:22  Fddi2/0        00000C05A3E000000C035753AAAA0300
                   00000800
131.108.2.160/32   0:06:12  Fddi2/0        00000C05A3E000000C035753AAAA0300
                   00000800
131.108.3.0/24     0:00:21  Ethernet1/2    00000C026BC600000C03574D0800
131.108.4.0/24     0:02:00  Ethernet1/2    00000C026BC600000C03574D0800
131.108.5.0/24     0:00:00  Ethernet1/2    00000C04520800000C03574D0800
131.108.10.15/32   0:05:17  Ethernet0/2    00000C025FF500000C0357450800
```

```

131.108.11.7/32      0:04:08  Ethernet1/2      00000C010E3A00000C03574D0800
131.108.11.12/32   0:05:10  Ethernet0/0      00000C01281200000C0357430800
131.108.11.57/32   0:06:29  Ethernet0/0      00000C01281200000C0357430800

```

Table 28 describes the significant fields shown in the display.

Table 28 show ip cache Field Descriptions

Field	Description
IP routing cache version	Version number of this table. This number is incremented any time the table is flushed.
entries	Number of valid entries.
bytes	Number of bytes of processor memory for valid entries.
hash overflows	Number of times autonomous switching cache overflowed.
Minimum invalidation interval	Minimum time delay between cache invalidation request and actual invalidation.
maximum interval	Maximum time delay between cache invalidation request and actual invalidation.
quiet interval	Length of time between cache flush requests before the cache will be flushed.
threshold <n> requests	Maximum number of requests that can occur while the cache is considered quiet.
Invalidation rate <n> in last <m> seconds	Number of cache invalidations during the last <m> seconds.
0 in last 3 seconds	Number of cache invalidation requests during the last quiet interval.
Last full cache invalidation occurred <hh:mm:ss> ago	Time since last full cache invalidation was performed.
Prefix/Length	Network reachability information for cache entry.
Age	Age of cache entry.
Interface	Output interface type and number.
MAC Header	Layer 2 encapsulation information for cache entry.

The following is sample output from the **show ip cache** command with a prefix and mask specified:

```

Router# show ip cache 131.108.5.0 255.255.255.0

IP routing cache version 4490, 119 entries, 17464 bytes, 0 hash overflows
Minimum invalidation interval 2 seconds, maximum interval 5 seconds,
  quiet interval 3 seconds, threshold 0 requests
Invalidation rate 0 in last second, 0 in last 3 seconds
Last full cache invalidation occurred 0:11:56 ago

Prefix/Length      Age      Interface      MAC Header
131.108.5.0/24     0:00:34  Ethernet1/2    00000C04520800000C03574D0800

```

The following is sample output from the **show ip cache** command with an interface specified:

```
Router# show ip cache e0/2
```

```
IP routing cache version 4490, 141 entries, 20772 bytes, 0 hash overflows  
Minimum invalidation interval 2 seconds, maximum interval 5 seconds,  
  quiet interval 3 seconds, threshold 0 requests  
Invalidation rate 0 in last second, 0 in last 3 seconds  
Last full cache invalidation occurred 0:06:31 ago
```

Prefix/Length	Age	Interface	MAC Header
131.108.10.15/32	0:05:17	Ethernet0/2	00000C025FF500000C0357450800

show ip cache flow

To display a summary of NetFlow statistics, use the **show ip cache flow** command in user EXEC or privileged EXEC mode.

show ip cache [*prefix mask*] [*type number*] **flow**

Syntax Description		
<i>prefix mask</i>	(Optional)	Displays only the entries in the cache that match the prefix and mask combination.
<i>type number</i>	(Optional)	Displays only the entries in the cache that match the interface type and number combination.

Command Modes	
	User EXEC Privileged EXEC

Command History	Release	Modification
	11.1	This command was introduced.
	11.1 CA	The information display for the command was updated.
	12.3(4)T, 12.3(6), 12.2(20)S	The execute-on command was implemented on the Cisco 7500 platform to include the remote execution of the show ip cache flow command.

Usage Guidelines

Some of the content in the display of the **show ip cache flow** command uses multiline headings and multiline data fields. [Figure 1](#) uses an example of the output from the **show ip cache verbose flow** to show how to associate the headings with the correct data fields when there are two or more lines of headings and two or more lines of data fields. The first line of the headings is associated with the first line of data fields. The second line of the headings is associated with the second line of data fields, and so on.

When other features such as IP Multicast are configured, the number of lines in the headings and data fields increases. The method for associating the headings with the correct data fields remains the same.

Figure 1 How to Use the Multiline Headings and Multiline Data Fields in the Display Output of the `show ip cache verbose flow` Command

```

Router# show ip cache verbose flow
IP packet size distribution (25229 total packets):
 1-32  64  96 128 160 192 224 256 288 320 352 384 416 448 480
 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
 512 544 576 1024 1536 2048 2560 3072 3584 4096 4608
 .000 .000 .000 .206 .793 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
 6 active, 4090 inactive, 17 added
 505 ager polls, 0 flow alloc failures
 Active flows timeout in 1 minutes
 Inactive flows timeout in 10 seconds
IP Sub Flow Cache, 25736 bytes
 12 active, 1012 inactive, 39 added, 17 added to flow
 0 alloc failures, 0 force free
 1 chunk, 1 chunk added
 last clearing of statistics never

Protocol      Total      Flows      Packets Bytes  Packets Active(Sec) Idle(Sec)
-----      -
Flows        /Sec      /Flow /Pkt  /Sec  /Flow  /Flow
TCP-Telnet    1         0.0       362  940   2.7   60.2   0.0
TCP-FTP       1         0.0       362  840   2.7   60.2   0.0
TCP-FTPD     1         0.0       362  840   2.7   60.1   0.1
TCP-SMTP     1         0.0       361 1040   2.7   60.0   0.1
UDP-other    5         0.0        1   66    0.0    1.0  10.6
ICMP         2         0.0      8829 1378  135.8  60.7   0.0
Total:       11        0.0      1737 1343  147.0  33.4   4.8

SrcIf          SrcIPAddress  DstIf          DstIPAddress  Pr  TOS  Flgs  Pkts
Port Msk AS    Port Msk AS   NextHop       E/Pk Active
Et0/0.1       10.251.138.2 Et1/0.1       172.16.10.2   06 80 00    65
0015 /0 0      0015 /0 0     0.0.0.0       840 10.8
MAC: (VLAN id) aaaa.bbbb.cc03 (0005)  aaaa.bbbb.cc06 (0006)
Min plen:      840
Min TTL:       59
IP id:         0

```

Displaying Detailed NetFlow Cache Information on Platforms Running Distributed Cisco Express Forwarding

On platforms running Distributed Cisco Express Forwarding (dCEF), NetFlow cache information is maintained on each line card or Versatile Interface Processor. To display this information on a distributed platform by use of the `show ip cache flow` command, you must enter the command at a line card prompt.

Cisco 7500 Series Platform

To display NetFlow cache information using the `show ip cache flow` command on a Cisco 7500 series router that is running dCEF, enter the following sequence of commands:

```

Router# if-con slot-number
LC-slot-number# show ip cache [prefix mask] [type number] [verbose] flow

```

For Cisco IOS Releases 12.3(4)T, 12.3(6), and 12.2(20)S and later, enter the following command to display NetFlow cache information:

```

Router# execute-on slot-number show ip cache [prefix mask] [type number] [verbose] flow

```

Cisco 12000 Series Platform

To display NetFlow cache information using the `show ip cache flow` command on a Cisco 12000 Series Internet router, you enter the following sequence of commands:

```

Router# attach slot-number
LC-slot-number# show ip cache [prefix mask] [type number] [verbose] flow

```

For Cisco IOS Releases 12.3(4)T, 12.3(6), and 12.2(20)S and later, enter the following command to display NetFlow cache information:

```
Router# execute-on slot-number show ip cache [prefix mask] [type number] [verbose] flow
```

Examples

The following is an sample display of a main cache using the **show ip cache flow** command:

```
Router# show ip cache flow
IP packet size distribution (2381 total packets):
  1-32  64  96 128 160 192 224 256 288 320 352 384 416 448 480
  .092 .000 .003 .000 .141 .048 .000 .000 .000 .093 .000 .000 .000 .000 .000

      512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
      .000 .000 .048 .189 .381 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  22 active, 4074 inactive, 45 added
  2270 ager polls, 0 flow alloc failures
  Active flows timeout in 1 minutes
  Inactive flows timeout in 100 seconds
IP Sub Flow Cache, 25736 bytes
  23 active, 1001 inactive, 47 added, 45 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
```

Protocol	Total	Flows	Packets	Bytes	Packets	Active(Sec)	Idle(Sec)
-----	Flows	/Sec	/Flow	/Pkt	/Sec	/Flow	/Flow
TCP-FTP	4	0.0	67	840	2.6	59.4	0.7
TCP-SMTP	1	0.0	67	168	0.6	59.4	0.5
TCP-BGP	1	0.0	68	1140	0.6	60.3	0.4
TCP-NNTP	1	0.0	68	1340	0.6	60.2	0.2
TCP-other	7	0.0	68	913	4.7	60.3	0.4
UDP-TFTP	1	0.0	68	156	0.6	60.2	0.1
UDP-other	4	0.0	36	151	1.4	45.6	14.7
ICMP	4	0.0	67	529	2.7	60.0	0.2
Total:	23	0.2	62	710	14.3	57.5	2.9

```

SrcIf      SrcIPAddress  DstIf      DstIPAddress Pr SrcP DstP  Pkts
Et2/0     192.168.137.78 Et3/0*     192.168.10.67 06 0041 0041  39
Et2/0     172.19.216.196 Et3/0*     192.168.10.38 06 0077 0077  39
Et0/0.1   10.56.78.128   Et1/0.1    172.16.30.231 06 00B3 00B3  48
Et0/0.1   10.10.18.1     Et1/0.1    172.16.30.112 11 0043 0043  47
Et0/0.1   10.162.37.71   Et1/0.1    172.16.30.218 06 027C 027C  48
Et0/0.1   172.16.6.1     Null       224.0.0.9     11 0208 0208  1
Et0/0.1   10.231.159.251 Et1/0.1    172.16.10.2   06 00DC 00DC  48
Et2/0     10.234.53.1    Et3/0*     192.168.10.32 06 0016 0015  39
Et2/0     10.210.211.213 Et3/0*     192.168.10.127 06 006E 006E  38
Et0/0.1   10.234.53.1    Et1/0.1    172.16.30.222 01 0000 0000  47
Et0/0.1   10.90.34.193   Et1/0.1    172.16.10.2   06 0016 0015  48
Et0/0.1   10.10.10.2     Et1/0.1    172.16.10.2   06 0016 0015  48
Et2/0     10.10.18.1     Et3/0*     192.168.10.162 11 0045 0045  39
Et0/0.1   192.168.3.185  Et1/0.1    172.16.10.2   06 0089 0089  48
Et0/0.1   10.10.11.1     Et1/0.1    172.16.30.51  06 0019 0019  49
Et0/0.1   10.254.254.235 Et1/0.1    172.16.10.2   11 00A1 00A1  48
Et2/0     192.168.23.2   Et3/0*     192.168.10.2   01 0000 0000  39
Et0/0.1   10.251.10.1    Et1/0.1    172.16.10.2   01 0000 0800  47
R3#
```

Table 29 describes the significant fields shown in the flow switching cache lines of the display.

Table 29 *show ip cache flow Field Descriptions in Flow Switching Cache Display*

Field	Description
bytes	Number of bytes of memory used by the NetFlow cache.
active	Number of active flows in the NetFlow cache at the time this command was entered.
inactive	Number of flow buffers that are allocated in the NetFlow cache, but are not currently assigned to a specific flow at the time this command is entered.
added	Number of flows created since the start of the summary period.
ager polls	Number of times the NetFlow code looked at the cache to cause entries to expire (used by Cisco for diagnostics only).
flow alloc failures	Number of times the NetFlow code tried to allocate a flow but could not.
Exporting flows	IP address and User Datagram Protocol (UDP) port number of the workstation to which flows are exported.
flows exported in udp datagrams	Total number of flows exported and the total number of UDP datagrams used to export the flows to the workstation.
failed	Number of flows that could not be exported by the router because of output interface limitations.
last clearing of statistics	Standard time output (hh:mm:ss) since the clear ip flow stats privileged EXEC command was executed. This time output changes to hours and days after the time exceeds 24 hours.

Table 30 describes the significant fields shown in the activity by protocol lines of the display.

Table 30 *show ip cache flow Field Descriptions in Activity By Protocol Display*

Field	Description
Protocol	IP protocol and the “well known” port number as described in RFC 1340.
Total Flows	Number of flows for this protocol since the last time statistics were cleared.
Flows/Sec	Average number of flows for this protocol seen per second; equal to total flows/number of seconds for this summary period.
Packets/Flow	Average number of packets observed for the flows seen for this protocol. Equal to total packets for this protocol or number of flows for this protocol for this summary period.
Bytes/Pkt	Average number of bytes observed for the packets seen for this protocol (total bytes for this protocol or the total number of packet for this protocol for this summary period).
Packets/Sec	Average number of packets for this protocol per second (total packets for this protocol) or the total number of seconds for this summary period.

Table 30 show ip cache flow Field Descriptions in Activity By Protocol Display (continued)

Field	Description
Active(Sec)/Flow	Sum of all the seconds from the first packet to the last packet of an expired flow (for example, TCP FIN, timeout, and so on) in seconds or total flows for this protocol for this summary period.
Idle(Sec)/Flow	Sum of all the seconds from the last packet seen in each nonexpired flow for this protocol until the time at which this command was entered, in seconds or total flows for this protocol for this summary period.

Table 31 describes the significant fields in the NetFlow record lines of the displays:

Table 31 show ip cache flow Field Descriptions in NetFlow Record Display

Field	Description
SrcIf	Interface on which the packet was received.
SrcIPAddress	IP address of the device which transmitted the packet.
DstIf	Interface from which the packet was transmitted.
DstIPAddress	IP address of the destination device.
Pr	IP protocol “well-known” port number as described in RFC 1340, displayed in hexadecimal format.
SrcP	IP port from which the packet is transmitted, displayed in hexadecimal format.
DstP	IP port where the packet is to be delivered, displayed in hexadecimal format.
Pkts	Number of packets switched through this flow.

Table 32 describes the significant fields in the NetFlow record lines of the display.

Table 32 show ip cache verbose flow Field Descriptions in NetFlow Record Display

Field	Description
SrcIf	Interface on which the packet was received.
Port Msk AS	Source Border Gateway Protocol (BGP) autonomous system. This is always set to 0 in MPLS flows.
SrcIPAddress	IP address of the device which transmitted the packet.
DstIf	Interface from which the packet was transmitted.
Port Msk AS	Destination BGP autonomous system. This is always set to 0 in MPLS flows.
DstIPAddress	IP address of the destination device.
NextHop	Specifies the BGP next hop address. This is always set to 0 in MPLS flows.
Pr	IP protocol well-known port number as described in RFC 1340, displayed in hexadecimal format.
B/Pk	Average number of bytes observed for the packets seen for this protocol (total bytes for this protocol or the total number of flows for this protocol for this summary period).
Flgs	TCP flags (result of bitwise OR of TCP flags from all packets in the flow).

Table 32 *show ip cache verbose flow Field Descriptions in NetFlow Record Display (continued)*

Field	Description
Active	The time in seconds that this flow has been active at the time this command was entered.
Pkts	Number of packets switched through this flow.

Related Commands

Command	Description
clear ip flow stats	Clears the NetFlow statistics.
ip route-cache	Controls the use of high-speed switching caches for IP routing.
tunnel flow egress-records	Creates a NetFlow record for packets that are encapsulated by the GRE tunnel.

show ip cache flow aggregation

To display the aggregation cache configuration, use the **show ip cache flow aggregation** command in user EXEC or privileged EXEC mode.

```
show ip cache [prefix mask] [type number] [verbose] flow aggregation {as | as-tos |
bgp-nexthop-tos | destination-prefix | destination-prefix-tos | prefix | prefix-port |
prefix-tos | protocol-port | protocol-port-tos | source-prefix | source-prefix-tos}
```

Syntax Description		
<i>prefix mask</i>	(Optional)	Displays only the entries in the cache that match the prefix and mask combination.
<i>type number</i>	(Optional)	Displays only the entries in the cache that match the interface type and number combination.
verbose	(Optional)	Displays additional information from the aggregation cache.
as		Displays the configuration of the autonomous system aggregation cache scheme.
as-tos		Displays the configuration of the autonomous system type of service (ToS) aggregation cache scheme.
bgp-nexthop-tos		Displays the BGP next hop and ToS aggregation cache scheme.
destination-prefix		Displays the configuration of the destination prefix aggregation cache scheme.
destination-prefix-tos		Displays the configuration of the destination prefix ToS aggregation cache scheme.
prefix		Displays the configuration of the prefix aggregation cache scheme.
prefix-port		Displays the configuration of the prefix port aggregation cache scheme.
prefix-tos		Displays the configuration of the prefix ToS aggregation cache scheme.
protocol-port		Displays the configuration of the protocol port aggregation cache scheme.
protocol-port-tos		Displays the configuration of the protocol port ToS aggregation cache scheme.
source-prefix		Displays the configuration of the source prefix aggregation cache scheme.
source-prefix-tos		Displays the configuration of the source prefix ToS aggregation cache scheme.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.0(15)S	This command was modified to include new show output for ToS aggregation schemes.
12.2(4)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(1)	The bgp-nexthop-tos keyword was added.

Usage Guidelines

Some of the content in the display of the **show ip cache flow aggregation** command uses multiline headings and multiline data fields. [Figure 2](#) uses an example of the output from the **show ip cache verbose flow** to show how to associate the headings with the correct data fields when there are two or more lines of headings and two or more lines of data fields. The first line of the headings is associated with the first line of data fields. The second line of the headings is associated with the second line of data fields, and so on.

When other features such as IP Multicast are configured, the number of lines in the headings and data fields increases. The method for associating the headings with the correct data fields remains the same.

Figure 2 How to Use the Multiline Headings and Multiline Data Fields in the Display Output of the **show ip cache verbose flow** Command

```

Router# show ip cache verbose flow
IP packet size distribution (25229 total packets):
  1-32  64  96 128 160 192 224 256 288 320 352 384 416 448 480
  .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
  512 544 576 1024 1536 2048 2560 3072 3584 4096 4608
  .000 .000 .000 .206 .793 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  6 active, 4090 inactive, 17 added
  505 ager polls, 0 flow alloc failures
  Active flows timeout in 1 minutes
  Inactive flows timeout in 10 seconds
IP Sub Flow Cache, 25736 bytes
  12 active, 1012 inactive, 39 added, 17 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never

Protocol      Total    Flows    Packets Bytes  Packets Active(Sec) Idle(Sec)
-----      -
Flows        /Sec    /Flow  /Pkt  /Sec  /Flow  /Flow
TCP-Telnet    1      0.0      362   940    2.7    60.2    0.0
TCP-FTP       1      0.0      362   840    2.7    60.2    0.0
TCP-FTPD      1      0.0      362   840    2.7    60.1    0.1
TCP-SMTP      1      0.0      361  1040    2.7    60.0    0.1
UDP-other     5      0.0      1     66     0.0    1.0    10.6
ICMP          2      0.0      8829 1378   135.8   60.7    0.0
Total:        11     0.0      1737 1343   147.0   33.4    4.8

  SrcIf          SrcIPaddress  DstIf          DstIPaddress  Pr TOS Flgs Pkts
  Port Msk AS    Port Msk AS    NextHop        E/Pk Active
  Et0/0.1        10.251.138.2  Et1/0.1        172.16.10.2   06 80 00    65
  0015 /0 0      0015 /0 0      0.0.0.0        840    10.8
  MAC: (VLAN id) aaaa.bbbb.cc03 (005)
  Max plen:      840
  Min TTL:       59
  IP id:         0
  aaaa.bbbb.cc06 (006)
  Max plen:      840
  Min TTL:       59
  127034

```

Examples

The following is a sample display of an autonomous system aggregation cache using the **show ip cache flow aggregation** as command:

show ip cache flow aggregation

```
Router# show ip cache flow aggregation as
```

```
IP Flow Switching Cache, 278544 bytes
 2 active, 4094 inactive, 13 added
 178 ager polls, 0 flow alloc failures
```

Src If	Src AS	Dst If	Dst AS	Flows	Pkts	B/Pk	Active
Fa1/0	0	Null	0	1	2	49	10.2
Fa1/0	0	Se2/0	20	1	5	100	0.0

The following is a sample display of an autonomous system aggregation cache for the prefix mask 10.0.0.1 255.0.0.0 using the **show ip cache flow aggregation as** command:

```
Router# show ip cache 10.0.0.1 255.0.0.0 flow aggregation as
```

```
IP Flow Switching Cache, 278544 bytes
 2 active, 4094 inactive, 13 added
 178 ager polls, 0 flow alloc failures
```

Src If	Src AS	Dst If	Dst AS	Flows	Pkts	B/Pk	Active
e1/2	0	Null	0	1	2	49	10.2
e1/2	0	e1/2	20	1	5	100	0.0

The following is a sample display of an autonomous system aggregation cache for 10.0.0.1 255.0.0.0 Ethernet1/2 using the **show ip cache verbose flow aggregation as** command:

```
Router# show ip cache 10.0.0.1 255.0.0.0 e1/2 verbose flow aggregation as
```

```
IP Flow Switching Cache, 278544 bytes
 2 active, 4094 inactive, 13 added
 178 ager polls, 0 flow alloc failures
```

Src If	Src AS	Dst If	Dst AS	Flows	Pkts	B/Pk	Active
e1/2	0	Null	0	1	2	49	10.2
e1/2	0	e1/2	20	1	5	100	0.0

The following is a sample display of an autonomous system ToS aggregation cache using the **show ip cache verbose flow aggregation as-tos** command:

```
Router# show ip cache verbose flow aggregation as-tos
```

```
IP Flow Switching Cache, 278544 bytes
 4 active, 4092 inactive, 103 added
 1609 ager polls, 0 flow alloc failures
```

Src If	Src AS	Dst If	Dst AS	TOS	Flows	Pkts	B/Pk	Active
Et1/2	50	Fd4/0	40	CC	1	3568	28	17.8
Et1/2	0	Fd4/0	40	C0	15	17K	28	17.8
Et1/1	50	Fd4/0	40	55	1	3748	28	17.8
Fd4/0	0	Null	0	C0	1	2	49	0.9

The following is a sample display of a protocol port ToS aggregation cache using the **show ip cache verbose flow aggregation protocol-port-tos** command:

```
Router# show ip cache verbose flow aggregation protocol-port-tos
```

```
IP Flow Switching Cache, 278544 bytes
 4 active, 4092 inactive, 102 added
 1584 ager polls, 0 flow alloc failures
```

Prot	Src If	SrcPort	Dst If	DstPort	TOS	Flows	Pkts	B/Pk	Active
0x01	Et1/2	0000	Fd4/0	0000	C0	15	17K	28	17.8
0x01	Et1/2	0000	Fd4/0	0000	CC	1	3568	28	17.8
0x01	Et1/1	0000	Fd4/0	0000	55	1	3748	28	17.8

```
0x06 Fd4/0          00B3 Null          2AF9 C0      1      2      49      0.9
```

The following is a sample display of a source prefix ToS aggregation cache using the **show ip cache verbose flow aggregation source-prefix-tos** command:

```
Router# show ip cache verbose flow aggregation source-prefix-tos
```

```
IP Flow Switching Cache, 278544 bytes
 4 active, 4092 inactive, 105 added
1683 ager polls, 0 flow alloc failures
```

Src If	Src Prefix	MsK	AS	TOS	Flows	Pkts	B/Pk	Active
Et1/1	52.0.0.0	/8	50	55	1	3748	28	17.8
Et1/2	52.0.0.0	/8	50	CC	1	3568	28	17.8
Et1/2	0.0.0.0	/0	0	C0	15	17K	28	17.8
Fd4/0	20.20.20.1	/32	0	C0	1	2	49	0.9

The following is a sample display of a destination prefix ToS aggregation cache using the **show ip cache verbose flow aggregation destination-prefix-tos** command:

```
Router# show ip cache verbose flow aggregation destination-prefix-tos
```

```
IP Flow Switching Cache, 278544 bytes
 4 active, 4092 inactive, 86 added
1480 ager polls, 0 flow alloc failures
```

Dst If	Dst Prefix	MsK	AS	TOS	Flows	Pkts	B/Pk	Active
Local	31.31.31.1	/32	0	C0	1	2	49	0.9
Fd4/0	42.0.0.0	/8	40	55	1	3748	28	17.8
Fd4/0	42.0.0.0	/8	40	CC	1	3568	28	17.8
Fd4/0	42.0.0.0	/8	40	C0	15	17K	28	17.8

The following is a sample display of a prefix ToS aggregation cache using the **show ip cache verbose flow aggregation prefix-tos** command:

```
Router# show ip cache verbose flow aggregation prefix-tos
```

```
IP Flow Switching Cache, 278544 bytes
 4 active, 4092 inactive, 4 added
14 ager polls, 0 flow alloc failures
```

Src If	Src Prefix	Dst If	Dst Prefix	TOS	Flows	Pkts
	MsK AS		MsK AS		B/Pk	Active
Et1/2	0.0.0.0	Fd4/0	42.0.0.0	C0	15	3933
	/0 0		/8 40		28	3.9
Et1/1	52.0.0.0	Fd4/0	42.0.0.0	55	1	826
	/8 50		/8 40		28	3.9
Et1/2	52.0.0.0	Fd4/0	42.0.0.0	CC	1	787
	/8 50		/8 40		28	3.9

The following is a sample display of a prefix port aggregation cache using the **show ip cache verbose flow aggregation prefix-port** command:

show ip cache flow aggregation

```
Router# show ip cache verbose flow aggregation prefix-port
```

```
IP Flow Switching Cache, 278544 bytes
 4 active, 4092 inactive, 105 added
1679 ager polls, 0 flow alloc failures
```

Src If	Src Prefix Port Msk	Dst If	Dst Prefix Port Msk	TOS	Flows Pr B/Pk	Pkts Active
Fd4/0	20.20.20.1 00B3 /32	Local	31.31.31.1 2AF9 /32	C0	1 06 49	2 0.9
Et1/2	0.0.0.0 0000 /0	Fd4/0	42.0.0.0 0000 /8	C0	15 01 28	17K 17.8
Et1/1	52.0.0.0 0000 /8	Fd4/0	42.0.0.0 0000 /8	55	1 01 28	3748 17.8
Et1/2	52.0.0.0 0000 /8	Fd4/0	42.0.0.0 0000 /8	CC	1 01 28	3568 17.8

Table 33 describes the significant fields shown in these examples.

Table 33 show ip cache verbose flow aggregation Field Descriptions

Field	Description
bytes	Number of bytes of memory used by the NetFlow cache.
active	Number of active flows in the NetFlow cache at the time this command was entered.
inactive	Number of flow buffers that are allocated in the NetFlow cache, but are not currently assigned to a specific flow at the time this command is entered.
added	Number of flows created since the start of the summary period.
ager polls	Number of times the NetFlow code looked at the cache to cause entries to expire (used by Cisco for diagnostics only).
flow alloc failures	Number of times the NetFlow code tried to allocate a flow but could not.
Src If	Specifies the source interface.
Src AS	Specifies the source autonomous system.
Dst If	Specifies the destination interface.
Dst AS	Specifies the destination autonomous system.
Flows	Number of flows.
Pkts	Number of packets.
B/Pk	Average number of bytes observed for the packets seen for this protocol (total bytes for this protocol or the total number of flows for this protocol for this summary period).
Active	The time in seconds that this flow has been active at the time this command was entered.

Related Commands

Command	Description
ip flow-aggregation cache	Enables aggregation cache configuration mode.

show ip cache verbose flow

To displays a detailed summary of the NetFlow accounting statistics, use the **show ip cache verbose flow** command in user EXEC or privileged EXEC mode.

show ip cache [*prefix mask*] [*type number*] **verbose flow**

Syntax Description		
	<i>prefix mask</i>	(Optional) Displays only the entries in the cache that match the prefix and mask combination.
	<i>type number</i>	(Optional) Displays only the entries in the cache that match the interface type and number combination.

Command Modes	
	User EXEC Privileged EXEC

Command History	Release	Modification
	11.1	This command was introduced.
	11.1 CA	The information display for the command was updated.
	12.3(1)	The command output was updated to display additional NetFlow fields.
	12.3(4)T, 12.3(6), 12.2(20)S	The execute-on command was implemented on the Cisco 7500 platforms to include the remote execution of the show ip cache verbose flow command.

Usage Guidelines

Some of the content in the display of the **show ip cache verbose flow** command uses multiline headings and multiline data fields. [Figure 3](#) uses an example of the output from the **show ip cache verbose flow** to show how to associate the headings with the correct data fields when there are two or more lines of headings and two or more lines of data fields. The first line of the headings is associated with the first line of data fields. The second line of the headings is associated with the second line of data fields, and so on.

When other features such as IP Multicast are configured, the number of lines in the headings and data fields increases. The method for associating the headings with the correct data fields remains the same.

Figure 3 How to Use the Multiline Headings and Multiline Data Fields in the Display Output of the `show ip cache verbose flow` Command

```

Router# show ip cache verbose flow
IP packet size distribution (25229 total packets):
 1-32  64  96 128 160 192 224 256 288 320 352 384 416 448 480
 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
 512 544 576 1024 1536 2048 2560 3072 3584 4096 4608
 .000 .000 .000 .206 .793 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
 6 active, 4090 inactive, 17 added
 505 ager polls, 0 flow alloc failures
 Active flows timeout in 1 minutes
 Inactive flows timeout in 10 seconds
IP Sub Flow Cache, 25736 bytes
 12 active, 1012 inactive, 39 added, 17 added to flow
 0 alloc failures, 0 force free
 1 chunk, 1 chunk added
 last clearing of statistics never

Protocol      Total      Flows      Packets Bytes  Packets Active(Sec) Idle(Sec)
-----      -
              Flows      /Sec      /Flow /Pkt  /Sec  /Flow  /Flow
TCP-Telnet    1          0.0        362  940   2.7   60.2   0.0
TCP-FTP       1          0.0        362  840   2.7   60.2   0.0
TCP-FTPD      1          0.0        362  840   2.7   60.1   0.1
TCP-SMTP      1          0.0        361 1040   2.7   60.0   0.1
UDP-other     5          0.0         1   66    0.0    1.0  10.6
ICMP          2          0.0       8829 1378  135.8  60.7   0.0
Total:        11         0.0       1737 1343  147.0  33.4   4.8

SrcIf      SrcIPaddress  DstIf      DstIPaddress  Pr  TOS  Flgs  Pkts
Port Msk AS  Port Msk AS  NextHop      E/Pk Active
Et0/0.1    10.251.138.2 Et1/0.1     172.16.10.2  06  80  00    65
0015 /0 0    0015 /0 0    0.0.0.0      840  10.8
MAC: (VLAN id) aaaa.bbbb.cc03 (005)  aaaa.bbbb.cc06 (006)
Min plen:      840
Min TTL:       59
IP id:         0
Max plen:      840
Max TTL:       59

```

Use the `show ip cache verbose flow` command to display flow record fields in the NetFlow cache in addition to the fields that are displayed with the `show ip cache flow` command. The values in the additional fields that are shown depend on the NetFlow features that are enabled and the flags that are set in the flow.



Note

The flags, and therefore the fields, might vary from flow to flow.

When the NetFlow Multicast Support feature is enabled, this command displays the number of replicated packets and the packet byte count for NetFlow multicast accounting. When you configure the NetFlow Version 9 Export Format feature, this command displays additional NetFlow fields in the header.

Displaying Detailed NetFlow Cache Information on a Distributed Cisco 7500 Series Platform

To display detailed NetFlow cache information on a Cisco 7500 series router that is running distributed Cisco Express Forwarding (dCEF), enter the following sequence of commands:

```

Router# if-con slot-number
LC-slot-number# show ip cache verbose flow

```

For Cisco IOS Releases 12.3(4)T, 12.3(6), and 12.2(20)S and later, enter the following command to display detailed NetFlow cache information:

```

Router# execute-on slot-number show ip cache verbose flow

```

Displaying Detailed NetFlow Cache Information on a Distributed Cisco 12000 Series Platform

To display detailed NetFlow cache information on a Cisco 12000 series Internet router, you enter the following sequence of commands:

```
Router# attach slot-number
LC-slot-number# show ip cache verbose flow
```

For Cisco IOS Releases 12.3(4)T, 12.3(6), and 12.2(20)S and later, enter the following command to display detailed NetFlow cache information:

```
Router# execute-on slot-number show ip cache verbose flow
```

Examples

The following example shows output from the **show ip cache verbose flow** command:

```
Router# show ip cache verbose flow

IP packet size distribution (6 total packets):
 1-32  64  96 128 160 192 224 256 288 320 352 384 416 448 480
 .000 .833 .166 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

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

The output above shows the percentage distribution of packets by size. In this display, 83.3 percent of the packets fall in the 64-byte size range and 16.6 percent fall in the 96-byte range.

The next section of the output can be divided into three sections. The section and the table corresponding to each are as follows:

- NetFlow cache statistics lines ([Table 34](#))
- Protocol statistics ([Table 35](#))
- NetFlow record display ([Table 36](#))

```
IP Flow Switching Cache, 278544 bytes
 1 active, 4095 inactive, 2 added
 25 ager polls, 0 flow alloc failures
 Active flows timeout in 30 minutes
 Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 17096 bytes
 1 active, 1023 inactive, 2 added, 2 added to flow
 0 alloc failures, 0 force free
 1 chunk, 1 chunk added
 last clearing of statistics never
```

Protocol	Total	Flows	Packets	Bytes	Packets	Active(Sec)	Idle(Sec)
-----	Flows	/Sec	/Flow	/Pkt	/Sec	/Flow	/Flow
TCP-BGP	1	0.0	4	57	0.0	0.3	15.4
Total:	1	0.0	4	57	0.0	0.3	15.4

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	TOS	Flgs	Pkts
Port Msk AS		Port Msk AS	NextHop			B/Pk	Active
BGP: BGP NextHop							
Et0/0	3.3.3.3	Local	3.3.3.4	06	C0	18	2
2AF8 /24 0		00B3 /24 0	0.0.0.0			49	0.2
BGP: 0.0.0.0							

Table 34 describes the significant fields shown in the NetFlow cache lines of the display.

Table 34 *show ip cache verbose flow Field Descriptions in the NetFlow Cache Display*

Field	Description
bytes	Number of bytes of memory used by the NetFlow cache.
active	Number of active flows in the NetFlow cache at the time this command was entered.
inactive	Number of flow buffers that are allocated in the NetFlow cache but that are not assigned to a specific flow at the time this command is entered.
added	Number of flows created since the start of the summary period.
ager polls	Number of times the NetFlow code caused entries to expire (used by Cisco for diagnostics only).
flow alloc failures	Number of times the NetFlow code tried to allocate a flow but could not.
last clearing of statistics	Standard time output (hh:mm:ss) since the clear ip flow stats privileged EXEC command was last executed. This time output changes to hours and days after the time exceeds 24 hours.

Table 35 describes the significant fields shown in the activity by protocol lines of the display.

Table 35 *show ip cache verbose flow Field Descriptions in Activity By Protocol Display*

Field	Description
Protocol	IP protocol and the “well known” port number. (Refer to http://www.iana.org , <i>Protocol Assignment Number Services</i> for the latest RFC values.) Note Only a small subset of all protocols is displayed.
Total Flows	Number of flows for this protocol since the last time statistics were cleared.
Flows/Sec	Average number of flows for this protocol per second; equal to total flows divided by the number of seconds for this summary period.
Packets/Flow	Average number of packets for the flows for this protocol; equal to total packets for this protocol divided by the number of flows for this protocol for this summary period.
Bytes/Pkt	Average number of bytes for the packets for this protocol (total bytes for this protocol divided by the total number of packets for this protocol for this summary period).
Packets/Sec	Average number of packets for this protocol per second (total packets for this protocol divided by the total number of seconds for this summary period).

Table 35 show ip cache verbose flow Field Descriptions in Activity By Protocol Display (continued)

Field	Description
Active(Sec)/Flow	Number of seconds from the first packet to the last packet of an expired flow (for example, TCP connection close request [FIN], timeout, and so on) divided by the total flows for this protocol for this summary period.
Idle(Sec)/Flow	Number of seconds observed from the last packet in each nonexpired flow for this protocol until the time at which this command was entered divided by the total flows for this protocol for this summary period.

Table 36 describes the significant fields in the NetFlow record lines of the display.

Table 36 show ip cache verbose flow Field Descriptions in NetFlow Record Display

Field	Description
SrcIf	Interface on which the packet was received.
Port Msk AS	Source port number (displayed in hexadecimal format), IP address mask, and autonomous system number. This is always set to 0 in MPLS flows.
SrcIPAddress	IP address of the device which transmitted the packet.
DstIf	Interface from which the packet was transmitted.
Port Msk AS	Destination port number (displayed in hexadecimal format), IP address mask, and autonomous system. This is always set to 0 in MPLS flows.
DstIPAddress	IP address of the destination device.
NextHop	The BGP next hop address. This is always set to 0 in MPLS flows.
Pr	IP protocol “well-known” port number, displayed in hexadecimal format. (Refer to http://www.iana.org , <i>Protocol Assignment Number Services</i> , for the latest RFC values.)
TOS	Type of Service, displayed in hexadecimal format.
B/Pk	Average number of bytes observed for the packets seen for this protocol.
Flgs	TCP flags, shown in hexadecimal format (result of bitwise OR of TCP flags from all packets in the flow).
Pkts	Number of packets in this flow.
Active	The time in seconds that this flow has been active at the time this command was entered.

The following example shows the NetFlow output of the **show ip cache verbose cache flow** command in which the sampler, class-id, and general flags are set. What is displayed for a flow depends on what flags are set in the flow. If the flow was captured by a sampler, the output shows the sampler ID. If the flow was marked by Modular QoS CLI (MQC), the display includes the class ID. If any general flags are set, the output includes the flags.

```

...
SrcIf          SrcIPAddress  DstIf          DstIPAddress  Pr TOS Flgs  Pkts
Port Msk AS    Port Msk AS    NextHop        B/Pk  Active
BGP: BGP NextHop
Et1/0          8.8.8.8        Et0/0*         9.9.9.9       01 00 10      3
0000 /8 302      0800 /8 300    3.3.3.3       100    0.1
BGP: 2.2.2.2      Sampler: 1 Class: 1 FFlags: 01

```

Table 37 describes the significant fields shown in the NetFlow output for a sampler, an MQC policy class, and for general flags.

Table 37 *show ip cache verbose flow Field Descriptions for a NetFlow Sampler, an MQC Policy Class, and for General Flags*

Field	Description
Sampler: 1	Shows the ID of the sampler that captured the flow. The sampler ID in this example is 1.
Class: 1	Shows the ID of the MQC traffic class. The class ID in this example is 1.
FFlag: 01	Shows the general flow flag (shown in hexadecimal format), which is the bitwise OR of one or more of the following: <ul style="list-style-type: none"> • 01 = indicates an output (or egress) flow. (If this bit is not set, the flow is an input [or ingress] flow.) • 02 = indicates a flow that was dropped (for example, by an access list [ACL]). • 04 = indicates a Multiprotocol Label Switching (MPLS) flow. • 08 = indicates an IP Version 6 (IPv6) flow. The flow flag in this example is 01 (an egress flow).

The following example shows how to use the **show ip cache verbose flow** command to verify that NetFlow BGP next-hop accounting on a Cisco 7200 router is enabled:

```
Router# show ip cache verbose flow
```

```

...
SrcIf          SrcIPAddress  DstIf          DstIPAddress  Pr TOS Flgs  Pkts
Port Msk AS    Port Msk AS    NextHop        B/Pk  Active
MUL:M_Opaks  M_Obytes BGP:BGP_NextHop
Et0/0/2       12.0.0.2     Et0/0/4        13.0.0.5      01 00 10      20
0000 /8 0        0800 /8 0      11.0.0.6      100    0.0
BGP:26.0.0.6
Et0/0/2       12.0.0.2     Et0/0/4        15.0.0.7      01 00 10      20
0000 /8 0        0800 /8 0      11.0.0.6      100    0.0
BGP:26.0.0.6
Et0/0/2       12.0.0.2     Et0/0/4        15.0.0.7      01 00 10      20
0000 /8 0        0000 /8 0      11.0.0.6      100    0.0
BGP:26.0.0.6

```

Table 38 describes the significant fields shown in the NetFlow BGP next-hop accounting lines of the display.

Table 38 *show ip cache verbose flow Field Descriptions in NetFlow Multicast Accounting Output*

Field	Description
M_Opaks	Displays the number of IP multicast (IPM) output packets .
M_Obytes	Displays the number of IPM output bytes.
DstIPAddress	Displays the destination IP address for the IPM output packets.

The following example shows how the **show ip cache verbose flow** command can verify successful configuration of NetFlow multicast accounting:

```
Router# show ip cache verbose flow
```

```
...
SrcIf          SrcIPAddress  DstIf          DstIPAddress  Pr TOS Flgs Pkts
Port Msk AS    Port Msk AS    NextHop        B/Pk Active
IPM:OPkts     OBytes
IPM:  0        0
Et1/1/1       11.0.0.1      Null           227.1.1.1     01 55 10    100
0000 /8  0          0000 /0  0          0.0.0.0       28    0.0
IPM: 100      2800
Et1/1/1       11.0.0.1      Se2/1/1.16     227.1.1.1     01 55 10    100
0000 /8  0          0000 /0  0          0.0.0.0       28    0.0
IPM:  0        0
Et1/1/2       12.0.0.1      Et1/1/4        227.2.2.2     01 55 10    100
0000 /8  0          0000 /0  0          0.0.0.0       28    0.1
Et1/1/2       12.0.0.1      Null           227.2.2.2     01 55 10    100
0000 /8  0          0000 /0  0          0.0.0.0       28    0.1
IPM: 100      2800
```

Table 39 describes the significant fields shown in the NetFlow multicast accounting lines of the display.

Table 39 *show ip cache verbose flow Field Descriptions in NetFlow Multicasting Accounting Display*

Field	Description
OPkts	Displays the number of IP multicast (IPM) output packets.
OBytes	Displays the number of IPM output bytes.
DstIPAddress	Displays the destination IP address for the IPM output packets.

Related Commands

Command	Description
ip route-cache flow	Enables NetFlow data collection on the interface.
show ip cache flow	Displays a summary of the NetFlow statistics.