backup (NetFlow SCTP) through ip route-cache flow

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

backup (NetFlow SCTP)

To configure a backup destination for the reliable export of NetFlow accounting information in NetFlow cache entries, use the **backup**command in NetFlow ip flow export stream control transmission protocol (SCTP) configuration mode. To remove a destination for the reliable export of NetFlow accounting information, use the noform of this command.

backup {**destination** {*ip-address* | *hostname*} *sctp-port* | **fail-over** *time* | **mode** {**fail-over** | **redundant**} | **restore-time** *time*}

no backup {**destination** {*ip-address* | *hostname*} *sctp-port* | **fail-over** | **mode** {**fail-over** | **redundant**} | **restore-time**}

Syntax Description

ip-address | *hostname*	IP address or hostname of the workstation to which you want to send the NetFlow information.
port	Specifies the number of the stream control transmission protocol (SCTP) port on which the workstation is listening for the exported NetFlow datagrams.
fail-over *time*	(Optional) Specifies the length of time that the primary export destination must be unavailable before SCTP starts using the backup export destination. The default fail-over time for sctp to start using a backup export destination is 25 milliseconds (msec). Range: 0 to 3600 msec.
mode {**fail-over** | **redundant**}	(Optional) Specifies the mode that SCTP will use to establish a connection to the backup export destination: • **fail-over** --Opens an association with the backup export destination when the primary export destination becomes unavailable • **redundant** --Maintains a permanent association with the backup export destination.
restore-time *time*	(Optional) Specifies the length of time that the primary export destination must be available after an outage before SCTP reverts back to it. This is applicable only when SCTP is using the backup export destination. Range: 0 to 3600 seconds.

Command Default

Backup destinations for the reliable export of NetFlow information are not configured.

Command Modes NetFlow ip flow export SCTP (config-flow-export-sctp)

Usage Guidelines When you configure a backup export destination for SCTP messages are sent to the destination if the primary export destination becomes unavailable. When connectivity with the primary export destination has been lost and a backup export destination is configured, SCTP begins using the backup export destination. The default period of time that SCTP waits until it starts using the backup export destination is 25 sec. You can configure a different with the **fail-over***time* command.

Note SCTP retransmits messages that have not been acknowledged three times. The router will initiate fail-over after three retransmissions of the same message are not acknowledged by the primary collector.

The router sends periodic SCTP heart beat messages to the SCTP export destinations that you have configured. The router uses the SCTP heart-beat message acknowledgments from the export destinations to monitor the status of each export destination. This allows an application, such as NetFlow, to be quickly informed when connectivity to an export destination is lost.

You can configure SCTP backup in fail-over or redundant mode. When the router is configured with SCTP backup in fail-over mode the router waits to activate the association with the backup export destination until the router has not received acknowledgments for the SCTP heart beat messages from the primary export destination for the time specified by the **fail-over***time* command. When the router is configured with SCTP backup in redundant mode, the router activates the association with the backup export destination immediately instead of waiting for the primary export destination to fail. The router will not start sending SCTP messages to a backup export destination in redundant mode until the router has not received acknowledgements for the SCTP heart beat messages from the primary export destination for the time specified by the **fail-over***time* command. Fail-over mode is the preferred method when the backup export destination is on the end of an expensive lower-bandwidth link such as ISDN.

During the time that SCTP is using the backup export destination, SCTP continues to try to restore the association with the primary export destination. SCTP makes this attempt until connectivity is restored or the primary SCTP export destination is removed from the configuration.

When connectivity to the primary export destination is available again, the router waits for a period of time before reverting to using it as the primary destination. You use the **restore-time***time command to* configure the value of the period of time that SCTP waits until reverting. The default period of time that SCTP waits is 25 msecs.

Under either fail-over mode, any records which have been queued between loss of connectivity with the primary destination and, the establishing of the association with the backup export destination might be lost. A count of how many records were lost can be viewed through the use of the **show ip flow export sctp verbose** command.

To avoid a flapping SCTP association with an export destination (the SCTP association going up and down in quick succession), the time period configured with the **restore-time***time* command should be greater than the period of a typical connectivity problem. For example, your router is configured to use IP fast convergence for its routing table and you have a LAN interface that is going up and down repeatedly (flapping). This causes the IP route to the primary export destination to be added to and removed from the routing table (route flapping) every 2000 msec (2 sec) you need to configure the restore time for a value greater than 2000 msec.

The backup connection uses stream 0 for sending templates, options templates, and option records. The data stream(s) inherit the reliability settings of the primary export destination.

Command History

Release	Modification
12.4(4)T	This command was introduced.

Examples

The following example shows how to configure the networking device to use SCTP as the transport protocol for transmissions to multiple export destinations in redundant mode. The router activates the association with the backup export destination immediately instead of waiting until the primary export destination fails. The router starts sending SCTP messages to the backup export destination over the preexisting association after it fails to receive acknowledgments for its SCTP heart-beat messages from the primary export destination for 1500 msec. The router waits 3000 msec after the primary export destination is reachable again before resuming the association with the primary export destination.

```
Router(config)# ip flow-export destination 172.16.10.2 78 sctp
Router(config-flow-export-sctp)# backup destination 172.16.10.3 78
Router(config-flow-export-sctp)# backup mode redundant
Router(config-flow-export-sctp)# backup fail-over 1500
Router(config-flow-export-sctp)# backup restore-time 3000
```

The following example shows how to configure the networking device to use SCTP as the transport protocol to multiple export destinations in fail-over mode. The router activates the association with the backup export destination and starts sending SCTP messages to the backup export destination after it fails to receive acknowledgments for its SCTP heart beat messages from the primary export destination for 1500 msec. The router waits 3000 sec after the primary export destination is reachable again before resuming the association with the primary export destination. The SCTP association with the backup export destination is closed after the router resumes sending SCTP messages to the primary export destination.

```
Router(config)# ip flow-export destination 172.16.10.2 78 sctp
Router(config-flow-export-sctp)# backup destination 172.16.10.3 78
Router(config-flow-export-sctp)# backup mode fail-over
Router(config-flow-export-sctp)# backup fail-over 1500
Router(config-flow-export-sctp)# backup restore-time 3000
```

Related Commands

Command	Description
ip flow-export destination sctp	Enables the reliable export of NetFlow accounting information in NetFlow cache entries.
reliability	Specifies the level of reliability for the reliable export of NetFlow accounting information in NetFlow cache entries.
show ip flow export	Displays the status and the statistics for NetFlow accounting data export.

cache

To configure operational parameters for NetFlow accounting aggregation caches, use the **cache** command in NetFlow aggregation cache configuration mode. To disable the NetFlow aggregation cache operational parameters for NetFlow accounting, use the **no** form of this command.

cache {**entries** *number* | **timeout** {**active** *minutes* | **inactive** *seconds*}}

no cache {**entries** | **timeout** {**active** | **inactive**}}

Syntax Description

entries *number*	(Optional) The number of cached entries allowed in the aggregation cache. The range is from 1024 to 524288. The default is 4096. **Note** For the Cisco ASR 1000 Series Aggregation Services Router, the range is 1024 to 2000000 (2 million). The default is 4096.
timeout	(Optional) Configures aggregation cache time-outs.
active *minutes*	(Optional) The number of minutes that an active entry will stay in the aggregation cache before it is exported and removed. The range is from 1 to 60 minutes. The default is 30 minutes.
inactive *seconds*	(Optional) The number of seconds that an inactive entry will stay in the aggregation cache before it times out. The range is from 10 to 600 seconds. The default is 15 seconds.

Command Default

The operational parameters for NetFlow accounting aggregation caches are not configured.

Command Modes

NetFlow aggregation cache configuration (config-flow-cache)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(7)T	This command function was modified to support cache entries for IPv6.

Release	Modification
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You must have NetFlow accounting configured on your router before you can use this command. .

Examples

The following example shows how to set the NetFlow aggregation cache entry limits and timeout values for the NetFlow protocol-port aggregation cache:

```
Router(config)#
ip flow-aggregation cache protocol-port
Router(config-flow-cache)#
cache entries 2046
Router(config-flow-cache)#
cache timeout inactive 199
Router(config-flow-cache)#
cache timeout active 45
Router(config-flow-cache)#
enabled
```

Related Commands

Command	Description
enabled (aggregation cache)	Enables a NetFlow accounting aggregation cache.
export destination (aggregation cache)	Enables the exporting of NetFlow accounting information from NetFlow aggregation caches.
ip flow-aggregation cache	Enables NetFlow accounting aggregation cache schemes.
mask (IPv4)	Specifies the source or destination prefix mask for a NetFlow accounting prefix aggregation cache.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache flow aggregation	Displays the NetFlow accounting aggregation cache statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.

show ip flow interface	Displays NetFlow accounting configuration for interfaces.

cache-timeout

To specify the length of time for which the list of NetFlow top talkers (unaggregated top flows) is retained, use the **cache-timeout** command in NetFlow top talkers configuration mode. To return the timeout parameters for the list of top talkers to the default of 5 seconds, use the **no** form of this command.

cache-timeout *milliseconds*

no cache-timeout

Syntax Description

milliseconds	Length in milliseconds for which the list of top talkers is retained. The range is from 1 to 3,600,000 (1 millisecond to one hour). The default is 5000 (5 seconds).

Command Default

The default time for which the list of top talkers is retained is 5 seconds.

Command Modes

NetFlow top talkers configuration

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.3(11)T	This feature was integrated into Cisco IOS Release 12.3(11)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Configuring NetFlow top talkers

You must enable NetFlow on at least one interface in the router; and configure NetFlow top talkers before you can use the **show ip flow top-talkers** command to display the traffic statistics for the unaggregated top

flows in the network. NetFlow top talkers also requires that you configure the **sort-by** and **top** commands. Optionally, the **match** command can be configured to specify additional matching criteria.

Cache Timeout

The cache timeout starts after the list of top talkers is requested by entering the **show ip flow top-talkers**command or through the netflow MIB.

A long timeout period limits the system resources that are used by NetFlow top talkers. However, the list of top talkers is calculated only once during the timeout period. If a request to display the top talkers is made more than once during the timeout period, the same results are displayed for each request, and the list of top talkers is not recalculated until the timeout period expires.

A short timeout period ensures that the latest list of top talkers is retrieved; however too short a period can have undesired effects:

- The list of top talkers is lost when the timeout period expires. You should configure a timeout period for at least as long as it takes the network management system (NMS) to retrieve all the required NetFlow top talkers.
- The list of top talkers is updated every time the top talkers information is requested, possibly causing unnecessary usage of system resources.

A good method to ensure that the latest information is displayed, while also conserving system resources, is to configure a large value for the timeout period, but recalculate the list of top talkers by changing the parameters of the **cache-timeout**, **top**, or **sort-by** command prior to entering the **show ip flow top-talkers**command to display the top talkers. Changing the parameters of the **cache-timeout**, **top**, or **sort-by** command causes the list of top talkers to be recalculated upon receipt of the next command line interface (CLI) or MIB request.

Examples

In the following example, the list of top talkers is configured to be retained for 2 seconds (2000 milliseconds). There is a maximum of 4 top talkers, and the sort criterion is configured to sort the list of top talkers by the total number of bytes in each top talker.

```
Router(config)# ip flow-top-talkers
Router(config-flow-top-talkers)# cache-timeout 2000
Router(config-flow-top-talkers)# top 4
Router(config-flow-top-talkers)# sort-by bytes
```

The following example shows the output of the **show ip flow top talkers** command using the configuration from the previous example:

```
Router# show ip flow top-talkers

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP Bytes
Et0/0.1       10.10.18.1      Et1/0.1       172.16.10.232   11 00A1 00A1   349K
Et0/0.1       10.10.19.1      Et1/0.1       172.16.10.2     11 00A2 00A2   349K
Et0/0.1       172.30.216.196  Et1/0.1       172.16.10.2     06 0077 0077   328K
Et0/0.1       10.162.37.71    Et1/0.1       172.16.10.2     06 0050 0050   303K
4 of 4 top talkers shown. 11 flows processed
```

Related Commands

Command	Description
ip flow-top-talkers	Enters the configuration mode for the NetFlow MIB and top talkers (heaviest traffic patterns and most-used applications in the network) feature.
match (NetFlow)	Specifies match criteria for the NetFlow MIB and top talkers (heaviest traffic patterns and most-used applications in the network) feature.
show ip flow top-talkers	Displays the statistics for the top talkers (heaviest traffic patterns and most-used applications in the network).
sort-by	Specifies the sorting criterion for top talkers (heaviest traffic patterns and most-used applications in the network) to be displayed for the NetFlow MIB and top talkers feature.
top	Specifies the maximum number of top talkers (heaviest traffic patterns and most-used applications in the network) to be displayed for the NetFlow MIB and top talkers feature.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

clear fm netflow counters

To clear the NetFlow counters, use the **clear fm netflow counters** command in privileged EXEC mode.

clear fm netflow counters

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on systems that are configured with a Supervisor Engine 2.

Examples

This example shows how to clear the NetFlow counters:

```
Router# clear fm netflow counters
Router#
```

clear ip flow stats

To clear the NetFlow accounting statistics, use the **clear ip flow stats** command in privileged EXEC mode.

clear ip flow stats [**nbar**]

Syntax Description

nbar	(Optional) Clears Network Based Application Recognition (NBAR) NetFlow statistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.1CA	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2(17d)SXB release.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)ZYA2	This command was modified. The **nbar**keyword was added.

Usage Guidelines

You must have NetFlow accounting configured on your router before you can use this command.

The **show ip cache flow**command displays the NetFlow accounting statistics. Use the **clear ip flow stats**command to clear the NetFlow accounting statistics.

Examples

The following example shows how to clear the NetFlow accounting statistics on the router:

```
Router# clear ip flow stats
```

Related Commands

Command	Description
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.
show ip interface	Displays the usability status of interfaces configured for IP.

clear mls nde flow counters

To clear the NDE counters, use the **clearmlsndeflowcounters** command.

clear mls nde flow counters

Syntax Description

This command has no keywords or arguments.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to reset the NDE counters:

```
Router#
clear mls nde flow counters
Router#
```

Related Commands

Command	Description
show mls nde	Displays information about the NDE hardware-switched flow.

clear mls netflow

To clear the MLS NetFlow-shortcut entries, use the **clearmlsnetflow**command.

clear mls netflow ip [**destination** *ip-addr* [**source** *ip-addr-spec*]] [**dynamic** | **sw-installed** [**non-static** | **static**]] [**module** *mod*]

clear mls netflow ipv6 [**destination** *ipv6-addr* [**slash** *ipv6-prefix*] [**source** *ipv6-addr* [**slash** *ipv6-prefix*]]] [**flow** {**tcp** | **udp**}] [{**destination** | **source**} *port-num*] [**dynamic** | **sw-installed** [**non-static** | **static**]] [**module** *mod*]

clear mls netflow mpls [**top-label** *entry*] [**dynamic** | **sw-installed** [**non-static** | **static**]] [**module** *mod*]

clear mls ipx [[**module** *mod*] [**destination** *ipx-network* [*ipx-node*]] [**source** *ipx-network*] [**macs** *mac-addr*] [**macd** *mac-addr*] [**interface** *interface-num*] | [**all**]]

Syntax Description

ip	Clears IP MLS entries.
destination *ip-addr*	(Optional) Specifies a destination f ull IP address or a subnet address. See the “Usage Guidelines” section for formatting guidelines.
source *ip-addr*	(Optional) Specifies a source f ull IP address or a subnet address. See the “Usage Guidelines” section for formatting guidelines.
dynamic	(Optional) Clears NetFlow-statistics entries that are created in the hardware.
sw-installed non-static	(Optional) Clears software-installed nonstatic entries.
sw-installed static	(Optional) Clears software-installed static entries.
module *mod*	(Optional) Specifies a module number.
ipv6	Clears IP version 6 software-installed entries.
destination *ipv6-addr*	(Optional) Specifies a destination f ull IPv6 address or a subnet address. See the “Usage Guidelines” section for formatting guidelines.
/ *ipv6-prefix*	(Optional) IPv6 prefix; valid values are from 0 to 128.
source *iv6p-addr*	(Optional) Specifies a source f ull IPv6 address or a subnet address. See the “Usage Guidelines” section for formatting guidelines.
flow tcp	(Optional) Clears TCP flow information.

flow udp	(Optional) Clears UDP flow information.
destination *port-num*	(Optional) Specifies a destination port number.
source*port-num*	(Optional) Specifies a source port number.
mpls	Clears MPLS software-installed entries.
top-label *entry*	(Optional) Clears top-label entries; valid values are from 1 to 4294967295.
ipx	Clears IPX MLS entries.
destination *ipx-network*	(Optional) Specifies the destination IPX address. See the “Usage Guidelines” section for formatting guidelines.
ipx-node	(Optional) IPX node address. See the “Usage Guidelines” section for formatting guidelines.
source *ipx-network*	(Optional) Specifies the source IPX address. See the “Usage Guidelines” section for formatting guidelines.
macs *mac-addr*	(Optional) Specifies the source MAC addresses to consider when searching for entries to purge.
macd *mac-addr*	(Optional) Specifies the destination MAC addresses to consider when searching for entries to purge.
interface *interface-num*	(Optional) Clears entries that are associated with the specified VLAN or interface.
all	(Optional) Clears all entries.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.

Release	Modification
12.2(17a)SX	This command was changed as follows: • Replaced the **routes** keyword with **sw-installed**. • Replaced the **statistics** keyword with **dynamic**. • Changed the syntax from **clearmls** [**ip** | **ipv6** | **mpls**] to **clearmlsnetflow** [**ip** | **ipv6** | **mpls**]
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(18)SXF	This command was changed as follows: • Removed support for the **any** keyword. • Added the */ipv6-prefix* argument.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **destination***ipx-network, ipx-node*, and**source***ipx-network* keywords and arguments are supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2 only.

When entering the IPX address syntax, use the following format:

- IPX network address--1..FFFFFFFE
- IPX node address--x.x.x where x is 0..FFFF
- IPX address--ipx_net.ipx_node (for example, 3.0034.1245.AB45, A43.0000.0000.0001)

Entering any combination of input parameters narrows the search of entries to be cleared. The **destination** or **source***port-num* keyword and argument should be specified as one of the following: telnet, FTP, WWW, SMTP, X, or DNS.

Up to 16 routers can be included explicitly as MLS-RPs.

Use the following syntax to specify an IP subnet address:

- *ip-subnet-addr* or *ipv6-subnet-addr*--Short subnet address format. The trailing decimal number 00 in an IP or IPv6 address YY.YY.YY.00 specifies the boundary for an IP or IPv6 subnet address. For example, 172.22.36.00 indicates a 24-bit subnet address (subnet mask 172.22.36.00/255.255.255.0), and 173.24.00.00 indicates a 16-bit subnet address (subnet mask 173.24.00.00/255.255.0.0). However, this format can identify only a subnet address of 8, 16, or 24 bits.
- *ip-addr/subnet-mask* or *ipv6-addr/subnet-mask*--Long subnet address format. For example, 172.22.252.00/255.255.252.00 indicates a 22-bit subnet address. This format can specify a subnet address of any bit number. To provide more flexibility, the *ip-addr* or *ipv6-addr*is a full host address, such as 172.22.253.1/255.255.252.00.
- *ip-addr/maskbits* or *ipv6-addr/maskbits*--Simplified long subnet address format. The mask bits specify the number of bits of the network masks. For example, 172.22.252.00/22 indicates a 22-bit subnet address. The *ip-addr*or *ipv6-addr* is a full host address, such as 193.22.253.1/22, which has the same subnet address as the *ip-subnet-addr*or *ipv6-subnet-addr*.

If you do not use the **all** keyword, you must specify at least one of the other four keywords (**source**, **destination**, **flow**, or **interface**) an d its arguments.

A 0 value for the **destination** or **source***port-num* keyword and argument clears all entries. Unspecified options are treated as wildcards, and all entries are cleared.

Examples

This example shows how to clear all the entries that are associated with a specific module (2) and that have a specific destination IP address (173.11.50.89):

```
Router#
 clear mls netflow ip destination 173.11.50.89 module 2
Router#
```

This example shows how to clear the IPv6 software-installed entries:

```
Router#
clear mls netflow ipv6
Router#
```

This example shows how to clear the statistical information:

```
Router#
clear mls netflow dynamic
Router#
```

Related Commands

Command	Description
show mls netflow ip	Displays information about the hardware NetFlow IP.
show mls netflow ipv6	Displays information about the hardware NetFlow IPv6 configuration.

debug mpls netflow

To display debug messages for MPLS egress NetFlow accounting, use the **debug mpls netflow**command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug mpls netflow

no debug mpls netflow

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Examples

Here is sample output from the **debug mpls netflow** command:

```
Router# debug mpls netflow
MPLS Egress NetFlow debugging is on
Router#
Router#
Router#
4d00h:Egress flow:entry created, dest 3.3.3.3/32, src 34.0.0.1/8
Router#
Router#
4d00h:Egress flow:entry created, dest 3.3.3.3/32, src 42.42.42.42/32
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# int eth1/4
Router(config-if)# no mpls netflow egress
Router(config-if)#
```

```
4d00h:MPLS output feature change, trigger TFIB scan
4d00h:tfib_scanner_walk, prefix 5.5.5.5/32, rewrite flow flag 0
4d00h:tfib_scanner_walk, prefix 2.0.0.0/8, rewrite flow flag 0
4d00h:tfib_scanner_walk, prefix 3.3.3.3/32, rewrite flow flag 0
4d00h:tfib_scanner_walk, prefix 40.40.40.40/32, rewrite flow flag 0
4d00h:tfib_scanner_walk, prefix 50.50.50.50/32, rewrite flow flag 0
4d00h:tfib_scanner_walk, prefix 100.100.100.100/32, rewrite flow flag 0
4d00h:tfib_scanner_walk, prefix 180.1.1.0/24, rewrite flow flag 0
4d00h:tfib_scanner_walk, prefix 190.1.1.0/24, rewrite flow flag 1
4d00h:tfib_scanner_walk, prefix 2.0.0.0/8, rewrite flow flag 1
4d00h:tfib_scanner_walk, prefix 4.4.4.4/32, rewrite flow flag 1
4d00h:tfib_scanner_walk, prefix 40.40.40.40/32, rewrite flow flag 0
4d00h:tfib_scanner_walk, prefix 50.50.50.50/32, rewrite flow flag 0
4d00h:tfib_scanner_walk, prefix 177.1.1.0/24, rewrite flow flag 1
4d00h:tfib_scanner_walk, prefix 180.1.1.0/24, rewrite flow flag 0
4d00h:tfib_scanner_walk, prefix 190.1.1.0/24, rewrite flow flag 1
Router(config-if)#
Router(config-if)# mpls netflow egress
Router(config-if)#
4d00h:Interface refcount with output feature enabled = 2
4d00h:MPLS output feature change, trigger TFIB scan
4d00h:tfib_scanner_walk, prefix 5.5.5.5/32, rewrite flow flag 0
4d00h:tfib_scanner_walk, prefix 2.0.0.0/8, rewrite flow flag 1
4d00h:tfib_scanner_walk, prefix 3.3.3.3/32, rewrite flow flag 1
4d00h:tfib_scanner_walk, prefix 40.40.40.40/32, rewrite flow flag 0
4d00h:tfib_scanner_walk, prefix 50.50.50.50/32, rewrite flow flag 0
4d00h:tfib_scanner_walk, prefix 100.100.100.100/32, rewrite flow flag 1
4d00h:tfib_scanner_walk, prefix 180.1.1.0/24, rewrite flow flag 1
4d00h:tfib_scanner_walk, prefix 190.1.1.0/24, rewrite flow flag 1
4d00h:tfib_scanner_walk, prefix 2.0.0.0/8, rewrite flow flag 1
4d00h:tfib_scanner_walk, prefix 4.4.4.4/32, rewrite flow flag 1
4d00h:tfib_scanner_walk, prefix 40.40.40.40/32, rewrite flow flag 0
4d00h:tfib_scanner_walk, prefix 50.50.50.50/32, rewrite flow flag 0
4d00h:tfib_scanner_walk, prefix 177.1.1.0/24, rewrite flow flag 1
4d00h:tfib_scanner_walk, prefix 180.1.1.0/24, rewrite flow flag 1
4d00h:tfib_scanner_walk, prefix 190.1.1.0/24, rewrite flow flag 1
4d00h:Egress flow:entry created, dest 3.3.3.3/32, src 42.42.42.42/32
Router(config-if)#
Router(config-if)# end
Router# show run int eth1/4
Building configuration...
Current configuration:
!
interface Ethernet1/4
 ip vrf forwarding vpn1
 ip address 180.1.1.1 255.255.255.0
 no ip directed-broadcast
 mpls netflow egress
end
Router#
Router#
4d00h:%SYS-5-CONFIG_I:Configured from console by console
Router#
```

Note Flow flag 1 prefixes are reachable through this interface; therefore, MPLS egress NetFlow accounting is applied to all packets going out the destination prefix. Flow flag 0 prefixes are not reachable through this interface; therefore, MPLS egress NetFlow accounting is not applied to any packets going out the destination prefix.

Related Commands

Command	Description
show debug	Displays active debug output.

enabled (aggregation cache)

To enable a NetFlow accounting aggregation cache, use the **enabled** command in NetFlow aggregation cache configuration mode. To disable a NetFlow accounting aggregation cache, use the **no** form of thiscommand.

enabled

no enabled

Syntax Description

This command has no arguments or keywords.

Command Default

No aggregation cache is enabled.

Command Modes

NetFlow aggregation cache configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You must have NetFlow accounting configured on your router before you can use this command.

Examples

The following example shows how to enable a NetFlow protocol-port aggregation cache:

Router(config)# **ip flow-aggregation cache protocol-port**

```
Router(config-flow-cache)# enabled
```

The following example shows how to disable a NetFlow protocol-port aggregation cache:

Router(config)# **ip flow-aggregation cache protocol-port**

```
Router(config-flow-cache)# no
 enabled
```

Related Commands

Command	Description
cache	Defines operational parameters for NetFlow accounting aggregation caches.
export destination (aggregation cache)	Enables the exporting of NetFlow accounting information from NetFlow aggregation caches.
ip flow-aggregation cache	Enables NetFlow accounting aggregation cache schemes.
mask (IPv4)	Specifies the source or destination prefix mask for a NetFlow accounting prefix aggregation cache.
show ip cache flow aggregation	Displays the NetFlow accounting aggregation cache statistics.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

export destination

To enable the exporting of NetFlow accounting information from NetFlow aggregation caches, use the **export destination** command in NetFlow aggregation cache configuration mode. To disable the export of NetFlow accounting information from NetFlow aggregation caches, use the **no** form of this command.

export destination {*hostname* | *ip-address*} *port* [**vrf** *vrf-name*] [**udp**]

no export destination {*hostname* | *ip-address*} *port* [**vrf** *vrf-name*] [**udp**]

Syntax Description

ip-address | *hostname*	IP address or hostname of the workstation to which you want to send the NetFlow information
port	Specifies the number of the user datagram protocol (UDP) port on which the workstation is listening for the exported NetFlow datagrams.
vrf *vrf-name*	(Optional) The **vrf** keyword specifies that the export data packets are to be sent to the named Virtual Private Network (VPN) routing forwarding instance (VRF) for routing to the destination, instead of to the global routing table. **Note** The *vrf-name* argument is the name of the VRF
udp	(Optional) Specifies UDP as the transport protocol. UDP is the default transport protocol.

Command Default

Export of NetFlow information from NetFlow aggregation caches is disabled.

Command Modes

NetFlow aggregation cache configuration (config-flow-cache)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2T	This command was modified to enable multiple NetFlow export destinations to be used.
12.3(1)	Support for the NetFlow v9 Export Format feature was added.

Release	Modification
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S, and support for the Multiple Export Destinations feature was added.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If the version of Cisco IOS that you have installed on your networking device supports the NetFlow Multiple Export Destinations feature, you can configure your networking device to export NetFlow data to a maximum of 2 export destinations (collectors) per cache (main and aggregation caches), using any combination of UDP and SCTP as the transport protocol for the destinations. A destination is identified by a unique combination of hostname or IP address and port number or port type.

Note UDP is the default transport protocol used by the **export destination**command. In some Cisco IOS releases you can configure SCTP as the transport protocol if you need reliability and additional redundancy. Refer to the **export destination sctp** command for more information.

The table below shows examples of the 2 permitted NetFlow export destinations for each cache.

Table 1 Examples of Permitted Multiple NetFlow Export Destinations for Each Cache

First Export Destination	Second Export Destination
ip flow-export *10.25.89.32 100 udp*	**ip flow-export** *10.25.89.32 285 udp*
ip flow-export *10.25.89.32 100 udp*	**ip flow-export** *172.16.89.32 100 udp*
ip flow-export *10.25.89.32 100 udp*	**ip flow-export** *172.16.89.32 285 udp*
ip flow-export *10.25.89.32 100 udp*	**ip flow-export** *10.25.89.32 100 sctp*
ip flow-export *10.25.89.32 100 sctp*	**ip flow-export** *10.25.89.32 285 sctp*
ip flow-export *10.25.89.32 100 sctp*	**ip flow-export** *172.16.89.32 100 sctp*
ip flow-export *10.25.89.32 100 sctp*	**ip flow-export** *172.16.89.32 285 sctp*

The most common use of the multiple-destination feature is to send the NetFlow cache entries to two different destinations for redundancy. Therefore, in most cases the second destination IP address is not the same as the first IP address. The port numbers can be the same when you are configuring two unique destination IP addresses. If you want to configure both instances of the command to use the same destination IP address, you must use unique port numbers. You receive a warning message when you

configure the two instances of the command with the same IP address. The warning message is, "%Warning: Second destination address is the same as previous address <ip-address>".

VRF Destinations for Exporting NetFlow Data

Before Cisco IOS Releases 12.4(4)T and 12.2(18)SXH, only one routing option existed for NetFlow export data packets. NetFlow sent all export data packets to the global routing table for routing to the export destinations you specified.

Cisco IOS 12.4(4)T, 12.2(18)SXH, and later releases provide an additional routing option for NetFlow export data packets. You can send NetFlow data export packets to a Virtual Private Network (VPN) routing/forwarding instance (VRF) for routing to the destinations that you specify.

To send NetFlow data export packets to a VRF for routing to a destination, you enter the optional **vrf***vrf-name* keyword and argument with the **ip flow-export destination** *ip-addressport* command. To configure the global routing table option, enter this command without the optional **vrf***vrf-name* keyword and argument.

Examples

The following example shows how to configure two export destinations for a NetFlow accounting protocol-port aggregation cache scheme:

```
Router(config)#
ip flow-aggregation cache protocol-port
Router(config-flow-cache)# export destination 10.41.41.1 9992
Router(config-flow-cache)# export destination 172.16.89.1 9992
Router(config-flow-cache)# enabled
```

The following example shows how to configure the networking device for exporting from the NetFlow **source-prefix-tos** aggregation cache to an export destination that is reachable in VRF group1:

```
Router(config)#
ip flow-aggregation cache source-prefix-tos
Router(config-flow-cache)#
 export destination 172.16.10.2 78 vrf group1
Router(config-flow-cache)#
enabled
```

Related Commands

Command	Description
export template	Configures template options for the export of NetFlow accounting information in NetFlow aggregation cache entries
export version	Specifies the export version format for the exporting of NetFlow accounting information in NetFlow aggregation cache entries
show ip flow export	Displays the status and the statistics for NetFlow accounting data export.

export destination sctp (NetFlow aggregation cache)

To enable the reliable export of NetFlow accounting information from NetFlow aggregation caches, use the **export destination sctp** command in NetFlow aggregation cache configuration mode. To disable the reliable export of NetFlow accounting information from NetFlow aggregation caches, use the **no** form of this command.

export destination {*ip-address* | *hostname*} *port* [**vrf** *vrf-name*] **sctp**

no export destination {*ip-address* | *hostname*} *port* [**vrf** *vrf-name*] **sctp**

Syntax Description

ip-address | *hostname*	IP address or hostname of the workstation to which you want to send the NetFlow information.
port	Specifies the number of the stream control transmission protocol (SCTP) port on which the workstation is listening for the exported NetFlow datagrams.
vrf *vrf-name*	(Optional) The **vrf** keyword specifies that the export data packets are to be sent to the named Virtual Private Network (VPN) routing forwarding instance (VRF) for routing to the destination, instead of to the global routing table. **Note** The *vrf-name* argument is the name of the VRF

Command Default

Reliable export of NetFlow information from NetFlow aggregation caches is disabled.

Command Modes

NetFlow aggregation cache configuration (config-flow-cache)

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

NetFlow Reliable Export Using SCTP

SCTP can be used as an alternative to UDP when you need a more robust and flexible transport protocol than UDP. SCTP is a reliable message-oriented transport layer protocol, which allows data to be transmitted between two end-points in a reliable, partially reliable, or unreliable manner.

An SCTP session consists of an association (connection) between two end-points (peers), which can contain one or more logical channels called streams. The default mode of transmission for a stream is to guarantee reliable ordered delivery of messages using a selective-acknowledgment scheme. SCTP buffers messages until their receipt has been acknowledged by the receiving end-point. SCTP has a congestion control mechanism which limits how much memory is consumed by the SCTP stack, in packet buffering.

VRF Destinations for Exporting NetFlow Data

Before Cisco IOS Release 12.4(4)T, one routing option existed for NetFlow export data packets. NetFlow sent all export data packets to the global routing table for routing to the destinations you specified.

Cisco IOS 12.4(4)T and later releases provide an additional routing option for NetFlow export data packets. You can send NetFlow data export packets to a Virtual Private Network (VPN) routing/forwarding instance (VRF) for routing to the destinations that you specify.

To send NetFlow data export packets to a VRF for routing to a destination, you enter the optional **vrf***vrf-name* keyword and argument with the **export destination** *ip-addressport* command. To configure the global routing table option, enter this command without the optional **vrf***vrf-name* keyword and argument.

Examples

The following example shows how to configure the networking device to use SCTP as the transport protocol when exporting NetFlow data from a NetFlow AS aggregation cache to a host:

```
Router(config)#
ip flow-aggregation cache as
Router(config
-flow-cache
)# export destination 172.16.10.2 78 sctp
Router(config
-flow-cache
)# enabled
```

The following example shows how to configure the networking device to use SCTP as the transport protocol when exporting NetFlow data from a NetFlow AS aggregation cache to a host that is reachable in VRF group1:

```
Router(config)#
ip flow-aggregation cache as
Router(config
-flow-cache
)# export destination 172.16.10.2 78 vrf group1 sctp
Router(config
-flow-cache
)# enabled
```

Related Commands

Command	Description
backup	Configures a backup destination for the reliable export of NetFlow accounting information in NetFlow cache entries

Command	Description
export destination	Enables the export of NetFlow accounting information in NetFlow aggregation cache entries to a remote device such as a server running an application that analyzes NetFlow data.
export template	Configures template options for the export of NetFlow accounting information in NetFlow aggregation cache entries
export version	Specifies the export version format for the exporting of NetFlow accounting information in NetFlow aggregation cache entries
reliability	Specifies the level of reliability for the reliable export of NetFlow accounting information in NetFlow cache entries.
show ip flow export	Displays the status and the statistics for NetFlow accounting data export.

export template

To configure template options for the export of NetFlow accounting information from NetFlow aggregation caches, use the **export template** command in NetFlow aggregation cache configuration mode. To return to the default behavior, use the noform of this command.

Configure template only

export template {**refresh-rate** *packets* | **timeout-rate** *minutes*}

no export template {**refresh-rate** | **timeout-rate**}

Configure template options

ip export template options {**export-stats** | **refresh-rate** *packets* | **timeout-rate** *minutes* | **sampler**}

no export template options {**export-stats** | **refresh-rate** | **timeout-rate** | **sampler**}

Syntax Description

template	Enables the **refresh-rate** and **timeout-rate** keywords for the configuring of Version 9 export templates.
refresh-rate *packets*	(Optional) Specifies the number of export packets that are sent before the options and flow templates are resent. Range:1 to 600 packets. The default is 20 packets. **Note** This applies to the **export template refresh-rate** *packets* command.
timeout-rate *minutes*	(Optional) Specifies the interval (in minutes) that the router waits after sending the templates (flow and options) before sending them again. Range: 1 to 3600 minutes. The default is 30 minutes. **Note** This applies to the **export template timeout-rate** *minutes* command.
options	(Optional) Enables the **export-stats**, **refresh-rate**, **sampler** and **timeout-rate** keywords for configuring Version 9 export options.
export-stats	(Optional) Enables the export of statistics including the total number of flows exported and the total number of packets exported.

sampler	(Optional) When Version 9 export is configured, this keyword enables the export of an option containing a random-sampler configuration, including the sampler ID, sampling mode, and sampling interval for each configured random sampler. **Note** You must have a flow sampler map configured before you can configure the sampler keyword for the **export template options** command.
refresh-rate *packets*	(Optional) Specifies the number of packets that are sent before the configured options records are resent. Range: 1 to 600 packets. The default is 20 packets. **Note** This applies to the **export template options refresh-rate** *packets* command.
timeout-rate *minutes*	(Optional) Specifies the interval (in minutes) that the router will wait after sending the options records before they are sent again. Range: 1 to 3600 minutes. The default is 30 minutes. **Note** This applies to the **export template options timeout-rate** *minutes* command.

Command Default

The default parameters as noted in the Syntax Description table are used.

Command Modes

NetFlow aggregation cache configuration (config-flow-cache)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **export template options export-stats** command requires that the NetFlow Version 9 export format be already configured on the router.

The **export template options sampler** command requires that the NetFlow Version 9 export format and a flow sampler map be already configured on the router.

Examples

The following example shows how to configure a NetFlow accounting protocol-port aggregation cache so that the networking device sends the export statistics (total flows and packets exported) as options data:

```
Router(config)#
ip flow-aggregation cache protocol-port
Router(config-flow-cache)# export template options export-stats
Router(config-flow-cache)# enabled
```

The following example shows how to configure a NetFlow accounting protocol-port aggregation cache to wait until 100 export packets have been sent, or 60 minutes have passed since the last time the templates were sent (whichever comes first) before the templates are resent to the destination host:

```
Router(config)#
ip flow-aggregation cache protocol-port
Router(config-flow-cache)# export template refresh-rate 100
Router(config-flow-cache)# export template timeout-rate 60
Router(config-flow-cache)# enabled
```

The following example shows how to configure a NetFlow accounting protocol-port aggregation cache to enable the export of information about NetFlow random samplers:

```
Router(config)#
ip flow-aggregation cache protocol-port
Router(config-flow-cache)# export template option sampler
Router(config-flow-cache)# enabled
```

Tip You must have a **flow-sampler** map configured before you can configure the sampler keyword for the **ip flow-export template options** command.

Related Commands

Command	Description
export destination	Enables the export of NetFlow accounting information in NetFlow aggregation cache entries to a remote device such as a server running an application that analyzes NetFlow data.
export version	Specifies the export version format for the exporting of NetFlow accounting information in NetFlow aggregation cache entries
show ip flow export	Displays the status and the statistics for NetFlow accounting data export.

export version

To specify the version of the export format of NetFlow accounting information from NetFlow aggregation caches, use the **export version**command in NetFlow aggregation cache configuration mode. To return to the default behavior, use the **no** form of this command.

export version {**8** | **9**}

no export version

Syntax Description

version {**8**| **9**}	Version of the format for NetFlow data export.

Command Default

Version 9 is the default format for the exporting of NetFlow accounting information from NetFlow aggregation caches.

Command Modes

NetFlow aggregation cache configuration (config-flow-cache)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.4(4)T	The **sctp** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

NetFlow aggregation caches export data in UDP datagrams using either the Version 9 or Version 8 export format.

The table below describes how to determine the most appropriate export format for your requirements.

Table 2 Selecting a NetFlow Export Format

Export Format	Select When...
Version 9	You need a flexible and extensible format, which provides the versatility needed for support of new fields and record types. This format accommodates new NetFlow-supported technologies such as Multicast, IPv6 NetFlow, Egress NetFlow, NetFlow Layer 2 and security exports, Multiprotocol Label Switching (MPLS), and Border Gateway Protocol (BGP) next hop. Version 9 export format enables you to use the same version for main and aggregation caches, and because the format is extensible you can use the same export format with future features.
Version 8	Version 8 export format is available only for export from aggregation caches. Use Version 8 when your NetFlow Collection Engine (NFC) does not support Version 9.

The **export version** command supports two export data formats: Version 8, and Version 9. Version 8 should be used only when it is the only NetFlow data export format version that is supported by the application that you are using to analyze the exported NetFlow data. Version 9 is the only flexible export format version.

The NetFlow Version 9 Export Format feature was introduced in Cisco IOS Release 12.0(24)S and was integrated into Cisco IOS Release 12.3(1) and Cisco IOS Release 12.2(18)S.

NetFlow Version 9 is a flexible and extensible means for transferring NetFlow records from a network node to a collector. NetFlow Version 9 has definable record types and is self-describing for easier NetFlow Collection Engine configuration.

Third-party business partners who produce applications that provide NetFlow Collection Engine or display services for NetFlow do not need to recompile their applications each time a new NetFlow technology is added. Instead, with the NetFlow Version 9 Export Format feature, they can use an external data file that documents the known template formats and field types.

NetFlow Version 9 has the following characteristics:

- Record formats are defined by templates.
- Template descriptions are communicated from the router to the NetFlow Collection Engine.
- Flow records are sent from the router to the NetFlow Collection Engine with minimal template information so that the NetFlow Collection Engine can relate the records to the appropriate template.

Version 9 is independent of the underlying transport (UDP, TCP, SCTP, and so on).

Note In order for the BGP information to be populated in the main cache, you must have either a NetFlow export destination configured or a NetFlow aggregation configured.

Note The AS values for the **peer-as** and the **origin-as** keywords are captured only if you have configured an export destination with the **ip flow-export destination** command.

Note The AS values for the **peer-as** and the **origin-as** keywords are captured only if you have configured an export destination with the **ip flow-export destination** command.

For more information on the available export data formats, see the *Cisco IOS NetFlow Configuration Guide*, Release 12.4T. For more information on the Version 9 data format, see the *Cisco IOS NetFlow Version 9 Export Format Feature Guide* .

Examples

The following example shows how to configure version 9 as the export format for a NetFlow accounting protocol-port aggregation cache scheme:

```
Router(config)#
ip flow-aggregation cache protocol-port
Router(config-flow-cache)# export version 9
Router(config-flow-cache)# enabled
```

Related Commands

Command	Description
export destination	Enables the export of NetFlow accounting information in NetFlow aggregation cache entries to a remote device such as a server running an application that analyzes NetFlow data.
export template	Configures template options for the export of NetFlow accounting information in NetFlow aggregation cache entries
show ip flow export	Displays the status and the statistics for NetFlow accounting data export.

flow hardware mpls-vpn ip

To ensure the creation and export of hardware NetFlow cache entries for traffic entering the router on the last MPLS hop of an IPv4 MPLS VPN network, use the flow **hardware mpls-vpn ip** command in global configuration mode. To disable the creation and export of hardware NetFlow cache entries for this traffic, use the **no** form of this command.

flow hardware mpls-vpn ip *vrf-id*

no flow hardware mpls-vpn ip *vrf-id*

Syntax Description

vrf-id	The name of a VRF that you have previously configured.

Command Default

Creation and export of hardware NetFlow cache entries for traffic entering the router on the last MPLS hop of an IPv4 MPLS VPN network is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

NetFlow Aggregation

If you want to include IPV4 MPLS VPN traffic in a NetFlow aggregation scheme on your router, you must configure the **flow hardware mpls-vpn ip** command.

NetFlow Sampling

If you want to include IPV4 MPLS VPN traffic in the traffic that is analyzed using NetFlow sampling on your router, you must configure the **flow hardware mpls-vpn ip** command.

Examples

The following example configures NDE for VRF vpn1:

```
Router(config)# flow hardware mpls-vpn ip vpn1
```

Related Commands

Command	Description
show mls netflow ip	Displays information about the hardware NetFlow IP flows.

flow-sampler

To apply a flow sampler map for random sampled NetFlow accounting to an interface, use the **flow-sampler**command in interface configuration mode. To remove a flow sampler map for random sampled NetFlow accounting from an interface, use the **no**form of this command.

flow-sampler *sampler-map-name* [**egress**]

no flow-sampler *sampler-map-name* [**egress**]

Syntax Description

sampler-map-name	Name of the flow sampler map to apply to the interface.
egress	(Optional) Specifies that the sampler map is to be applied to egress traffic.

Command Default

Flow sampler maps for NetFlow accounting are not applied to interfaces by default.

Command Modes

Interface configuration Subinterface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.3(11)T	NetFlow egress support was added.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You must create and enable the random sampler NetFlow map for random sampled NetFlow accounting using the **flow-sampler-map** and **mode** commands before you can use the **flow-sampler** command to apply the random sampler NetFlow map to an interface.

Random sampled NetFlow accounting cannot be run concurrently with (ingress) NetFlow accounting, egress NetFlow accounting, or NetFlow accounting with input filter sampling on the same interface, or subinterface. You must disable ingress NetFlow accounting, egress NetFlow accounting, or NetFlow accounting with input filter sampling on the interface, or subinterface, if you want to enable random sampled NetFlow accounting on the interface, or subinterface.

You must enable either Cisco Express Forwarding (CEF) or distributed CEF (dCEF) before using this command.

Tip If you disable CEF or DCEF globally using the **no ip cef [distributed]** command the **flow-sampler** *sampler-map-name* command is removed from any interfaces that you previously configured for random sampled NetFlow accounting. You must reenter the **flow-sampler** *sampler-map-name* command after you reenable CEF or dCEF to reactivate random sampled NetFlow accounting.

Tip If your router is running Cisco IOS release 12.2(14)S or a later release, or Cisco IOS Release 12.2(15)T or a later release, NetFlow accounting might be enabled through the use of the **ip flow ingress** command instead of the **ip route-cache flow** command. If your router has NetFlow accounting enabled through the use of **ip flow ingress** command you must disable NetFlow accounting, using the **no** form of this command, before you apply a random sampler map for random sampled NetFlow accounting on an interface otherwise the full, un-sampled traffic will continue to be seen.

Examples

The following example shows how to create and enable a random sampler map for random sampled (ingress) NetFlow accounting with CEF switching on Ethernet interface 0/0:

```
Router(config)# ip cef
Router(config)# flow-sampler-map my-map
Router(config-sampler)# mode random one-out-of 100
Router(config-sampler)# interface ethernet 0/0
Router(config-if)# no ip route-cache flow
Router(config-if)# ip
 route-cache cef
Router(config-if)# flow-sampler my-map
```

The following example shows how to create and enable a random sampler map for random sampled egress NetFlow accounting with CEF switching on Ethernet interface 1/0:

```
Router(config)# ip cef
Router(config)# flow-sampler-map my-map
Router(config-sampler)# mode random one-out-of 100
Router(config-sampler)# interface ethernet 1/0
Router(config-if)# no
 ip flow egress
Router(config-if)# ip
 route-cache cef
Router(config-if)# flow-sampler my-map egress
```

The following output from the **show flow-sampler** command verifies that random sampled NetFlow accounting is active:

```
Router# show flow-sampler
```

```
Sampler : my-map, id : 1, packets matched : 7, mode : random sampling mode
 sampling interval is : 100
```

Related Commands

Command	Description
flow-sampler-map	Defines a flow sampler map for random sampled NetFlow accounting.
mode (flow sampler configuration)	Specifies a packet interval for NetFlow accounting random sampling mode and enables the flow sampler map.
netflow-sampler	Enables NetFlow accounting with input filter sampling.
show flow-sampler	Displays the status of random sampled NetFlow (including mode, packet interval, and number of packets matched for each flow sampler).
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

flow-sampler-map

To define a flow sampler map for random sampled NetFlow accounting, use the **flow-sampler-map**command in global configuration mode. To remove a flow sampler map for random sampled NetFlow accounting, use the **no** form of this command.

flow-sampler-map *sampler-map-name*

no flow-sampler-map *sampler-map-name*

Syntax Description

sampler-map-name	Name of the flow sampler map to be defined for random sampled NetFlow accounting.

Command Default

No flow sampler maps for random sampled NetFlow accounting are defined.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Random sampled NetFlow accounting does not start sampling traffic until (1) the random sampler map is activated through the use of the **mode** command and (2) the sampler map has been applied to an interface through the use of the **flow-sampler** command.

Random Sampled NetFlow accounting cannot be run concurrently with (ingress) NetFlow accounting, egress NetFlow accounting, or NetFlow accounting with input filter sampling on the same interface, or

subinterface. You must disable (ingress) NetFlow accounting, egress NetFlow accounting, or NetFlow accounting with input filter sampling on the interface or subinterface, if you want to enable random sampled NetFlow accounting on that interface or subinterface.

You must enable either Cisco Express Forwarding (CEF) or distributed CEF (dCEF) before using this command.

Tip If you disable dCEF globally using the **no ip cef [distributed]** command, the **flow-sampler** *sampler-map-name* command is removed from any interfaces that you previously configured for random sampled NetFlow accounting. You must reenter the **flow-sampler** *sampler-map-name* command after you reenable CEF or dCEF to reactivate random sampled NetFlow accounting.

Tip If your router is running Cisco IOS release 12.2(14)S or a later release, or Cisco IOS Release 12.2(15)T or a later release, NetFlow accounting might be enabled through the use of the **ip flow ingress** command instead of the **ip route-cache flow** command. If your router has NetFlow accounting enabled through the use of **ip flow ingress** command you must disable NetFlow accounting, using the **no** form of this command, before you apply a random sampler map for random sampled NetFlow accounting on an interface otherwise the full, un-sampled traffic will continue to be seen.

Examples

The following example shows how to create and enable a random sampler map for random sampled (ingress) NetFlow accounting with CEF switching on Ethernet interface 0/0:

```
Router(config)# ip cef
Router(config)# flow-sampler-map my-map
Router(config-sampler)# mode random one-out-of 100
Router(config-sampler)# interface ethernet 0/0
Router(config-if)# no ip route-cache flow
Router(config-if)# ip
 route-cache cef
Router(config-if)# flow-sampler my-map
```

The following example shows how to create and enable a random sampler map for random sampled egress NetFlow accounting with CEF switching on Ethernet interface 1/0:

```
Router(config)# ip cef
Router(config)# flow-sampler-map my-map
Router(config-sampler)# mode random one-out-of 100
Router(config-sampler)# interface ethernet 1/0
Router(config-if)# no
 ip flow egress
Router(config-if)# ip
 route-cache cef
Router(config-if)# flow-sampler my-map egress
```

The following output from the **show flow-sampler** command verifies that random sampled NetFlow accounting is active:

```
Router# show flow-sampler

 Sampler : my-map, id : 1, packets matched : 7, mode : random sampling mode
  sampling interval is : 100
```

Related Commands

Command	Description
flow-sampler-map	Defines a flow sampler map for random sampled NetFlow accounting.
mode (flow sampler configuration)	Specifies a packet interval for NetFlow accounting random sampling mode and enables the flow sampler map.
netflow-sampler	Enables NetFlow accounting with input filter sampling.
show flow-sampler	Displays the status of random sampled NetFlow (including mode, packet interval, and number of packets matched for each flow sampler).
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

ip flow

To enable NetFlow accounting for inbound (received) or outbound (transmitted) network traffic, use the **ip flow**command in interface or subinterface configuration mode. To disable NetFlow accounting, use the **no** form of this command.

ip flow {**ingress** | **egress**}

no ip flow {**ingress** | **egress**}

Syntax Description

ingress	Enables NetFlow accounting for traffic that is received on an interface. **Note** This is also known as ingress NetFlow accounting.
egress	Enables NetFlow accounting for traffic that is transmitted on an interface. **Note** This is also known as egress NetFlow accounting.

Command Default

NetFlow accounting is disabled.

Command Modes

Interface configuration (config-if) Subinterface configuration (config-sub-if)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(25)S	Output of the **show running configuration** command was modified so that the **ip route-cache flow**command as well as the **ip flow ingress** command will appear when either command is configured.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(11)T	The egress keyword was added.

Release	Modification
12.2(28)SBB	This command was integrated into Cisco IOS Release 12.2(27)SBB and implemented for the Cisco 10000 series routers.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF. This command was changed to allow you to dynamically create NetFlow entries on a 7600.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Cisco 7600 Series Platforms

The **ip flow ingress**command is supported on the Supervisor Engine 720 in PFC3B and PFC3BXL mode.

The **ip flow ingress**command is supported on the Supervisor Engine 2 with a PFC2.

In Release 12.2(18)SXF and later releases, to create a NetFlow entry, you need to enter the **ip flow ingress** command. In releases prior to Release 12.2(18)SXF, the NetFlow entries are created automatically.

Other Platforms

Use this command on an interface or subinterface to enable NetFlow accounting for traffic.

You must enable CEF or dCEF globally on the networking device, and on the interface or subinterface that you want to enable NetFlow accounting on before you enable either ingress or egress NetFlow accounting.

Examples

The following example shows how to configure ingress NetFlow accounting for traffic that is received on FastEthernet interface 0/0:

```
Router(config)# interface fastethernet0/0
Router(config-if)# ip flow ingress
```

The following example shows how to configure egress NetFlow accounting for traffic that is transmitted on FastEthernet interface 0/0:

```
Router(config)# interface fastethernet0/0
Router(config-if)# ip flow egress
```

Related Commands

Command	Description
ip flow-egress input-interface	Removes the NetFlow egress accounting flow key that specifies an output interface and adds a flow key that specifies an input interface for NetFlow egress accounting.
ip flow-cache timeout	Specifies NetFlow accounting flow cache parameters
ip flow-cache entries	Changes the number of entries maintained in the NetFlow accounting cache.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

ip flow layer2-switched

To enable the creation of switched, bridged, and Layer 2 IP flows for a specific VLAN, use the **ip flow layer2-switched** command in global configuration mode. Use the **no** form of this command to return to the default settings.

ip flow {**ingress** | **export**} **layer2-switched vlan** {*num* | *vlanlist*}

no ip flow {**ingress** | **export**} **layer2-switched vlan** {*num* | *vlanlist*}

Syntax Description

ingress	Enables the collection of switched, bridged, and IP flows in Layer 2.
export	Enables the export of switched, bridged, and IP flows in Layer 2.
vlan *num* | *vlanlist*	Specifies the VLAN or range of VLANs; valid values are from 1 to 4094. See the "Usage Guidelines" section for additional information.

Command Default

The defaults are as follows:

- **ip flow ingress layer2switch** is disabled.
- **ip flow export layer2switched** is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **ip flow layer2-switched**command is supported on the Supervisor Engine 720 in PFC3B and PFC3BXL mode only.

The **ip flow layer2-switched**command is supported on the Supervisor Engine 2 with a PFC2.

Before using this command on Cisco 7600 series routers that are configured with a Supervisor Engine 720, you must ensure that a corresponding VLAN interface is available and has a valid IP address. This guideline does not apply to Cisco 7600 series routers that are configured with a Supervisor Engine 2.

You can enter one or multiple VLANs. The following examples are samples of valid VLAN lists: 1; 1,2,3; 1-3,7.

Examples

This example shows how to enable the collection of Layer 2-switched flows on a specific VLAN:

```
Router(config)# ip flow ingress layer2-switched vlan 2
Router(config)#
```

This example shows how to enable export of Layer 2-switched flows on a range of VLANs:

```
Router(config)# ip flow export layer2-switched vlan 1-3,7
Router(config)#
```

This example shows how to disable the collection of Layer 2-switched flows on a specific VLAN:

```
Router(config)# no ip flow ingress layer2-switched vlan 2
Router(config#
```

ip flow-aggregation cache

To enable NetFlow accounting aggregation cache schemes, use the **ip flow-aggregation cache**command in global configuration mode. To disable NetFlow accounting aggregation cache schemes, use the **no** form of this command.

ip flow-aggregation cache {**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** | **exp-bgp-prefix**}

no ip flow-aggregation cache {**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** | **exp-bgp-prefix**}

Syntax Description

as	Configures the autonomous system aggregation cache scheme.
as-tos	Configures the autonomous system type of service (ToS) aggregation cache scheme.
bgp-nexthop-tos	Configures the Border Gateway Protocol (BGP) next hop ToS aggregation cache scheme. **Note** This keyword is not supported on the Cisco ASR 1000 Series Aggregation Services Router.
destination-prefix	Configures the destination-prefix aggregation cache scheme.
destination-prefix-tos	Configures the destination prefix ToS aggregation cache scheme.
prefix	Configures the prefix aggregation cache scheme.
prefix-port	Configures the prefix port aggregation cache scheme.
prefix-tos	Configures the prefix ToS aggregation cache scheme.
protocol-port	Configures the protocol-port aggregation cache scheme.
protocol-port-tos	Configures the protocol-port ToS aggregation cache scheme.
source-prefix	Configures the source-prefix aggregation cache scheme.

source-prefix-tos	Configures the source-prefix ToS aggregation cache scheme.
exp-bgp-prefix	Configures the exp-bgp-prefix aggregation cache scheme.

Command Default

This command is not enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.0(15)S	This command was modified to include the ToS aggregation scheme keywords.
12.2(2)T	This command was modified to enable multiple NetFlow export destinations.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(1)	Support for the BGP Next Hop Support feature was added.
12.2(18)S	Support for the BGP Next Hop Support feature was added.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. The **exp-bgp-prefix** aggregation cache keyword was added.

Usage Guidelines

You must have NetFlow accounting configured on your router before you can use this command. The **export destination** command supports a maximum of two concurrent export destinations.

The ToS aggregation cache scheme keywords enable NetFlow accounting aggregation cache schemes that include the ToS byte in their export records. The ToS byte is an 8-bit field in the IP header. The ToS byte specifies the quality of service for a datagram during its transmission through the Internet.

You can enable only one aggregation cache configuration scheme per command line. The following rules apply to configuring source and destination masks.

- The source mask can only be configured in the prefix, prefix-port, prefix-tos, source-prefix and source-prefix-tos aggregation modes.
- The destination mask can only be configured in the prefix, prefix-port, prefix-tos, destination-prefix and destination-prefix-tos aggregation modes.
- No masks can be configured in non-prefix aggregation modes

To enable aggregation (whether or not an aggregation cache is fully configured), you must enter the **enabled** command in aggregation cache configuration mode. (You can use the **no** form of this command to disable aggregation. The cache configuration remains unchanged even if aggregation is disabled.)

Examples

The following example shows how to configure a NetFlow accounting autonomous system aggregation cache scheme:

```
Router(config)# ip flow-aggregation cache as
Router(config-flow-cache)# enabled
```

The following example shows how to configure a minimum prefix mask of 16 bits for the NetFlow accounting destination-prefix aggregation cache scheme:

```
Router(config)# ip flow-aggregation cache destination-prefix
Router(config-flow-cache)# mask destination minimum 16
Router(config-flow-cache)# enabled
```

The following example shows how to configure a minimum prefix mask of 16 bits for the NetFlow accounting source-prefix aggregation cache scheme:

```
Router(config)# ip flow-aggregation cache source-prefix
Router(config-flow-cache)# mask source minimum 16
Router(config-flow-cache)# enabled
```

The following example shows how to configure multiple export destinations for the NetFlow accounting autonomous system ToS aggregation cache scheme:

```
Router(config)# ip flow-aggregation cache as-tos
Router(config-flow-cache)# export destination 172.17.24.65 9991
Router(config-flow-cache)# export destination 172.16.10.2 9991
Router(config-flow-cache)# enabled
```

Related Commands

Command	Description
export destination (aggregation cache)	Enables the exporting of NetFlow accounting information from NetFlow aggregation caches.
enabled (aggregation cache)	Enables the NetFlow aggregation cache.

Command	Description
mask	Specifies the source or destination prefix mask.
show ip cache flow aggregation	Displays a summary of the NetFlow accounting aggregation cache statistics.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

ip flow-cache entries

To change the number of entries maintained in the NetFlow accounting cache, use the **ip flow-cache entries**command in global configuration mode. To return to the default number of entries, use the **no** form of this command.

ip flow-cache entries *number*

no ip flow-cache entries

Syntax Description

number	Number of entries to maintain in the NetFlow cache. The range is from 1024 to 524288. The default is 4096. **Note** For the Cisco ASR 1000 Series Aggregation Services Router, the range is 1024 to 2000000 (2 million). The default is 200000.

Command Default

The default value of 4096 is used as the size of the NetFlow accounting cache.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

You must have NetFlow accounting configured on your router before you can use this command.

Normally the default size of the NetFlow cache will meet your needs. However, you can increase or decrease the number of entries maintained in the cache to meet the needs of your flow traffic rates. For environments with a high amount of flow traffic (such as an internet core router), a larger value such as 131072 (128K) is recommended. To obtain information on your flow traffic, use the **show ip cache flow** EXEC command.

Each cache entry is approximately 64 bytes of storage. Assuming a cache with the default number of entries, approximately 4 MB of DRAM would be required. Each time a new flow is taken from the free flow queue, the number of free flows is checked. If only a few free flows remain, NetFlow attempts to age 30 flows using an accelerated timeout. If only one free flow remains, NetFlow automatically ages 30 flows regardless of their age. The intent is to ensure that free flow entries are always available.

Caution We recommend that you not change the number of NetFlow cache entries. To return to the default number of NetFlow cache entries, use the **no ip flow-cache entries** global configuration command.

Examples

The following example shows how to increase the number of NetFlow cache entries to 131,072 (128K):

```
Router(config)# ip flow-cache entries 131072
%The change in number of entries will take effect after either the next reboot or when
netflow is turned off on all interfaces
```

Tip You turn off NetFlow accounting on interfaces by removing the command that you enabled NetFlow accounting with. For example, if you enabled NetFlow accounting on an interface with the **ip flow ingress** command you turn off NetFlow accounting for the interface using the **no** form of the command **-no ip flow ingress**. Remember to turn NetFlow accounting back on for the interface after you have turned it off.

Related Commands

Command	Description
ip flow-cache timeout	Specifies NetFlow accounting flow cache parameters.
ip flow egress	Enables NetFlow egress accounting for traffic that the router is forwarding.

Command	Description
ip flow-egress input-interface	Removes the NetFlow egress accounting flow key that specifies an output interface and adds a flow key that specifies an input interface for NetFlow egress accounting.
ip flow ingress	Enables NetFlow (ingress) accounting for traffic arriving on an interface.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

ip flow-cache mpls label-positions

To enable Multiprotocol Label Switching (MPLS)-Aware NetFlow, use the **ip flow-cache mpls label-positions** command in global configuration mode. To disable MPLS-aware NetFlow, use the **no** form of this command.

ip flow-cache mpls label-positions [*label-position-1* [*label-position-2* [*label-position-3*]]] [**exp-bgp-prefix-fields**] [**no-ip-fields**] [**mpls-length**]

no ip flow-cache mpls label-positions

Syntax Description

label-position-l	(Optional) Position of an MPLS label in the incoming label stack. Label positions are counted from the top of the stack, starting with 1.
exp-bgp-prefix-fields	(Optional) Generates a MPLS Provider Edge (PE) PE-to-PE traffic matrix. The following IP-related flow fields are included: • Input interface • BGP Nexthop • MPLS Experimental (EXP) bits The MPLS label values will be set to zero on the Cisco 10000 in the display output of the **show ip cache verbose flow aggregation exp-bgp-prefix** command.
no-ip-fields	(Optional) Controls the capture and reporting of MPLS flow fields. If the **no-ip-fields** keyword is not specified, the following IP-related flow fields are included: • Source IP address • Destination IP address • Transport layer protocol • Source application port number • Destination application port number • IP type of service (ToS) • TCP flag If the **no-ip-fields** keyword is specified, the IP-related fields are reported with a value of 0.

mpls-length	(Optional) Controls the reporting of packet length. If the **mpls-length** keyword is specified, the reported length represents the sum of the MPLS packet payload length and the MPLS label stack length. If the **mpls-length** keyword is not specified, only the length of the MPLS packet payload is reported.

Command Default

MPLS-Aware NetFlow is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.0(25)S	The **no-ip-fields** and **mpls-length** keywords were added.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. The **exp-bgp-prefix-fields** keyword was added.

Usage Guidelines

You must have NetFlow accounting configured on your router before you can use this command.

Use this command to configure the MPLS-aware NetFlow feature on a label switch router (LSR) and to specify labels of interest in the incoming label stack. Label positions are counted from the top of the stack, starting with 1. The position of the top label is 1, the position of the second label is 2, and so forth.

With MPLS-aware NetFlow enabled on the router, NetFlow collects data for incoming IP packets and for incoming MPLS packets on all interfaces where NetFlow is enabled in full or in sampled mode.

Caution When you enter the **ip flow-cache mpls label-positions** command on a Cisco 12000 series Internet router, NetFlow will stop collecting data for incoming IP packets on any Engine 4P line cards installed in the router on which NetFlow is enabled in full or in sampled mode. Engine 4P line cards in a Cisco 12000 series Internet router do not support NetFlow data collection of incoming IP packets and MPLS packets concurrently.

Tip MPLS-aware NetFlow is enabled in global configuration mode. NetFlow is enabled per interface.

Examples

The following example shows how to configure MPLS-aware NetFlow to capture the first (top), third, and fifth label:

```
Router(config)# ip flow-cache mpls label-positions 1 3 5
```

The following example shows how to configure MPLS-aware NetFlow to capture only MPLS flow information (no IP-related flow fields) and the length that represents the sum of the MPLS packet payload length and the MPLS label stack length:

```
Router(config)# ip flow-cache mpls label-positions no-ip-fields mpls-length
```

The following example shows how to configure MPLS PE-to-PE Traffic Statistics for Netflow:

```
Router(config)# ip flow-cache mpls label-positions 1 2 exp-bgp-prefix-fields
```

Related Commands

Command	Description
ip flow-cache entries	Changes the number of entries maintained in the NetFlow accounting cache.
ip flow-cache timeout	Specifies NetFlow accounting flow cache parameters.
ip flow egress	Enables NetFlow egress accounting for traffic that the router is forwarding.
ip flow-egress input-interface	Removes the NetFlow egress accounting flow key that specifies an output interface and adds a flow key that specifies an input interface for NetFlow egress accounting.
ip flow ingress	Enables NetFlow (ingress) accounting for traffic arriving on an interface.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.

Command	Description
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

ip flow-cache timeout

To specify NetFlow accounting flow cache parameters, use the **ip flow-cache timeout** command in global configuration mode. To disable the flow cache parameters, use the **no** form of this command.

ip flow-cache timeout [**active** *minutes* | **inactive** *seconds*]

no ip flow-cache timeout [**active** | **inactive**]

Syntax Description

active	Specifies the active flow timeout.
minutes	(Optional) The number of minutes that an active flow remains in the cache before it times out. The range is from 1 to 60. The default value is 30.
inactive	Specifies the inactive flow timeout.
seconds	(Optional) The number of seconds that an inactive flow remains in the cache before it times out. The range is from 10 to 600. The default value is 15.

Command Default

The flow-cache timeout values are set to the default values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You must have NetFlow accounting configured on your router before you can use this command.

Use this command to specify active and inactive timeout parameters.

A flow is considered to be active if packets belonging to the flow are detected wherever the NetFlow statistics are being collected. A flow is considered to be inactive if no further packets are detected for the flow at the collection point for NetFlow statistics.

Examples

In the following example, an active flow is allowed to remain in the cache for 20 minutes:

```
Router(config)# ip flow-cache timeout active 20
```

In the following example, an inactive flow is allowed to remain in the cache for 10 seconds before it times out and is removed:

```
Router(config)# ip flow-cache timeout inactive 10
```

Related Commands

Command	Description
ip flow egress	Enables NetFlow (egress) accounting for traffic that the router is forwarding.
ip flow ingress	Enables NetFlow (ingress) accounting for traffic arriving on an interface.
ip flow-cache entries	Changes the number of entries maintained in the NetFlow accounting cache.
ip flow-egress input-interface	Removes the NetFlow egress accounting flow key that specifies an output interface and adds a flow key that specifies an input interface for NetFlow egress accounting.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

ip flow-capture

To enable the capture of values from Layer 2 or additional Layer 3 fields in NetFlow traffic, use the **ip flow-capture** command in global configuration mode. To disable capturing Layer 2 or Layer 3 fields from NetFlow traffic, use the **no** form of this command.

ip flow-capture {**fragment-offset** | **icmp** | **ip-id** | **mac-addresses** | **packet-length** | **ttl** | **vlan-id** | **nbar**}

no ip flow-capture {**fragment-offset** | **icmp** | **ip-id** | **mac-addresses** | **packet-length** | **ttl** | **vlan-id** | **nbar**}

Syntax Description

fragment-offset	Captures the value of the 13-bit IP fragment offset field from the first fragmented IP datagram in a flow.
icmp	Captures the value of the ICMP type and code fields from the first ICMP datagram in a flow.
ip-id	Captures the value of the IP-ID field from the first IP datagram in a flow.
mac-addresses	Captures the values of the source MAC addresses from ingress packets and the destination MAC addresses from egress packets from the first packet in a flow. **Note** This command applies only to traffic that is received or transmitted over Ethernet interfaces.
packet-length	Captures the value of the packet length field from IP datagrams in a flow.
ttl	Captures the value of the time-to-live (TTL) field from IP datagrams in a flow.
vlan-id	Captures the value of the 802.1q or Inter-Switch Link (ISL) VLAN-ID field from VLAN-encapsulated frames in a flow when the frames are received or transmitted on trunk ports.
nbar	Exports Network Based Application Recognition (NBAR) information along with the NetFlow Version 9 record.

Command Default

Values from Layer 2 and Layer 3 fields are not captured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(2)T	The **fragment-offset** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)ZYA2	This command was modified. The **nbar** keyword was added.

Usage Guidelines

You must enable NetFlow accounting on an interface or a subinterface using the **ip flow** {**ingress** | **egress**} command for the **ip flow-capture** command to take effect. You can enable NetFlow accounting before or after you have entered the **ip flow-capture** command in global configuration mode.

If you want to export the information captured by the **ip flow-capture**command, you must configure NetFlow export using the **ip flow-export destination** command, and you must configure NetFlow to use the Version 9 export format. Use the **ip flow-export version 9** command to configure the NetFlow Version 9 export format.

The fields captured by the **ip flow-capture**command are currently not available in the NetFlow MIB.

Note You can capture the value from only one field at a time. Execute the command once for each value you want to capture.

ip flow-capture fragment-offset

IP fragmentation occurs when the size of an IP datagram exceeds the maximum transmission unit (MTU) of the Layer 2 frame type used by the next-hop network. For example, the IP MTU size of an ATM network is 4470 bytes. When a host needs to transmit an IP datagram that exceeds 4470 bytes on an ATM network, it must first fragment the datagram into two or more smaller IP datagrams.

An IP datagram sent by a host system such as a web server can also be fragmented by a router in the network if the router needs to transmit the IP datagram on a next-hop network that has an MTU that is smaller than the current size of the IP datagram. For example, if a router receives a 4470-byte IP datagram on an ATM interface and the next-hop network is a 100-Mbps Fast Ethernet network with an MTU of 1514, the router must fragment the IP datagram into three smaller IP datagrams (4470/1514). It is possible for an IP datagram to be fragmented two or more times on its path from the sending host to the destination host.

A fragmented IP datagram is reassembled by the destination host. The last fragment of an IP datagram is identified when the “more fragments” flag is set to 0. The length of a complete IP datagram is calculated by the receiving host by means of the fragment offset field and the length of the last fragment.

The **ip flow-capture fragment-offset**command captures the value of the IP fragment offset field from the first fragmented IP packet in the flow. If you are seeing several flows with the same value for the IP fragment offset field, it is possible that your network is being attacked by a host that is sending the same IP packets again and again.

ip flow-capture icmp

Internet Control Message Protocol (ICMP) is used for several purposes. One of the most common is the ping command. ICMP echo requests are sent by a host to a destination to verify that the destination is reachable by IP. If the destination is reachable, it should respond by sending an ICMP echo reply. Refer to RFC 792, *Darpa Internet Program Protocol Specification* (http://www.ietf.org/rfc/rfc0792.txt?number=792) for more information on ICMP.

ICMP packets have been used in many types of attacks on networks. Two of the most common attacks are the denial-of-service (DoS) attack and the “ping of death” attack.

- DoS attack--Any action or actions that prevent any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized delay of service. Generally, DoS attacks do not destroy data or resources, but prevent access or use. In network operations, flooding a device with ping packets when the device has not been configured to block or ignore them might effect a denial of service.
- “ping of death”--An attack that sends an improperly large ping echo request packet with the intent of overflowing the input buffers of the destination machine and causing it to crash.

Finding out the types of ICMP traffic in your network can help you decide if your network is being attacked by ICMP packets.

The **ip flow-capture icmp** command captures the value of the ICMP type field and the ICMP code field from the first ICMP packet detected in a flow.

ip flow-capture ip-id

It is possible for a host to receive IP datagrams from two or more senders concurrently. It is also possible for a host to receive multiple IP datagrams from the same host for different applications concurrently. For example, a server might be transferring email and HTTP traffic from the same host concurrently. When a host is receiving multiple IP datagrams concurrently, it must be able to identify the fragments from each of the incoming datagrams to ensure that they do not get mixed up during the datagram reassembly process. The receiving host uses the IP header identification field and the source IP address of the IP datagram fragment to ensure that it rebuilds the IP datagrams correctly.

The **ip flow-capture ip-id** command captures the value of the IP header identification field from the first packet in the flow. The value in the IP header identification field is a sequence number assigned by the host that originally transmitted the IP datagram. All of the fragments of an IP datagram have the same identifier value. This ensures that the destination host can match the IP datagram to the fragment during the IP datagram reassembly process. The sending host is responsible for ensuring that each subsequent IP datagram it sends to the same destination host has a unique value for the IP header identification field.

If you are seeing several flows with the same value for the IP header identification field, it is possible that your network is being attacked by a host that is sending the same IP packets again and again.

ip flow-capture packet-length

The value in the packet length field in an IP datagram indicates the length of the IP datagram, excluding the IP header.

Use the **ip flow-capture packet-length** command to capture the value of the IP header packet length field for packets in the flow. The **ip flow-capture packet-length** command keeps track of the minimum and maximum values captured from the flow. The minimum and maximum packet length values are stored in separate fields. This data is updated when a packet with a packet length that is lower or higher than the currently stored value is received. For example, if the currently stored value for the minimum packet length is 1024 bytes and the next packet received has a packet length of 512 bytes, the 1024 is replaced by 512.

If you are seeing several IP datagrams in the flow with the same value for the packet-length field, it is possible that your network is being attacked by a host that is constantly sending the same IP packets again and again.

ip flow-capture ttl

The TTL field is used to prevent the indefinite forwarding of IP datagrams. The TTL field contains a counter value set by the source host. Each router that processes this datagram decreases the TTL value by 1. When the TTL value reaches 0, the datagram is discarded.

There are two scenarios where an IP packet without a TTL field could live indefinitely in a network:

- The first scenario occurs when a host sends an IP datagram to an IP network that does not exist and the routers in the network have a gateway of last resort configured--that is, a gateway to which they forward IP datagrams for unknown destinations. Each router in the network receives the datagram and attempts to determine the best interface to use to forward it. Because the destination network is unknown, the best interface for the router to use to forward the datagram to the next hop is always the interface to which the gateway of last resort is assigned.
- The second scenario occurs when a wrong configuration in the network results in a routing loop. For example, if one router forwards an IP datagram to another router because it appears to be the correct next-hop router, then the receiving router sends it back because it believes that the correct next-hop router is the router that it received the IP datagram from in the first place.

The **ip flow-capture ttl** command keeps track of the TTL values captured from packets in the flow. The minimum and maximum TTL values are stored in separate fields. This data is updated when a packet with a TTL that is lower or higher than the currently stored value is received. For example if the currently stored value for the minimum TTL is 64 and the next packet received has a TTL of 12, the 64 is replaced by 12.

If you are seeing several flows with the same value for the TTL, it is possible that your network is being attacked by a host that is constantly sending the same IP packets again and again. Under normal circumstances, flows come from many sources, each a different distance away. Therefore you should see a variety of TTLs across all the flows that NetFlow is capturing.

ip flow-capture mac-addresses

Note This command applies only to the traffic that is received or transmitted over Ethernet interfaces.

The **ip flow-capture mac-addresses** command captures the MAC addresses of the incoming source and the outgoing destination from the first Layer 2 frame in the flow. If you discover that your network is attacked by Layer 3 traffic, use these addresses to identify the device that transmits the traffic received by the router and the next-hop or final destination device to which the router forwards the traffic.

ip flow-capture vlan-id

A virtual LAN (VLAN) is a broadcast domain within a switched network. A broadcast domain is defined by the network boundaries within which a network propagates a broadcast frame generated by a station. Some switches can be configured to support single or multiple VLANs. Whenever a switch supports multiple VLANs, broadcasts within one VLAN never appear in another VLAN.

Each VLAN is also a separate Layer 3 network. A router or a multilayer switch must be used to interconnect the Layer 3 networks that are assigned to the VLANs. For example, a device on VLAN 2 with an IP address of 172.16.0.76 communicating with a device on VLAN 3 with an IP address of 172.17.0.34 must use a router as an intermediary device because they are on different Class B IP networks. This is accomplished by connecting a switch to a router and configuring the link between them as a VLAN trunk. In order for the link to be used as a VLAN trunk, the interfaces on the router and the switch must be configured for the same VLAN encapsulation type.

Note When a router is configured to route traffic between VLANs, it is often referred to as an inter-VLAN router.

When a router or a switch needs to send traffic on a VLAN trunk, it must either tag the frames using the IEEE 802.1q protocol or encapsulate the frames using the Cisco Inter-Switch Link (ISL) protocol. The VLAN tag or encapsulation header must contain the correct VLAN ID to ensure that the device receiving the frames can process them properly. The device that receives the VLAN traffic examines the VLAN ID from each frame to find out how it should process the frame. For example, when a switch receives an IP broadcast datagram such as an Address Resolution Protocol (ARP) datagram with an 802.1q tagged VLAN ID of 6 from a router, it forwards the datagram to every interface that is assigned to VLAN 6 and any interfaces that are configured as VLAN trunks.

The **ip flow-capture vlan-id**command captures the VLAN ID number from the first frame in the flow it receives that has an 802.1q tag or that is encapsulated with ISL. When the received traffic in the flow is transmitted over an interface that is configured with either 802.1q or ISL trunking, the **ip flow-capture vlan-id**command captures the destination VLAN ID number from the 802.1q or ISL VLAN header from the first frame in the flow.

Note The **ip flow-capture vlan-id**command does not capture the type of VLAN encapsulation in use. The receiving and transmitting interfaces can use different VLAN protocols. If only one of the interfaces is configured as a VLAN trunk, the VLAN ID field is blank for the other interface.

Your router configuration must meet the following criteria before NetFlow can capture the value in the VLAN-ID field:

- It must have at least one LAN interface that is configured with one or more subinterfaces.
- The subinterfaces where you want to receive VLAN traffic must have either 802.1q or ISL enabled.
- The subinterfaces that are configured to receive VLAN traffic must have the **ip flow ingress** command configured on them.

If you discover that your network is being attacked by Layer 3 traffic, you can use the VLAN-ID information to help you find out which VLAN the device that is sending the traffic is on. The information can also help you identify the VLAN to which the router is forwarding the traffic.

ip flow-capture nbar

The **ip flow-capture nbar** command captures the application IDs and subapplication IDs exported as part of the NetFlow Version 9 record. The application IDs are mapped to applications. By means of the **ip flow-export template options nbar** command, this mapping information is exported to the NetFlow data collector. To capture Network Based Application Recognition (NBAR) information, you must enable NetFlow Version 9.

Note The subapplication ID value is always 0 in current release.

Examples

The following example shows how to configure NetFlow to capture the value of the IP fragment-offset field from the IP datagrams in the flow:

```
Router(config)# ip flow-capture fragment-offset
```

The following example shows how to configure NetFlow to capture the value of the ICMP type field and the value of the code field from the IP datagrams in the flow:

```
Router(config)# ip flow-capture icmp
```

The following example shows how to configure NetFlow to capture the value of the IP-ID field from the IP datagrams in the flow:

```
Router(config)# ip flow-capture ip-id
```

The following example shows how to configure NetFlow to capture the value of the packet length field from the IP datagrams in the flow:

```
Router(config)# ip flow-capture packet-length
```

The following example shows how to configure NetFlow to capture the TTL field from the IP datagrams in the flow:

```
Router(config)# ip flow-capture ttl
```

The following example shows how to configure NetFlow to capture the MAC addresses from the IP datagrams in the flow:

```
Router(config)# ip flow-capture mac-addresses
```

The following example shows how to configure NetFlow to capture the VLAN ID from the IP datagrams in the flow:

```
Router(config)# ip flow-capture vlan-id
```

The following example shows how to configure NetFlow to capture NBAR information:

```
Router(config)# ip flow-capture nbar
```

Related Commands

Command	Description
ip flow-cache entries	Changes the number of entries maintained in the NetFlow accounting cache.
ip flow-cache timeout	Specifies NetFlow accounting flow cache parameters.
ip flow egress	Enables NetFlow egress accounting for traffic that the router is forwarding.
ip flow-egress input-interface	Removes the NetFlow egress accounting flow key that specifies an output interface and adds a flow key that specifies an input interface for NetFlow egress accounting.

Command	Description
ip flow-export template options nbar	Exports application mapping information to the NetFlow data collector.
ip flow ingress	Enables NetFlow ingress accounting for traffic arriving on an interface.
show ip cache flow	Displays a summary of NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow export	Displays the status and the statistics for NetFlow accounting data export.
show ip flow interface	Displays the NetFlow accounting configuration for interfaces.

ip flow-egress input-interface

To remove the NetFlow egress accounting flow key that specifies an output interface and to add a flow key that specifies an input interface for NetFlow egress accounting, use the **ip flow-egress input-interface** command in global configuration mode. To change the flow key back from an input interface to an output interface for NetFlow egress statistics, use the **no** form of this command.

ip flow-egress input-interface

no ip flow-egress input-interface

Syntax Description

This command has no arguments or keywords.

Command Default

By default NetFlow egress statistics use the output interface as part of the flow key.

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You must have NetFlow egress accounting configured on your router before you can use this command.

When the NetFlow Egress Support feature is configured, by default it uses the output interface as part of the flow key. The **ip flow-egress input-interface**command changes the key for egress flows so that the ingress interface is used instead of the output interface. This command is used to create a new flow for each input interface.

Examples

In the following example the key for NetFlow reporting of egress traffic is changed from the output interface to the input interface:

```
Router(config)# ip flow-egress input-interface
```

Related Commands

Command	Description
ip flow ingress	Enables NetFlow (ingress) accounting for traffic arriving on an interface.
ip flow egress	Enables NetFlow egress accounting for traffic that the router is forwarding.
ip flow-cache timeout	Specifies NetFlow accounting flow cache parameters.
ip flow-cache entries	Changes the number of entries maintained in the NetFlow accounting cache.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

ip flow-export destination

To enable the export of NetFlow accounting information in NetFlow cache entries to a remote device such as a server running an application that analyzes NetFlow data, use the **ip flow-export destination** command in global configuration mode. To remove an export destination, use the noform of this command.

ip flow-export destination {*hostname* | *ip-address*} *port* [**udp**] [**vrf** *vrf-name*]

no ip flow-export destination {*hostname* | *ip-address*} *port* [**udp**] [**vrf** *vrf-name*]

Syntax Description

ip-address | *hostname*	IP address or hostname of the workstation to which you want to send the NetFlow information
port	Specifies the number of the user datagram protocol (UDP) port on which the workstation is listening for the exported NetFlow datagrams.
vrf *vrf-name*	(Optional) The **vrf** keyword specifies that the export data packets are to be sent to the named Virtual Private Network (VPN) routing forwarding instance (VRF) for routing to the destination, instead of to the global routing table. **Note** The *vrf-name* argument is the name of the VRF.
udp	(Optional) Specifies UDP as the transport protocol. UDP is the default transport protocol.

Command Default

Export of NetFlow information is disabled.

Command Modes

Global configuration (config)#

Command History

Release	Modification
11.1 CA	This command was introduced.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S, and support for the Multiple Export Destinations feature was added.

Release	Modification
12.2(2)T	This command was modified to enable multiple NetFlow export destinations to be used.
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(18)SXD	This command was changed to allow you to configure multiple NetFlow export destinations to a router.
12.2(18)SXE	This command was changed to allow you to enter two destination IP addresses on the Supervisor Engine 720 only. See the “Usage Guidelines” section for more information.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.4(4)T	The **vrf** keyword and *vrf name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS Release XE 2.6.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4. The **vrf** keyword and *vrf name* argument were added.

Usage Guidelines

Cisco Catalyst 6500 Series Switches

With a PFC3 and Release 12.2(18)SXE and later releases, you can enter multiple NetFlow export destinations on the Supervisor Engine 720 only.

Multiple Export Destinations

If the version of Cisco IOS that you have installed on your networking device supports the NetFlow Multiple Export Destinations feature, you can configure your networking device to export NetFlow data to a maximum of 2 export destinations (collectors) per cache (main and aggregation caches), using any combination of UDP and SCTP as the transport protocol for the destinations. A destination is identified by a unique combination of hostname or IP address and port number or port type.

Note UDP is the default transport protocol used by the **export destination**command. In some Cisco IOS releases you can configure SCTP as the transport protocol if you need reliability and additional redundancy. Refer to the **ip flow-export sctp** command for more information.

The table below shows examples of the 2 permitted NetFlow export destinations for each cache.

Table 3 Examples of Permitted Multiple NetFlow Export Destinations for Each Cache

First Export Destination	Second Export Destination
ip flow-export *10.25.89.32 100 udp*	**ip flow-export** *10.25.89.32 285 udp*
ip flow-export *10.25.89.32 100 udp*	**ip flow-export** *172.16.89.32 100 udp*
ip flow-export *10.25.89.32 100 udp*	**ip flow-export** *172.16.89.32 285 udp*
ip flow-export *10.25.89.32 100 udp*	**ip flow-export** *10.25.89.32 100 sctp*
ip flow-export *10.25.89.32 100 sctp*	**ip flow-export** *10.25.89.32 285 sctp*
ip flow-export *10.25.89.32 100 sctp*	**ip flow-export** *172.16.89.32 100 sctp*
ip flow-export *10.25.89.32 100 sctp*	**ip flow-export** *172.16.89.32 285 sctp*

The most common use of the multiple-destination feature is to send the NetFlow cache entries to two different destinations for redundancy. Therefore, in most cases the second destination IP address is not the same as the first IP address. The port numbers can be the same when you are configuring two unique destination IP addresses. If you want to configure both instances of the command to use the same destination IP address, you must use unique port numbers. You receive a warning message when you configure the two instances of the command with the same IP address. The warning message is, "%Warning: Second destination address is the same as previous address <ip-address>".

VRF Destinations for Exporting NetFlow Data

Before Cisco IOS Releases 12.4(4)T, 12.2(33)SXI4, and Cisco IOS XE Release 2.6, only one routing option existed for NetFlow export data packets. NetFlow sent all export data packets to the global routing table for routing to the export destinations you specified.

Cisco IOS Release 12.4(4)T, Cisco IOS XE Release 2.6, Cisco IOS Release 12.2(33)SXI4, and later releases provide an additional routing option for NetFlow export data packets. You can send NetFlow data export packets to a Virtual Private Network (VPN) routing/forwarding instance (VRF) for routing to the destinations that you specify.

To send NetFlow data export packets to a VRF for routing to a destination, you enter the optional **vrf***vrf-name* keyword and argument with the **ip flow-export destination** *ip-addressport* command. To configure the global routing table option, enter this command without the optional **vrf***vrf-name* keyword and argument.

More Information on NetFlow Data Export

For more information on NetFlow Data Export (NDE) on a Cisco Catalyst 6500 series switch, refer to the "Configuring NDE" chapter in the *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide* .

For more information on NetFlow Data Export (NDE) on a Cisco 7600 series router, refer to the "Configuring NDE" chapter in the *Cisco 7600 Series Cisco IOS Software Configuration Guide* .

For more information on NetFlow Data Export (NDE) on Cisco routers, refer to the “Configuring NetFlow and NetFlow Data Export” chapter in the *Cisco IOS NetFlow Configuration Guide* .

Examples

The following example shows how to configure the networking device to export the NetFlow cache entry to a single export destination system:

```
Router(config)# ip flow-export destination 10.42.42.1 9991
```

The following example shows how to configure the networking device to export the NetFlow cache entry to multiple destination systems:

```
Router(config)# ip flow-export destination 10.42.42.1 9991
Router(config)# ip flow-export destination 10.0.101.254 9991
```

The following example shows how to configure the networking device to export the NetFlow cache entry to two different UDP ports on the same destination system:

```
Router(config)# ip flow-export destination 10.42.42.1 9991
Router(config)# ip flow-export destination 10.42.42.1 9992
%Warning: Second destination address is the same as previous address 10.42.42.1
```

The following example shows how to configure the networking device to export NetFlow data to a export destination that is reachable in VRF group1:

```
Router(config)# ip flow-export destination 172.16.10.2 78 vrf group1
```

Related Commands

Command	Description
ip flow-export interface-names	Enables the inclusion of the interface names for the flows during the export of NetFlow accounting information in NetFlow cache entries.
ip flow-export source	Specifies the interface from which NetFlow will derive the source IP address for the NetFlow export datagrams containing NetFlow accounting information from NetFlow cache entries.
ip flow-export template	Configures template options for the export of NetFlow accounting information in NetFlow cache entries
ip flow-export version	Specifies the export version format for the exporting of NetFlow accounting information in NetFlow cache entries
show ip flow export	Displays the status and the statistics for NetFlow accounting data export.

ip flow-export destination sctp

To enable the reliable export of NetFlow accounting information in NetFlow cache entries, use the **ip flow-export destination sctp** command in global configuration mode. To disable the reliable export of information, use the noform of this command.

ip flow-export destination {*ip-address* | *hostname*} *port* [**vrf** *vrf-name*] **sctp**

no ip flow-export destination {*ip-address* | *hostname*} *port* [**vrf** *vrf-name*] **sctp**

Syntax Description

ip-address | *hostname*	IP address or hostname of the workstation to which you want to send the NetFlow information.
port	Specifies the number of the stream control transmission protocol (SCTP) port on which the workstation is listening for the exported NetFlow datagrams.
vrf *vrf-name*	(Optional) The **vrf** keyword specifies that the export data packets are to be sent to the named Virtual Private Network (VPN) routing forwarding instance (VRF) for routing to the destination, instead of to the global routing table. **Note** The *vrf-name* argument is the name of the VRF

Command Default

Reliable export of NetFlow information is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

NetFlow Reliable Export Using SCTP

SCTP can be used as an alternative to UDP when you need a more robust and flexible transport protocol than UDP. SCTP is a reliable message-oriented transport layer protocol, which allows data to be transmitted between two end-points in a reliable, partially reliable, or unreliable manner.

An SCTP session consists of an association (connection) between two end-points (peers), which can contain one or more logical channels called streams. The default mode of transmission for a stream is to

guarantee reliable ordered delivery of messages using a selective-acknowledgment scheme. SCTP buffers messages until their receipt has been acknowledged by the receiving end-point. SCTP has a congestion control mechanism which limits how much memory is consumed by the SCTP stack, in packet buffering.

VRF Destinations for Exporting NetFlow Data

Before Cisco IOS Release 12.4(4)T, one routing option existed for NetFlow export data packets. NetFlow sent all export data packets to the global routing table for routing to the destinations you specified.

Cisco IOS 12.4(4)T and later releases provide an additional routing option for NetFlow export data packets. You can send NetFlow data export packets to a Virtual Private Network (VPN) routing/forwarding instance (VRF) for routing to the destinations that you specify.

To send NetFlow data export packets to a VRF for routing to a destination, you enter the optional **vrf***vrf-name* keyword and argument with the **ip flow-export destination** *ip-addressport* command. To configure the global routing table option, enter this command without the optional **vrf***vrf-name* keyword and argument.

Examples

The following example shows how to configure the networking device to use SCTP as the transport protocol when exporting NetFlow data:

```
Router(config)# ip flow-export destination 172.16.10.2 78 sctp
```

The following example shows how to configure the networking device to use SCTP as the transport protocol when exporting NetFlow data to a host that is reachable in VRF group1:

```
Router(config)# ip flow-export destination 172.16.10.2 78 vrf group1 sctp
```

Related Commands

Command	Description
backup	Configures a backup destination for the reliable export of NetFlow accounting information in NetFlow cache entries
reliability	Specifies the level of reliability for the reliable export of NetFlow accounting information in NetFlow cache entries.
show ip flow export	Displays the status and the statistics for NetFlow accounting data export.

ip flow-export hardware version

To specify the NetFlow Data Export (NDE) version for hardware-switched flows, use the **ip flow-export hardware version**command in global configuration mode. To return to the default settings, use the noform of this command.

ip flow-export hardware version [**5** | **7**]

no ip flow-export hardware version

Syntax Description

5	Specifies that the export packet uses the version 5 format; see the “Usage Guidelines” section for additional information.
7	Specifies that the export packet uses the version 7 format; see the “Usage Guidelines” section for additional information.

Command Default

Version 7

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720 and the Supervisor Engine 2.

Usage Guidelines

The **ip flow-export hardware version** command is only supported on systems that have a version 2 Supervisior Engine.

Examples

This example shows how to specify the NDE version for hardware-switched flows:

```
Router(config)#
 ip flow-export hardware version 5
Router(config)#
```

Related Commands

Command	Description
ip flow-export interface	Enables the interface-based ingress NDE for hardware-switched flows.
ip flow-export version (Supervisor Engine 2)	Specifies the version for the export of information in NetFlow cache entries.
show mls nde	Displays information about the NDE hardware-switched flow.

ip flow-export interface-names

To enable the inclusion of the interface names for the flows during the export of NetFlow accounting information in NetFlow cache entries, use the **ip flow-export interface-names** command in global configuration mode. To return to the default behavior, use the noform of this command.

ip flow-export interface-names

no ip flow-export interface-names

Syntax Description

There are no keywords or arguments for this command.

Command Default

Inclusion the interface names for the flows during the export of NetFlow accounting information in NetFlow cache entries is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

The **interface-names** keyword for the **ip flow-export** command configures NetFlow to include the interface names from the flows when it exports the NetFlow cache entry to a destination system.

Prior to the addition of the **interface-names** keyword you had to poll the SNMP MIB for this information and correlate IF-index entries to interface names. After you enable the **ip flow-export interface-names** command the information is included in the exported NetFlow cache entries.

Note Interface names are exported as options templates/records.

Examples

The following example shows how to configure the networking device to include the interface names from the flows when it exports the NetFlow cache entry to a destination system:

```
Router(config)# ip flow-export interface-names
```

Related Commands

Command	Description
ip flow-export destination	Enables the export of NetFlow accounting information in NetFlow cache entries to a remote device such as a server running an application that analyzes NetFlow data.
ip flow-export source	Specifies the interface from which NetFlow will derive the source IP address for the NetFlow export datagrams containing NetFlow accounting information from NetFlow cache entries.
ip flow-export template	Configures template options for the export of NetFlow accounting information in NetFlow cache entries
ip flow-export version	Specifies the export version format for the exporting of NetFlow accounting information in NetFlow cache entries
show ip flow export	Displays the status and the statistics for NetFlow accounting data export.

ip flow-export source

To specify the interface from which NetFlow will derive the source IP address for the NetFlow export datagrams containing NetFlow accounting information from NetFlow cache entries, use the **ip flow-export source** command in global configuration mode. To return to the default behavior, use the noform of this command.

ip flow-export source interface *type number*

no ip flow-export source interface *type number*

Syntax Description

interface *type number*	Interface name followed by the interface type and number.

Command Default

NetFlow uses the IP address of the interface that the datagram is transmitted over as the source IP address for the NetFlow datagrams.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1 CA	This command was introduced.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)M	This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M. The **interface** *type number*keyword and arguments were added.

Release	Modification
12.2(33)SRC	This command was modified. The **interface** *type number*keyword and arguments were added.
12.2(33)SXI	This command was modified. The **interface** *type number*keyword and arguments were added.
Cisco IOS XE Release2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

After you configure NetFlow data export, use the **ip flow-export source**command to specify the interface that NetFlow will use to obtain the source IP address for the NetFlow datagrams that it sends to destination systems, such as a system running NFC Engine. This will override the default behavior (using the IP address of the interface that the datagram is transmitted over as the source IP address for the NetFlow datagrams).

Some of the benefits of using a consistent IP source address for the datagrams that NetFlow sends are:

- The source IP address of the datagrams exported by NetFlow is used by the destination system to determine which router the NetFlow data is arriving from. If your network has two or more paths that can be used to send NetFlow datagrams from the router to the destination system and you do not specify the source interface from which the source IP address is to obtained, the router uses the IP address of the interface that the datagram is transmitted over as the source IP address of the datagram. In this situation the destination system might receive NetFlow datagrams from the same router, but with different source IP addresses. This causes the destination system to treat the NetFlow datagrams as if they were being sent from different routers unless you have configured the destination system to aggregate the NetFlow datagrams it receives from all of the possible source IP addresses in the router into a single NetFlow flow.
- If your router has multiple interfaces that can be used to transmit datagrams to the CNS NFC, and you do not configure the **ip flow-export source interface**command, you will have to add an entry for the IP address of each interface into any access lists that you create for permitting NetFlow traffic. It is easier to create and maintain access-lists for permitting NetFlow traffic from known sources and blocking it from unknown sources when you limit the source IP address for NetFlow datagrams to a single IP address for each router that is exporting NetFlow traffic.

You can use the IP address of a loopback interface as the source IP address for NetFlow traffic by entering the **ip flow-export source interface** *type*[*number* | *slot*/*port*] command (for example, **ip flow-export source interface***loopback 0*)**.**Doing so makes it more difficult for people who want to attack your network by spoofing the source IP address of your NetFlow-enabled routers to determine which IP address to use. This is because the IP addresses assigned to loopback interfaces are not as easy to discover as the IP addresses assigned to physical interfaces on the router. For example, it is easy to determine the IP address of a Fast Ethernet interface on a router that is connected to a LAN that has end user devices on it. You simply check the configuration of one of the devices for its IP default gateway address.

If the export destination is in a VRF, the **ip flow-export source** command specifies an interface, which is not an interface in the same VRF as the destination. Therefore, the code will automatically pickup an interface on the local router that is in the same VRF as the export-destination and hence ignore the configured export source.

Examples

The following example shows how to configure NetFlow to use a loopback interface as the source interface for NetFlow traffic.

Caution The interface that you configure as the **ip flow-export source** interface must have an IP address configured and it must be up.

```
Router(config)# ip flow-export source loopback0
```

Related Commands

Command	Description
ip flow-export destination	Enables the export of NetFlow accounting information in NetFlow cache entries to a remote device such as a server running an application that analyzes NetFlow data.
ip flow-export interface-names	Enables the inclusion of the interface names for the flows during the export of NetFlow accounting information in NetFlow cache entries.
ip flow-export template	Configures template options for the export of NetFlow accounting information in NetFlow cache entries
ip flow-export version	Specifies the export version format for the exporting of NetFlow accounting information in NetFlow cache entries
show ip flow export	Displays the status and the statistics for NetFlow accounting data export.

ip flow-export template

To configure template options for the export of NetFlow accounting information in NetFlow cache entries, use the **ip flow-export template** command in global configuration mode. To remove the configured refresh-rate and timeout-rate and to return to the default rate, use the noform of this command.

Configure template only

ip flow-export template {**refresh-rate** *packets* | **timeout-rate** *minutes*}

no ip flow-export template {**refresh-rate** | **timeout-rate**}

Configure template options

ip flow-export template options {**export-stats** | **refresh-rate** *packets* | **timeout-rate** *minutes* | **sampler** | **nbar**}

no ip flow-export template options {**export-stats** | **refresh-rate** | **timeout-rate** | **sampler** | **nbar**}

Syntax Description

template	Enables the **refresh-rate** and **timeout-rate** keywords for the configuring of Version 9 export templates.
refresh-rate *packets*	Specifies the number of export packets that are sent before the options and flow templates are resent. Range: 1 to 600. Default: 20.
timeout-rate *minutes*	Specifies the interval (in minutes) that the router waits after sending the templates (flow and options) before sending them again. Range: 1 to 3600. Default: 30.
options	Enables the **export-stats**, **refresh-rate**, **sampler** and **timeout-rate** keywords for configuring Version 9 export options.
export-stats	Enables the export of statistics including the total number of flows exported and the total number of packets exported.
sampler	When Version 9 export is configured, this keyword enables the export of an option containing a random-sampler configuration, including the sampler ID, sampling mode, and sampling interval for each configured random sampler. **Note** You must have a flow sampler map configured before you can configure the sampler keyword for the **ip flow-export template options** command.

nbar	Exports application mapping information to the NetFlow data collector.

Command Default

The export template and export template options are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)ZYA2	This command was modified. The **nbar**keyword was added.

Usage Guidelines

The **ip flow-export template options export-stats** command requires that the NetFlow Version 9 export format be already configured on the router.

The **ip flow-export template options sampler** command requires that the NetFlow Version 9 export format and a flow sampler map be already configured on the router.

The **ip flow-export template options nbar** command exports application IDs to string mapping as options. It displays string values for application IDs to which they are mapped. To export the application mapping information, you must enable NetFlow Export Version 9 export format and have Network Based Application Recognition (NBAR) configured on the device.

Examples

The following example shows how to configure NetFlow so that the networking device sends the export statistics (total flows and packets exported) as options data:

```
Router(config)# ip flow-export template options export-stats
```

The following example shows how to configure NetFlow to wait until 100 export packets have been sent or 60 minutes have passed since the last time the templates were sent (whichever comes first) before the templates are resent to the destination host:

```
Router(config)# ip flow-export template refresh-rate 100
Router(config)# ip flow-export template timeout-rate 60
```

The following example shows how to configure NetFlow to enable the export of information about NetFlow random samplers:

```
Router(config)# ip flow-export template options sampler
```

Tip You must have a **flow-sampler** map configured before you can configure the sampler keyword for the **ip flow-export template options** command.

The following example shows how to configure NetFlow to enable the export of application mapping information:

```
Router(config)# ip flow-export template options nbar
```

Related Commands

Command	Description
ip flow-export destination	Enables the export of NetFlow accounting information in NetFlow cache entries to a remote device such as a server running an application that analyzes NetFlow data.
ip flow-export interface-names	Enables the inclusion of the interface names for the flows during the export of NetFlow accounting information in NetFlow cache entries.
ip flow-export source	Specifies the interface from which NetFlow will derive the source IP address for the NetFlow export datagrams containing NetFlow accounting information from NetFlow cache entries.
ip flow-export version	Specifies the export version format for the exporting of NetFlow accounting information in NetFlow cache entries
show ip flow export	Displays the status and the statistics for NetFlow accounting data export.

ip flow-export version

To specify the export version format for the exporting of NetFlow accounting information in NetFlow cache entries, use the **ip flow-export version** command in global configuration mode. To return to the default behavior, use the noform of this command.

ip flow-export version {**1** | {**5** | **9**} [**origin-as** | **peer-as**] [**bgp-nexthop**]}

no ip flow-export version {**1** | {**5** | **9**} [**origin-as** | **peer-as**] [**bgp-nexthop**]}

Syntax Description

1	Specifies that the export datagram uses the version 1 format. This is the default.
5	Specifies that the export datagram uses the version 5 format.
9	(Specifies that the export datagram uses the version 9 format.
origin-as	(Optional) Specifies that export statistics include the originating autonomous system (AS) for the source and destination.
peer-as	(Optional) Specifies that export statistics include the peer AS for the source and destination.
bgp-nexthop	(Optional) Specifies that export statistics include Border Gateway Protocol (BGP) next-hop-related information.

Command Default

Version 1 is the default export format for the exporting of NetFlow accounting information in NetFlow cache entries.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1CA	This command was introduced.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S, and the **9** keyword was added.

Release	Modification
12.0(26)S	Support for the BGP Next Hop Support feature was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(1)	Support for the BGP Next Hop Support and NetFlow v9 Export Format features was added.
12.2(18)S	Support for the BGP Next Hop Support and NetFlow v9 Export Format features was added.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **ip flow-export version** command supports three export data formats: Version 1, Version 5, and Version 9. Version 1 should be used only when it is the only NetFlow data export format version that is supported by the application that you are using to analyze the exported NetFlow data. Version 5 exports more fields than Version 1. Version 9 is the only flexible export format version.

The NetFlow Version 9 Export Format feature was introduced in Cisco IOS Release 12.0(24)S and was integrated into Cisco IOS Release 12.3(1) and Cisco IOS Release 12.2(18)S.

NetFlow Version 9 is a flexible and extensible means for transferring NetFlow records from a network node to a collector. NetFlow Version 9 has definable record types and is self-describing for easier NetFlow Collection Engine configuration.

Third-party business partners who produce applications that provide NetFlow Collection Engine or display services for NetFlow do not need to recompile their applications each time a new NetFlow technology is added. Instead, with the NetFlow Version 9 Export Format feature, they can use an external data file that documents the known template formats and field types.

NetFlow Version 9 has the following characteristics:

- Record formats are defined by templates.
- Template descriptions are communicated from the router to the NetFlow Collection (NFC) Engine.
- Flow records are sent from the router to the NetFlow Collection Engine with minimal template information so that the NetFlow Collection Engine can relate the records to the appropriate template.

Version 9 is independent of the underlying transport (UDP, TCP, SCTP, and so on).

Note The values for the BGP next hop IP address captured by the **bgp-nexthop** command are exported to a NetFlow export destination only when the Version 9 export format is configured.

Note In order for the BGP information to be populated in the main cache, you must have either a NetFlow export destination configured or a NetFlow aggregation configured.

Note The AS values for the **peer-as** and the **origin-as** keywords are captured only if you have configured an export destination with the **ip flow-export destination** command.

For more information on the available export data formats, see the *Cisco IOS NetFlow Configuration Guide*, Release 12.4T. For more information on the Version 9 data format, see the *Cisco IOS NetFlow Version 9 Export Format Feature Guide* .

Caution Entering the **ip flow-export version**or **no ip flow-export version**command on the Cisco 12000 series Internet routers, Cisco 6500 series routers, and Cisco 7600 series routers and specifying a format other than version 1 (in other words, entering the **ip flow-export version**or **no ip flow-export version**command and specifying the **5** keyword) causes packet forwarding to stop for a few seconds while NetFlow reloads the Route Processor and line card Cisco Express Forwarding tables. To avoid interruption of service to a live network, apply this command during a change window, or include it in the startup-config file to be executed during a router reboot.

Examples

The following example shows how to configure the networking device to use the NetFlow Version 9 format for the exported data and how to include the originating autonomous system (origin-as) with its corresponding next BGP hop (bgp-nexthop):

```
Router(config)# ip flow-export version 9 origin-as bgp-nexthop
```

Related Commands

Command	Description
ip flow-export destination	Enables the export of NetFlow accounting information in NetFlow cache entries to a remote device such as a server running an application that analyzes NetFlow data.
ip flow-export interface-names	Enables the inclusion of the interface names for the flows during the export of NetFlow accounting information in NetFlow cache entries.
ip flow-export source	Specifies the interface from which NetFlow will derive the source IP address for the NetFlow export datagrams containing NetFlow accounting information from NetFlow cache entries.

Command	Description
ip flow-export template	Configures template options for the export of NetFlow accounting information in NetFlow cache entries
show ip flow export	Displays the status and the statistics for NetFlow accounting data export.

ip flow-export version (Supervisor Engine 2)

To specify the version for the export of information in NetFlow cache entries, use the **ip flow-export version**command in global configuration mode. To disable information exporting, use the noform of this command.

ip flow-export version {**1** | **5** [**origin-as** | **peer-as**] | **6** [**origin-as** | **peer-as**]}

no ip flow-export version

Syntax Description

1	Specifies that the export packet uses the version 1 format; see the “Usage Guidelines” section for additional information.
5	Specifies that the export packet uses the version 5 format; see the “Usage Guidelines” section for additional information.
origin-as	(Optional) Specifies that export statistics include the origin autonomous system for the source and destination.
peer-as	(Optional) Specifies that export statistics include the peer autonomous system for the source and destination.
6	Specifies that the export packet uses the version 6 format; see the “Usage Guidelines” section for additional information.

Command Default

Version 1

Command Modes

Global configuration

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.

Usage Guidelines

This command documentation applies only to systems that have a version 2 Supervisior Engine.

NDE makes traffic statistics available for analysis by an external data collector. You can use NDE to monitor all Layer 3 switched and all routed IP unicast traffic. In the Cisco 7600 series router, both the

Policy Feature Card (PFC) and the Multilayer Switch Feature Card (MSFC) maintain NetFlow caches that capture flow-based traffic statistics. The cache on the PFC captures statistics for Layer 3-switched flows. The cache on the MSFC captures statistics for routed flows.

Note NDE can use NDE version 1, 5, or 6 to export the statistics that are captured on the MSFC for routed traffic.

The number of records stored in the datagram is a variable from 1 to 24 for version 1. The number of records stored in the datagram is a variable between 1 and 30 for version 5.

For more information on NDE, refer to the “Configuring NDE” chapter in the Cisco 7600 Series Router Cisco IOS Software Configuration Guide.

Examples

This example shows how to export the data using the version 5 format and include the peer autonomous system information:

```
Router# configure terminal
Router(config)# interface loopback0
Router(config-if)# ip address 4.0.0.1 255.0.0.0
Router(config-if)# exit
Router(config)# interface serial 5/0:0
Router(config-if)# ip unnumbered loopback0
Router(config-if)# no ip mroute-cache
Router(config-if)# encapsulation ppp
Router(config-if)# ip route-cache flow
Router(config-if)# exit
Router(config)# ip flow-export version 5 peer-as
Router(config)# exit
```

Related Commands

Command	Description
ip flow-export destination	Exports the NetFlow cache entries to a specific destination.
ip flow-export source	Specifies the source interface IP address that is used in the NDE datagram.
ip route-cache flow	Enables NetFlow switching for IP routing.

ip flow-export version (Supervisor Engine 720)

To specify the version for the export of information in NetFlow cache entries, use the **ip flow-export version**command in global configuration mode. To return to the default settings, use the noform of this command.

ip flow-export version {**1** | **5** [**origin-as** | **peer-as**] | **9** [**bgp-nexthop** | **origin-as** | **peer-as**]}

no ip flow-export version

Syntax Description

1	Specifies that the export packet use the version 1 format; see the “Usage Guidelines” section for additional information.
5	Specifies that the export packet use the version 5 format; see the “Usage Guidelines” section for additional information.
origin-as	(Optional) Specifies that export statistics include the origin autonomous system for the source and destination.
peer-as	(Optional) Specifies that export statistics include the peer autonomous system for the source and destination.
9	Specifies that the export packet uses the version 9 format; see the “Usage Guidelines” section for additional information.
bgp-nexthop	(Optional) Specifies that export statistics include the BGP next hop for the source and destination.

Command Default

Export of information in NetFlow cache entries is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(17d)SXB	This command was introduced on the Supervisor Engine 720.

Release	Modification
12.2(18)SXF	Support was added for NetFlow version 9 export format on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Version 5 and version 9 formats include the source and destination autonomous-system addresses and source and destination prefix masks. Also, version 9 includes BGP next-hop information.

The number of records stored in the datagram is a variable from 1 to 24 for version 1. The number of records stored in the datagram is a variable between 1 and 30 for version 5.

For more information on NDE, refer to the “Configuring NDE” chapter in the Cisco 7600 Series Router Cisco IOS Software Configuration Guide.

Caution Entering the **ip flow-export version**or **no ip flow-export version**command on the Cisco 12000 series Internet routers, Cisco 6500 series routers, and Cisco 7600 series routers and specifying a format other than version 1 (in other words, entering the **ip flow-export version**or **no ip flow-export version**command and specifying the **5** keyword) causes packet forwarding to stop for a few seconds while NetFlow reloads the Route Processor and line card Cisco Express Forwarding tables. To avoid interruption of service to a live network, apply this command during a change window, or include it in the startup-config file to be executed during a router reboot.

Examples

This example shows how to export the data using the version 5 format:

```
Router(config)# ip flow-export version 5
```

Related Commands

Command	Description
ip flow-export version (Supervisor Engine 2)	Specifies the version for the export of information in NetFlow cache entries.
show mls nde	Displays information about the NDE hardware-switched flow.

ip flow-top-talkers

To configure NetFlow top talkers to capture traffic statistics for the unaggregated top flows of the heaviest traffic patterns and most-used applications in the network, use the **ip flow-top-talkers**command in global configuration mode. To disable NetFlow top talkers, use the **no** form of this command.

ip flow-top-talkers

no ip flow-top-talkers

Syntax Description

This command has no arguments or keywords.

Command Default

NetFlow top talkers is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.3(11)T	This feature was integrated into Cisco IOS Release 12.3(11)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Tip The **ip flow-top-talkers**command does not appear in the configuration until you have configured the **top***number* and **sort-by** [**bytes** | **packets**] commands.

Enabling NetFlow

You must enable NetFlow on at least one interface in the router; and configure NetFlow top talkers before you can use the **show ip flow top-talkers** command to display the traffic statistics for the unaggregated top

flows in the network. NetFlow top talkers also requires that you configure the **sort-by** and **top** commands. Optionally, the **match** command can be configured to specify additional matching criteria.

Cache Timeout

The timeout period as specified by the **cache-timeout** command does not start until the **show ip flow top-talkers** command is entered. From that time, the same top talkers are displayed until the timeout period expires. To recalculate a new list of top talkers before the timeout period expires, you can change the parameters of the **cache-timeout**, **top**, or **sort-by** command prior to entering the **show ip flow top-talkers**command.

A long timeout period for the **cache-timeout** command limits the system resources that are used by the NetFlow top talkers feature. However, the list of top talkers is calculated only once during the timeout period. If a request to display the top talkers is made more than once during the timeout period, the same results are displayed for each request, and the list of top talkers is not recalculated until the timeout period expires.

A short timeout period ensures that the latest list of top talkers is retrieved; however too short a period can have undesired effects:

- The list of top talkers is lost when the timeout period expires. You should configure a timeout period for at least as long as it takes the network management system (NMS) to retrieve all the required NetFlow top talkers.
- The list of top talkers is updated every time the top talkers information is requested, possibly causing unnecessary usage of system resources.

A good method to ensure that the latest information is displayed, while also conserving system resources, is to configure a large value for the timeout period, but cause the list of top talkers to be recalculated by changing the parameters of the **cache-timeout**, **top**, or **sort-by** command prior to entering the **show ip flow top-talkers**command to display the top talkers. Changing the parameters of the **cache-timeout**, **top**, or **sort-by** command causes the list of top talkers to be recalculated upon receipt of the next command line interface (CLI) or MIB request.

Use the **show ip flow top-talkers** command to display the list of unaggregated top flows.

Examples

In the following example, a maximum of four top talkers is configured. The sort criterion is configured to sort the list of top talkers by the total number of bytes for each Top Talker.

```
Router(config)# ip flow-top-talkers
Router(config-flow-top-talkers)# top 4
Router(config-flow-top-talkers)# sort-by bytes
```

The following example shows the output of the **show ip flow top talkers** command with the configuration from the previous example:

```
Router# show ip flow top-talkers

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP Bytes
Et0/0.1       10.10.18.1      Et1/0.1       172.16.10.232   11 00A1 00A1   349K
Et0/0.1       10.10.19.1      Et1/0.1       172.16.10.2     11 00A2 00A2   349K
Et0/0.1       172.30.216.196  Et1/0.1       172.16.10.2     06 0077 0077   328K
Et0/0.1       10.162.37.71    Et1/0.1       172.16.10.2     06 0050 0050   303K
4 of 4 top talkers shown. 11 flows processed
```

Related Commands

Command	Description
cache-timeout	Specifies the length of time for which the list of top talkers (heaviest traffic patterns and most-used applications in the network) for the NetFlow MIB and top talkers feature is retained.
match (NetFlow)	Specifies match criteria for the NetFlow MIB and top talkers (heaviest traffic patterns and most-used applications in the network) feature.
show ip flow top-talkers	Displays the statistics for the top talkers (heaviest traffic patterns and most-used applications in the network).
sort-by	Specifies the sorting criterion for top talkers (heaviest traffic patterns and most-used applications in the network) to be displayed for the NetFlow MIB and top talkers feature.
top	Specifies the maximum number of top talkers (heaviest traffic patterns and most-used applications in the network) to be displayed for the NetFlow MIB and top talkers feature.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

ip multicast netflow

To configure multicast NetFlow accounting on an interface, use the **ip multicast netflow**command in interface configuration mode. To disable multicast NetFlow accounting, use the **no** form of this command.

ip multicast netflow {**ingress** | **egress**}

no ip multicast netflow {**ingress** | **egress**}

Syntax Description

ingress	Enables multicast NetFlow (ingress) accounting.
egress	Enables multicast NetFlow (egress) accounting.

Command Default

Multicast ingress NetFlow accounting is enabled.

Multicast egress NetFlow accounting is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Release	Modification
12.4(11)T	In Cisco IOS Release 12.4(11)T this command was moved to global configuration mode and the **ingress** and **egress** keywords were replaced by the **output-counters** keyword. See the **ip multicast netflow output-counters** command.
12.4(12)	In Cisco IOS Release 12.4(12) this command was moved to global configuration mode and the **ingress** and **egress** keywords were replaced by the **output-counters** keyword. See the **ip multicast netflow output-counters** command.
12.(33)SRB	In Cisco IOS Release 12.(33)SRB this command was moved to global configuration mode and the **ingress** and **egress** keywords were replaced by the **output-counters** keyword. See the **ip multicast netflow output-counters** command.
12.(33)SXH	In Cisco IOS Release 12.(33)SXH this command was moved to global configuration mode and the **ingress** and **egress** keywords were replaced by the **output-counters** keyword. See the **ip multicast netflow output-counters** command.
12.(33)SB	In Cisco IOS Release 12.(33)SB this command was moved to global configuration mode and the **ingress** and **egress** keywords were replaced by the **output-counters** keyword. See the **ip multicast netflow output-counters** command.

Usage Guidelines

You must have NetFlow accounting configured on your router before you can use this command.

ip multicast netflow ingress

NetFlow (ingress) accounting for multicast traffic is enabled by default. The **ip multicast netflow ingress** command does not appear in the configuration.

ip multicast netflow egress

You must enable multicast egress NetFlow accounting on all interfaces for which you want to count outgoing multicast streams.

To display the multicast entries, enter the **show mls netflow ip** command.

Examples

The following example shows how to enable multicast ingress NetFlow accounting on the ingress Ethernet 1/0 interface:

```
Router(config)# interface ethernet 1/0
Router(config-if)# ip multicast netflow ingress
```

The following example shows how to enable multicast egress NetFlow accounting on the egress Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ip multicast netflow egress
```

Related Commands

Command	Description
ip multicast netflow rpf-failure	Enables accounting for multicast data that fails the RPF check.
show ip cache flow	Displays a summary of the NetFlow statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.
show ip mroute	Displays the contents of the IP multicast routing (mroute) table.
show mls netflow ip	Displays information about the hardware NetFlow IP.

ip multicast netflow output-counters

To enable NetFlow accounting for the number of bytes and packets of multicast traffic forwarded from an ingress flow, use the **ip multicast netflow output-counters**command in global configuration mode. To disable accounting for the number of bytes and packets forwarded, use the **no** form of this command.

ip multicast netflow output-counters

no ip multicast netflow output-counters

Syntax Description

This command has no arguments or keywords.

Command Default

Accounting for the number of bytes and packets of multicast traffic that is forwarded is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.4(12)	This command was integrated into Cisco IOS Release 12.4(12).
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

You must have NetFlow accounting configured on your router before you can use this command.

Examples

The following example shows how to enable NetFlow accounting for the number of bytes and packets of multicast traffic forwarded from an ingress flow:

```
Router# configure terminal
Router(config)# ip multicast netflow output-counters
Router(config)# end
```

Related Commands

Command	Description
ip multicast netflow	Configures multicast NetFlow accounting on an interface.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.
show ip mroute	Displays the contents of the IP multicast routing (mroute) table.
show ip rpf	Displays how IP multicast routing does RPF.
show ip rpf events	Displays the last 15 triggered multicast RPF check events.

ip multicast netflow rpf-failure

To enable NetFlow accounting for multicast data that fails the reverse path forwarding (RPF) check (meaning any IP packets that lack a verifiable IP source address), use the **ip multicast netflow rpf-failure** command in global configuration mode. To disable accounting for multicast data that fails the RPF check, use the **no** form of this command.

ip multicast netflow rpf-failure

no ip multicast netflow rpf-failure

Syntax Description

This command has no arguments or keywords.

Command Default

Accounting for multicast data that fails the RPF check is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You must have NetFlow accounting configured on your router before you can use this command.

Examples

The following example shows how to enable accounting for multicast data that fails the RPF check:

```
Router# configure terminal
Router(config)# ip multicast netflow rpf-failure
Router(config)# end
```

Related Commands

Command	Description
ip multicast netflow	Configures multicast NetFlow accounting on an interface.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.
show ip mroute	Displays the contents of the IP multicast routing (mroute) table.
show ip rpf	Displays how IP multicast routing does RPF.
show ip rpf events	Displays the last 15 triggered multicast RPF check events.

ip route-cache flow

Effective with Cisco IOS Releases 12.4(2)T and 12.2(18)SXD, the **ip route-cache flow**command is replaced by the **ip flow ingress**command. See the **ip flow ingress** command for more information.

To enable NetFlow (ingress) accounting for traffic arriving on an interface, use the **ip route-cache flow**command in interface configuration mode. To disable NetFlow (ingress) accounting for traffic arriving on an interface, use the **no** form of this command in interface configuration mode.

ip route-cache flow

no route-cache flow

Syntax Description

This command has no arguments or keywords.

Command Default

This command is not enabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
12.4(2)T	The **ip route-cache flow** command is automatically remapped to the **ip flow-ingress** command.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(25)S	The **ip route-cache flow** command is automatically remapped to the **ip flow-ingress** command.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(18)SXD	The **ip route-cache flow** command is automatically remapped to the **ip flow-ingress** command.

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

Usage Guidelines

Use this command on an interface or subinterface to enable NetFlow (ingress) accounting for traffic that is being received by the router.

Cisco IOS Release 12.2(25)S and 12.2(18)SXD

When you enter the **ip route-cache flow** command to enable NetFlow (ingress) accounting on an interface in a router that is running Cisco IOS Release 12.2(25)S or later, or Cisco IOS Release 12.2(18)SXD or later, the command is automatically remapped to the **ip flow-ingress** command before it is added to the in the running configuration. Therefore you must use the **no ip flow ingress** command to disable NetFlow (ingress) accounting on the interface.

Examples

The following example shows how to enable NetFlow (ingress) accounting on Ethernet interface 0/0 using the **ip route-cache flow** command:

```
Router(config)# interface Ethernet0/0
Router(config-if)# ip
 route-cache flow
```

The following example shows how to disable NetFlow (ingress) accounting on Ethernet interface 0/0 of a router that is running Cisco IOS Release 12.2(25)S or later using the **no ip flow ingress** command:

```
Router(config)# interface Ethernet0/0
Router(config-if)# no ip flow ingress
```

Related Commands

Command	Description
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
ip flow ingress	Enables NetFlow (ingress) accounting for traffic arriving on an interface.