NetFlow Reliable Export With SCTP

NetFlow is a Cisco IOS application that provides statistics on packets flowing through the router. It is emerging as a primary network accounting and security technology. This document describes the NetFlow application and the new NetFlow Reliable Export With Stream Control Transmission Protocol (SCTP) feature.

The NetFlow Reliable Export with SCTP feature adds the ability for NetFlow to use the reliable and congestion-aware SCTP when exporting statistics to a network management system that supports the NetFlow data export formats, such as a system running CNS NetFlow Collection Engine (NFC).

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for NetFlow Reliable Export With SCTP

NetFlow and Cisco Express Forwarding (CEF), distributed CEF (dCEF), or fast switching must be configured on your system.

Restrictions for NetFlow Reliable Export With SCTP

The NetFlow SCTP collector must support SCTP.

Information About NetFlow Reliable Export With SCTP

NetFlow Data Capture

NetFlow identifies packet flows for both ingress and egress IP packets. It does not involve any connection-setup protocol. NetFlow is completely transparent to the existing network, including end stations and application software and network devices like LAN switches. Also, NetFlow capture and export are performed independently on each internetworking device; NetFlow need not be operational on each router in the network.

NetFlow is supported on IP and IP encapsulated traffic over most interface types and Layer 2 encapsulations.

You can display and clear NetFlow statistics. NetFlow statistics consist of IP packet size distribution, IP flow switching cache information, and flow information.

NetFlow Benefits

NetFlow can capture a rich set of traffic statistics. These traffic statistics include user, protocol, port, and type of service (ToS) information that can be used for a wide variety of purposes, including network traffic analysis and capacity planning, security, enterprise accounting and departmental chargebacks, Internet Service Provider (ISP) billing, data warehousing, and data mining for marketing purposes.

Network Application and User Monitoring

NetFlow data enables you to view detailed, time and application based usage of a network. This information allows you to plan and allocate network and application resources, and provides for extensive near real-time network monitoring capabilities. It can be used to display traffic patterns and application-based views. NetFlow provides proactive problem detection and efficient troubleshooting, and it facilitates rapid problem resolution. You can use NetFlow information to efficiently allocate network resources and to detect and resolve potential security and policy violations.

Network Analysis and Planning

You can use NetFlow to capture data for extended periods of time, which enables you to track network utilization and anticipate network growth and plan upgrades. NetFlow service data can be used to optimize network planning, which includes peering, backbone upgrades, and routing policy planning. It also enables you to minimize the total cost of network operations while maximizing network performance, capacity, and reliability. NetFlow detects unwanted WAN traffic, validates bandwidth and quality of service (QoS) behavior,

and enables the analysis of new network applications. NetFlow offers valuable information that you can use to reduce the cost of operating the network.

Denial of Service and Security Analysis

You can use NetFlow data to identify and classify in real time denial of service (DoS) attacks, viruses, and worms. Changes in network behavior indicate anomalies that are clearly reflected in NetFlow data. The data is also a valuable forensic tool that you can use to understand and replay the history of security incidents.

Accounting and Billing

NetFlow data provides fine-grained metering for highly flexible and detailed resource utilization accounting. For example, flow data includes details such as IP addresses, packet and byte counts, timestamps, and information about type of service (ToS) and application ports. Service providers might utilize the information for billing based on time-of-day, bandwidth usage, application usage, or QoS. Enterprise customers might utilize the information for departmental charge-back or cost allocation for resource utilization.

Traffic Engineering

NetFlow provides autonomous system (AS) traffic engineering details. You can use NetFlow-captured traffic data to understand source-to-destination traffic trends. This data can be used for load-balancing traffic across alternate paths or for forwarding traffic along a preferred route. NetFlow can measure the amount of traffic crossing peering or transit points. You can use the data to help you decide if a peering arrangement with other service providers is fair and equitable.

NetFlow Data Storage and Data Mining

NetFlow data can be stored for later retrieval and analysis in support of marketing and customer service programs. For example, the data can be mined to find out which applications and services are being used by internal and external users and target the users for improved service and advertising. In addition, NetFlow data gives market researchers access to the who, what, where, and how long information relevant to enterprises and service providers.

NetFlow Cisco IOS Packaging Information

Cisco 7200/7500/7400/MGX/AS5850

Although NetFlow functionality is included in all software images for these platforms, you must purchase a separate NetFlow feature license. NetFlow licenses are sold on a per-node basis.

Other Routers

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn . You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Elements of a NetFlow Network Flow

A NetFlow network flow is defined as a unidirectional stream of packets between a given source and destination. The source and destination are each defined by a network-layer IP address and transport-layer source and destination port numbers. Specifically, a flow is defined by the combination of the following seven key fields:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Layer 3 protocol type
- Type of service
- Input logical interface

These seven key fields define a unique flow. If a packet has one key field different from another packet, it is considered to belong to another flow. A flow might also contain other accounting fields (such as the AS number in the NetFlow export Version 5 flow format). The fields that a given flow contains depend on the export record version that you configure. Flows are stored in the NetFlow cache.

NetFlow Main Cache Operation

The key components of NetFlow are the NetFlow cache that stores IP flow information and the NetFlow export or transport mechanism that sends NetFlow data to a network management collector, such as the NetFlow Collection Engine. NetFlow operates by creating a NetFlow cache entry (a flow record) for each active flow. NetFlow maintains a flow record within the cache for each active flow. Each flow record in the NetFlow cache contains values for the fields that are being monitored that can later be exported to a collection device, such as the NetFlow Collection Engine.

NetFlow Data Capture

NetFlow captures data from ingress (incoming) and egress (outgoing) packets. NetFlow gathers data for the following ingress IP packets:

- IP-to-IP packets
- IP-to-Multiprotocol Label Switching (MPLS) packets

NetFlow captures data for all egress (outgoing) packets through use of the following features:

- Egress NetFlow Accounting--NetFlow gathers data for all egress packets for IP traffic only.
- NetFlow MPLS Egress--NetFlow gathers data for all egress MPLS-to-IP packets.

NetFlow Export Formats

NetFlow exports data in User Datagram Protocol (UDP) datagrams in one of five formats: Version 9, Version 8, Version 7, Version 5, or Version 1. Version 9 export format, the latest version, is the most flexible and extensible format. Version 1 was the initial NetFlow export format; Version 8 only supports export from aggregation caches, and Version 7 is supported only on certain platforms. (Versions 2 through 4 and Version 6 were either not released or are not supported.)

- Version 9--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 MPLS, and Border Gateway Protocol (BGP) next hop. The distinguishing feature of the NetFlow Version 9 format is that it is template based. Templates provide an extensible design to the record format, a feature that should allow future enhancements to NetFlow services without requiring concurrent changes to the basic flow-record format. Internet Protocol Information Export (IPFIX) was based on the Version 9 export format.

- Version 8--A format added to support data export from aggregation caches. Version 8 allows export datagrams to contain a subset of the usual Version 5 export data, if that data is valid for a particular aggregation cache scheme.

- Version 7--A version supported on a Catalyst 6000 series switch with a multilayer switch feature card (MSFC) running CatOS Release 5.5(7) and later. On a Catalyst 6000 series switch with an MSFC, you can export using either the Version 7 or the Version 8 format.

- Version 5--A version that adds BGP AS information and flow sequence numbers.

- Version 1--The initially released export format, rarely used today. Do not use the Version 1 export format unless the legacy collection system you are using requires it. Use either the Version 9 export format or the Version 5 export format for data export from the main cache.

NetFlow Reliable Export With SCTP

Prior to the introduction of the NetFlow Reliable Export With SCTP feature in Cisco IOS Release 12.4(4)T exporting NetFlow information was unreliable because NetFlow encapsulated the exported traffic in UDP packets for transmission to the NFC. Using an unreliable transport protocol such as UDP for sending information across a network has two major disadvantages:

- Lack of congestion awareness--The exporter sends packets as fast as it can generate them, without any regard to the bandwidth available on the network. If the link is fully congested when the NetFlow router attempts to send, the packet might simply be dropped, either before it is put on the exporter's output queue or before it gets to the next hop's input queue.

- Lack of reliability--With export over UDP, the collector has no method of signaling to the exporter that it didn't receive an exported packet. Most versions of NetFlow export packet contain a sequence number, so the collector often knows when it has lost a packet. But given that the exporter discards the export packet as soon as it has been sent and that the NetFlow router lacks a mechanism to request a retransmission of the packet, exporting over UDP can be considered to be unreliable

The NetFlow Reliable Export With SCTP feature uses the SCTP to overcome the two major disadvantages of using UDP as the transport layer protocol:

- SCTP has a congestion control mechanism to ensure that the router does not send data to the collector faster than it can receive it.

- SCTP transmits messages in a reliable manner. SCTP messages are buffered on the router until they have been acknowledged by the collector. Messages that are not acknowledged by the collector are retransmitted by the router.

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 between two end-points, which may contain one or more logical channels called streams. SCTP's stream based transmission model facilitates the export of a mix of different data types, such as NetFlow templates and NetFlow data, over the same connection. The maximum number of inbound and outbound streams supported by an end-point is negotiated during the SCTP association initialization process.

When you configure the NetFlow Version 9 Export and NetFlow Reliable Export features, NetFlow creates a minimum of two streams--stream 0 for templates and options, and one or more streams for carrying data, as required. The following commands are not applicable when you configure the NetFlow Version 9 Export and NetFlow Reliable Export features together because NetFlow Reliable Export export connections use SCTP reliable stream 0 for NetFlow Version 9 Export, and these commands apply only to NetFlow export connections that use UDP:

- **ip flow-export template refresh-rate**

- **ip flow-export template timeout-rate**

- **ip flow-export template options refresh-rate**

- **ip flow-export template options timeout-rate**

When more than one cache (main cache and one or more aggregation caches) is exporting data, each cache creates its own streams with their own configured reliability levels. For example, you can configure the main cache to use SCTP in full reliability mode and the NetFlow prefix aggregation cache to use partial reliability mode to send messages to the same collector using the same SCTP port.

Note When you are using SCTP as the transport protocol for exporting NetFlow traffic, the traffic is usually referred to as messages instead of datagrams because SCTP is a message-oriented protocol. When you are using UDP as the transport protocol for exporting NetFlow traffic, the traffic is usually referred to as datagrams because UDP is a datagram-oriented protocol.

Security

SCTP contains several built-in features to counter many common security threats such as the syn-flood type of DoS attack.

SCTP uses the following techniques to resist flooding attacks:

- A four-way start-up handshake is used to ensure that anyone opening an association is a genuine caller, rather the someone performing a 'syn-flood' type of DoS attack.

- Cookies are used to defer commitment of resources at the responding SCTP node until the handshake is completed.

- Verification Tags are used to prevent insertion of extraneous packets into the flow of an established association.

Reliability Options

SCTP allows data to be transmitted between two end-points (a router running NetFlow SCTP export and a collector that is receiving and acknowledging the SCTP messages) in a reliable manner. In addition to the default behavior of full reliability, SCTP can be configured for partially-reliable or unreliable transmission for applications that do not require full reliability.

When SCTP is operating in full reliability mode, it uses a selective-acknowledgment scheme to guarantee the ordered delivery of messages. The SCTP protocol stack buffers messages until their receipt has been acknowledged by the receiving end-point. (collector). SCTP has a congestion control mechanism that can be used to limit how much memory is consumed by SCTP for buffering packets.

If a stream is specified as unreliable, then the packet is simply sent once and not buffered on the exporter. If the packet is lost enroute to the receiver, the exporter cannot retransmit it.

When a stream is specified as partially-reliable a limit is placed on how much memory should be dedicated to storing un-acknowledged packets. The limit on how much memory should be dedicated to storing unacknowledged packets is configurable by means of the **buffer-limit** *limit* command. If the limit on how much memory should be dedicated to storing unacknowledged packets is exceeded and the router attempts to buffer another packet, the oldest unacknowledged packet is discarded. When SCTP discards the oldest unacknowledged packet, a message called a forward-tsn (transmit sequence number) is sent to the collector to indicate that this packet will not be received. This prevents NetFlow from consuming all the free memory on a router when a situation has arisen which requires many packets to be buffered, for example when SCTP is experiencing long response times from an SCTP peer connection.

When SCTP is operating in partially reliable mode, the limit on how much memory should be dedicated to storing un-acknowledged packets should initially be set as high as possible. The limit can be reduced if other processes on the router begin to run out of memory. Deciding on the best value for the limit involves a trade-off between avoiding starving other processes of the memory that they require to operate and dropping SCTP messages that have not been acknowledged by the collector.

Unreliable SCTP can be used when the collector that you are using doesn't support UDP as a transport protocol for receiving NetFlow export datagrams and you do not want to allocate the resources on your router required to provide reliable, or partially reliable, SCTP connections.

Congestion Avoidance

SCTP uses congestion avoidance algorithms that are similar to those for TCP. An SCTP end-point advertises the size of its receive window (rWnd) to ensure that a sender cannot flood it with more messages than it can store in its input queues.

Each SCTP sender also maintains a congestion window (cWnd), which determines the number of unacknowledged packets that can be outstanding at a given time. SCTP uses the same 'slow-start' algorithm as TCP, in which it starts with a small cWnd and gradually increases it until it reaches its optimum size.

Whenever a packet isn't acknowledged within the given timeout period, the value of cWnd is halved. This method of congestion avoidance is known as added increase / multiplicative decrease and has been shown to be the most effective congestion avoidance algorithm in most circumstances.

SCTP also employs the fast-retransmit algorithm whereby it retransmits a message if it receives acknowledgments from four messages which were sent after the message in question. This is preferable to waiting for the timeout period to elapse and triggering a retransmit of the message.

Options for Backup Collectors

You can configure a backup collector for SCTP. It is used as a message destination in the event that the primary collector becomes unavailable. When connectivity with the primary collector has been lost, and a backup

collector is configured, SCTP begins using the backup collector. The default period of time that SCTP waits until it starts using the backup collector is 25 milliseconds (msec). You can configure a different value for interval with the **fail-over** *time* command.

The router sends periodic SCTP heartbeat messages to the SCTP collectors that you have configured. The router uses the SCTP heartbeat message acknowledgements from the collectors to monitor the status of each collector. This allows an application, such as NetFlow, to be quickly informed when connectivity to a collector 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 collector until the router has not received acknowledgements for the SCTP heartbeat messages from the primary collector for the time specified by the **fail-over** *time* command (or the default of 25 msec if this parameter has not been modified).

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.

When the router is configured with SCTP backup in redundant mode, the router activates the association with the backup collector immediately, and if NetFlow v9 export is configured the router sends the (options) templates in advance. The router will not start sending other SCTP messages to a backup collector in redundant mode until the router has not received acknowledgments for the SCTP heartbeat messages from the primary collector for the time specified by the **fail-over** *time* command. Fail-over mode is the preferred method when the backup collector is on the end of an expensive lower-bandwidth link such as ISDN.

During the time that SCTP is using the backup collector, SCTP continues to try to restore the association with the primary collector. This goes on until connectivity is restored or the primary SCTP collector is removed from the configuration.

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

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

To avoid a flapping SCTP association with a collector (the SCTP association goes 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). That causes the IP route to the primary collector to be added and removed from the routing table repeatedly (route flapping) every 2000 msec (2 sec). you need to configure the restore time for a value greater than 2000 msecs.

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

Export to Multiple Collectors

You can configure your networking device to export NetFlow data to a maximum of two export destinations (collectors) per cache (main and aggregation caches), using any combination of UDP and SCTP. A destination is identified by a unique combination of hostname or IP address and port number or port type. The table below shows examples of permitted multiple 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>".

SCTP Support For Export Formats

SCTP based reliable transport is available for all NetFlow export formats: Versions 1, 5, 8 and 9.

How to Configure NetFlow Reliable Export with SCTP

You can configure two primary SCTP export destinations (collectors) and two backup SCTP export destinations for each NetFlow cache (main cache and aggregation caches). The backup SCTP export destinations inherit the reliability characteristics of the primary SCTP export destination. For example, if you configure partial reliability with a buffer limit of 2000 packets for the primary SCTP export destination, the backup SCTP destination also uses partial reliability and a buffer limit of 2000 packets.

You can use several permutations when you configure NetFlow Reliable Export With SCTP. The most basic configuration requires only one SCTP export destination. The other tasks below explain how to configure some of the more common permutations of NetFlow Reliable Export With SCTP.

Configuring NetFlow SCTP Export for One Export Destination

This is the most basic NetFlow SCTP export configuration. This NetFlow SCTP export configuration uses full reliability.

Before You Begin

You must have NetFlow enabled on at least one interface in your router before you can export NetFlow data.

You must have a NetFlow collector in your network that supports NetFlow SCTP export.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-export destination** [*ip-address* | *hostname*] *port* **sctp**
4. **end**
5. **show ip flow export sctp** verbose

DETAILED STEPS

Step 1 **enable**
Enters privileged EXEC mode.

Example:

Router> **enable**

Step 2 **configure terminal**
Enters global configuration mode.

Example:

Router# **configure terminal**

Step 3 **ip flow-export destination** [*ip-address* | *hostname*] *port* **sctp**
Configures an export destination using SCTP on port 100.

Example:

Router (config)# **ip flow-export destination 172.16.12.200 100 sctp**

Step 4 **end**
Returns to privileged EXEC mode.

Example:

Router(config-flow-export-sctp)# **end**

Step 5 **show ip flow export sctp** verbose
Displays the status and statistics for NetFlow SCTP export. Reliability is set to the default of full.

Example:

Router# **show ip flow export sctp verbose**

```
IPv4 main cache exporting to 172.16.12.200, port 100, full
status: connected
backup mode: redundant
4 flows exported in 4 sctp messages.
0 packets dropped due to lack of SCTP resources
fail-over time: 25 milli-seconds
restore time:   25 seconds
```

Configuring NetFlow SCTP Export for One Export Destination with Partial Reliability

This NetFlow SCTP export configuration uses partial reliability.

Before You Begin

You must have NetFlow enabled on at least one interface in your router before you can export NetFlow data.

You must have a NetFlow collector in your network that supports NetFlow SCTP export.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-export destination** [*ip-address* | *hostname*] *port* **sctp**
4. **reliability partial buffer-limit** *limit*
5. **end**
6. **show ip flow export sctp** verbose

DETAILED STEPS

Step 1 **enable**
Enters privileged EXEC mode.

Example:

Router> **enable**

Step 2 **configure terminal**
Enters global configuration mode.

Example:

Router# **configure terminal**

Step 3 **ip flow-export destination** [*ip-address* | *hostname*] *port* **sctp**
Configures an export destination using SCTP on port 100.

Example:

```
Router (config)# ip flow-export destination 172.16.12.200 100 sctp
```

Step 4 **reliability partial buffer-limit** *limit*
Configures partial reliability for this SCTP export destination and sets the packet buffer limit to 3000.

Example:

```
Router(config-flow-export-sctp)# reliability partial buffer-limit 3000
```

Step 5 **end**
Returns to privileged EXEC mode.

Example:

```
Router(config-flow-export-sctp)# end
```

Step 6 **show ip flow export sctp** verbose
Displays the status and statistics for NetFlow SCTP export. Reliability is now set to partial.

Example:

```
Router# show ip flow export sctp verbose

Pv4 main cache exporting to 172.16.12.200, port 100, partial
status: connected
backup mode: redundant
11 flows exported in 11 sctp messages.
0 packets dropped due to lack of SCTP resources
fail-over time: 25 milli-seconds
restore time:   25 seconds
```

Configuring NetFlow SCTP Export for One Export Destination with No Reliability

Reliability is disabled in this NetFlow SCTP export configuration.

Before You Begin

You must have NetFlow enabled on at least one interface in your router before you can export NetFlow data.

You must have a NetFlow collector in your network that supports NetFlow SCTP export.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-export destination** [*ip-address | hostname*] *port* **sctp**
4. **reliability none**
5. **end**
6. **show ip flow export sctp verbose**

DETAILED STEPS

Step 1   **enable**
Enters privileged EXEC mode.

Example:

```
Router> enable
```

Step 2   **configure terminal**
Enters global configuration mode.

Example:

```
Router# configure terminal
```

Step 3   **ip flow-export destination** [*ip-address | hostname*] *port* **sctp**
Configures an export destination using SCTP on port 100.

Example:

```
Router (config)# ip flow-export destination 172.16.12.200 100 sctp
```

Step 4   **reliability none**
Configures partial reliability for this SCTP export destination and sets the packet buffer limit to none.

Example:

```
Router(config-flow-export-sctp)# reliability none
```

Step 5   **end**
Returns to privileged EXEC mode.

Example:

```
Router(config-flow-export-sctp)# end
```

Step 6   **show ip flow export sctp verbose**
Displays the status and statistics for NetFlow SCTP export. Reliability is now set to none.

Example:

```
Router# show ip flow export sctp verbose

Pv4 main cache exporting to 172.16.12.200, port 100, none
status: connected
backup mode: redundant
15 flows exported in 15 sctp messages.
0 packets dropped due to lack of SCTP resources
fail-over time: 25 milli-seconds
restore time:   25 seconds
```

Configuring NetFlow SCTP Export for One Export Destination and One Backup Export Destination

This NetFlow SCTP export configuration uses full reliability, a backup SCTP export destination, and redundant mode backup.

Before You Begin

You must have NetFlow enabled on at least one interface in your router before you can export NetFlow data.

You must have a NetFlow collector in your network that supports NetFlow SCTP export.

SUMMARY STEPS

1. **enable**
2. **configure   terminal**
3. **ip flow-export destination** [*ip-address* | *hostname*] *port* **sctp**
4. **backup destination** [*ip-address* | *hostname*] *sctp-port*
5. **end**
6. **show ip flow export sctp verbose**

DETAILED STEPS

Step 1   **enable**
Enters privileged EXEC mode.

Example:

```
Router> enable
```

Step 2   **configure   terminal**
Enters global configuration mode.

Example:

```
Router# configure terminal
```

Step 3   **ip flow-export destination** [*ip-address* | *hostname*] *port* **sctp**
Configures an export destination using SCTP on port 100.

Example:

```
Router (config)# ip flow-export destination 172.16.12.200 100 sctp
```

Step 4   **backup destination** [*ip-address* | *hostname*] *sctp-port*
Configures an SCTP backup destination using SCTP on port 200.

Example:

```
Router(config-flow-export-sctp)# backup destination 192.168.247.198 200
```

Step 5   **end**
Returns to privileged EXEC mode.

Example:

```
Router(config-flow-export-sctp)# end
```

Step 6   **show ip flow export sctp verbose**
Displays the status and statistics for NetFlow SCTP export. Backup mode is redundant. The association with the SCTP backup export destination is active (connected). The SCTP backup export destination is not being used because the primary export destination is still active (connected).

Example:

```
Router# show ip flow export sctp verbose

IPv4 main cache exporting to 172.16.12.200, port 100, full
status: connected
backup mode: redundant
35 flows exported in 35 sctp messages.
0 packets dropped due to lack of SCTP resources
fail-over time: 25 milli-seconds
restore time:   25 seconds
backup: 192.168.247.198, port 200
   status: connected
   fail-overs: 0
   0 flows exported in 0 sctp messages.
   0 packets dropped due to lack of SCTP resources
```

Configuring NetFlow SCTP Export for One Export Destination and One Backup Exp Dest With Fail-Over Mode Backup

Perform this task to configure NetFlow SCTP export for one export and one backup destination with fail-over mode backup.

Before You Begin

You must have NetFlow enabled on at least one interface in your router before you can export NetFlow data.

You must have a NetFlow collector in your network that supports NetFlow SCTP export.

This NetFlow SCTP export configuration uses full reliability, a backup SCTP export destination, and fail-over mode backup.

> **Note**　The backup fail-over and restore times are modified here so that you can see an example of how to configure these commands. The values used in this example might not be suitable for your network. If you want to override the default values for the fail-over and restore times you need to analyze the performance of your network and the collector that you are using to determine values that are appropriate for your network.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-export destination** [*ip-address* | *hostname*] *port* **sctp**
4. **backup destination** [*ip-address* | *hostname*] *sctp-port*
5. **backup mode fail-over**
6. **backup fail-over** *fail-over-time*
7. **backup restore-time** *restore-time*
8. **end**
9. **show ip flow export sctp verbose**

DETAILED STEPS

Step 1　**enable**
Enters privileged EXEC mode.

Example:

```
Router> enable
```

Step 2　**configure terminal**
Enters global configuration mode.

Example:

```
Router# configure terminal
```

Step 3   **ip flow-export destination** [*ip-address* | *hostname*] *port* **sctp**
Configures an export destination using SCTP on port 100.

Example:

```
Router (config)# ip flow-export destination 172.16.12.200 100 sctp
```

Step 4   **backup destination** [*ip-address* | *hostname*] *sctp-port*
Configures an SCTP backup destination using SCTP on port 200.

Example:

```
Router(config-flow-export-sctp)# backup destination 192.168.247.198 200
```

Step 5   **backup mode fail-over**
Configures the router to fail-over mode for the backup export destination.

Example:

```
Router(config-flow-export-sctp)# backup mode fail-over
```

Step 6   **backup fail-over** *fail-over-time*
The length of time that the router will wait until failing over to the backup SCTP export destination has been increased to 3500 msec.

Example:

```
Router(config-flow-export-sctp)# backup fail-over 3500
```

Step 7   **backup restore-time** *restore-time*
The length of time that the router will wait until reverting to the primary SCTP export destination has been increased to 1500 msecs.

Example:

```
Router (config)# backup restore-time 1500
```

Step 8   **end**
Returns to privileged EXEC mode.

Example:

```
Router(config-flow-export-sctp)# end
```

Step 9   **show ip flow export sctp verbose**

Displays the status and statistics for NetFlow SCTP export. Backup mode is fail-over. The association with the SCTP backup export destination is not active (not connected) because NetFlow SCTP export waits to activate the association with the backup destination until the primary export destination is no longer available.

Example:

```
Router# show ip flow export sctp verbose

IPv4 main cache exporting to 172.16.12.200, port 100, full
status: connected
backup mode: fail-over
114 flows exported in 93 sctp messages.
0 packets dropped due to lack of SCTP resources
fail-over time: 3500 milli-seconds
restore time:   1500 seconds
backup: 192.168.247.198, port 200
   status: not connected
   fail-overs: 0
   0 flows exported in 0 sctp messages.
   0 packets dropped due to lack of SCTP resources
```

Configuring NetFlow SCTP Export for Two Export Destinations and Two Backup Export Destinations

This configuration is the most basic SCTP export configuration that uses multiple export destinations. You can configure a maximum of two export destinations for every NetFlow cache.

Each SCTP export destination has its own area in the configuration file for the options that you can configure for it such as fail-over mode, fail-over timers and reliability. Therefore you must make certain that the last SCTP export destination that you entered in the router's configuration is the SCTP export destination that you want to modify.

For example, if you enter these commands in this order:

- **ip flow-export destination** *172.16.12.200 100* **sctp**

- **ip flow-export destination** *172.16.45.57 100* **sctp**

- **backup destination** *192.168.100.2 200*

The **backup destination** *192.168.100.2 200* is assigned to the **ip flow-export destination** *172.16.45.57 100* **sctp**command.

To change the SCTP export destination that you are modifying, reenter the command line for the SCTP export destination that you want to modify.

Before You Begin

You must have NetFlow enabled on at least one interface in your router before you can export NetFlow data.

You must have a NetFlow collector in your network that supports NetFlow SCTP export.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-export destination** [*ip-address | hostname*] *port* **sctp**
4. **backup destination** [*ip-address | hostname*] *sctp-port*
5. **ip flow-export destination** [*ip-address | hostname*] *port* **sctp**
6. **backup destination** [*ip-address | hostname*] *sctp-port*
7. **end**
8. **show ip flow export sctp verbose**

DETAILED STEPS

Step 1 **enable**
Enters privileged EXEC mode.

Example:

```
Router> enable
```

Step 2 **configure terminal**
Enters global configuration mode.

Example:

```
Router# configure terminal
```

Step 3 **ip flow-export destination** [*ip-address | hostname*] *port* **sctp**
Configures an export destination using SCTP on port 100.

Example:

```
Router (config)# ip flow-export destination 172.16.12.200 100 sctp
```

Step 4 **backup destination** [*ip-address | hostname*] *sctp-port*
Configures an SCTP backup destination using SCTP on port 200.

Example:

```
Router(config-flow-export-sctp)# backup destination 192.168.247.198 200
```

Step 5 **ip flow-export destination** [*ip-address | hostname*] *port* **sctp**
Configures a second export destination using SCTP on port 100.

Example:

```
Router (config)# ip flow-export destination 172.16.45.57 100 sctp
```

Step 6 **backup destination** [*ip-address | hostname*] *sctp-port*

Configures a second SCTP backup destination using SCTP on port 200.

Example:

```
Router(config-flow-export-sctp)# backup destination 192.168.100.2 200
```

Step 7   **end**
Returns to privileged EXEC mode.

Example:

```
Router(config-flow-export-sctp)# end
```

Step 8   **show ip flow export sctp verbose**
Displays the status and statistics for the two primary and backup NetFlow SCTP export destinations. Reliability is set to the default of full.

Example:

```
Router# show ip flow export sctp verbose

IPv4 main cache exporting to 172.16.12.200, port 100, full
status: connected
backup mode: redundant
219 flows exported in 176 sctp messages.
0 packets dropped due to lack of SCTP resources
fail-over time: 3500 milli-seconds
restore time:   10 seconds
backup: 192.168.247.198, port 200
   status: connected
   fail-overs: 0
   0 flows exported in 0 sctp messages.
   0 packets dropped due to lack of SCTP resources
IPv4 main cache exporting to 172.16.45.57, port 100, full
status: connected
backup mode: redundant
66 flows exported in 47 sctp messages.
0 packets dropped due to lack of SCTP resources
fail-over time: 25 milli-seconds
restore time:   25 seconds
backup: 192.168.100.2, port 200
   status: connected
   fail-overs: 1
   0 flows exported in 0 sctp messages.
   0 packets dropped due to lack of SCTP resources
```

Configuring NetFlow SCTP Export for One Fully Reliable and One Partially Reliable Export Destination

This SCTP export configuration uses two SCTP export destinations. One of the export destinations uses full reliability and the other export destination uses partial reliability.

Before You Begin

You must have NetFlow enabled on at least one interface in your router before you can export NetFlow data.

You must have a NetFlow collector in your network that supports NetFlow SCTP export.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-export destination** [*ip-address* | *hostname*] *port* **sctp**
4. **ip flow-export destination** [*ip-address* | *hostname*] *port* **sctp**
5. **reliability partial buffer-limit** *limit*
6. **end**
7. **show ip flow export sctp verbose**

DETAILED STEPS

Step 1   **enable**
Enters privileged EXEC mode.

Example:

```
Router> enable
```

Step 2   **configure terminal**
Enters global configuration mode.

Example:

```
Router# configure terminal
```

Step 3   **ip flow-export destination** [*ip-address* | *hostname*] *port* **sctp**
Configures an export destination using SCTP on port 100.

Example:

```
Router (config)# ip flow-export destination 172.16.12.200 100 sctp
```

Step 4   **ip flow-export destination** [*ip-address* | *hostname*] *port* **sctp**
Configures a second export destination using SCTP on port 100.

Example:

```
Router (config)# ip flow-export destination 172.16.45.57 100 sctp
```

Step 5   **reliability partial buffer-limit** *limit*
Configures partial reliability for this SCTP export destination and sets the packet buffer limit to 3000.

Example:

```
Router(config-flow-export-sctp)# reliability partial buffer-limit 3000
```

Step 6   **end**
Returns to privileged EXEC mode.

Example:

```
Router(config-flow-export-sctp)# end
```

Step 7   **show ip flow export sctp verbose**
Displays the status and statistics for NetFlow export with SCTP. Reliability is set to full for SCTP export destination 172.16.12.200 and to partial SCTP export destination 172.16.45.57.

Example:

```
Router# show ip flow export sctp verbose

IPv4 main cache exporting to 172.16.12.200, port 100, full
status: connected
backup mode: redundant
229 flows exported in 186 sctp messages.
0 packets dropped due to lack of SCTP resources
fail-over time: 3500 milli-seconds
restore time:   10 seconds
backup: 192.168.247.198, port 200
   status: connected
   fail-overs: 0
   0 flows exported in 0 sctp messages.
   0 packets dropped due to lack of SCTP resources
IPv4 main cache exporting to 172.16.45.57, port 100, partial
status: connected
backup mode: redundant
76 flows exported in 57 sctp messages.
0 packets dropped due to lack of SCTP resources
fail-over time: 25 milli-seconds
restore time:   25 seconds
backup: 192.168.100.2, port 200
   status: connected
   fail-overs: 1
   0 flows exported in 0 sctp messages.
   0 packets dropped due to lack of SCTP resources
```

Configuring NetFlow SCTP Export for the NetFlow Source-Prefix Aggregation Cache

This SCTP export example shows how to configure NetFlow SCTP export for the NetFlow source prefix aggregation cache. You can configure a maximum of two export destinations for every NetFlow cache.

When you enter NetFlow aggregation cache configuration mode in the router the current router prompt changes to reflect this mode.

For example, if the current router prompt is, Router(config)# and you enter the **ip flow-aggregation cache prefix** command, the router prompt is changed to the NetFlow aggregation cache configuration prompt of Router(config-flow-cache)#.

You need to pay close attention when you are configuring NetFlow SCTP export options for NetFlow aggregation caches because the NetFlow aggregation cache configuration prompt is changed to the NetFlow SCTP export prompt when you enter a NetFlow SCTP export command in NetFlow aggregation cache configuration mode, even though you are still working in NetFlow aggregation cache configuration mode.

For example, if your current prompt is the NetFlow aggregation cache configuration prompt, Router(config-flow-cache)#, and you enter the **export destination** *172.16.12.200 100* **sctp** command, the router prompt will change to the NetFlow SCTP export configuration mode prompt, Router(config-flow-export-sctp)#. The NetFlow SCTP export commands that you configure are assigned to the NetFlow aggregation cache that you are modify with NetFlow SCTP export options.

Use the configuration in the Configuration Examples for NetFlow Reliable Export With SCTP, on page 27 to practice using the different configuration modes

Prerequisites

You must have NetFlow enabled on at least one interface in your router before you can export NetFlow data.

You must have a NetFlow collector in your network that supports NetFlow SCTP export.

SCTP Export for NetFlow Aggregation Caches

All of the NetFlow SCTP options that are available for the main NetFlow cache are also available in NetFlow Aggregation cache mode.

SUMMARY STEPS

1. **enable**
2. **configure   terminal**
3. **ip flow-aggregation cache aggregation-cache-type**
4. **enable**
5. **export destination** [*ip-address | hostname*] *port* **sctp**
6. **end**
7. **show ip flow export sctp verbose**

DETAILED STEPS

Step 1   **enable**
Enters privileged EXEC mode.

Example:

```
Router> enable
```

Step 2   **configure   terminal**
Enters global configuration mode.

Example:

```
Router# configure terminal
```

Step 3 **ip flow-aggregation cache aggregation-cache-type**

Enters NetFlow aggregation cache mode for the cache type.

Example:

```
Router (config)# ip flow-aggregation cache source-prefix
```

Step 4 **enable**

Activates the NetFlow aggregation cache.

Example:

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

Step 5 **export destination** [*ip-address | hostname*] *port* **sctp**

Configures an export destination using SCTP for the aggregation cache.

Example:

```
Router (config-flow-cache)# export destination 172.16.12.200 100 sctp
```

Step 6 **end**

Returns to privileged EXEC mode.

Example:

```
Router(config-flow-export-sctp)# end
```

Step 7 **show ip flow export sctp verbose**

Displays the status and statistics for NetFlow export with SCTP.

Example:

```
Router# show ip flow export sctp verbose

source-prefix cache exporting to 172.16.12.200, port 100, full
status: connected
backup mode: redundant
0 flows exported in 0 sctp messages.
0 packets dropped due to lack of SCTP resources
fail-over time: 25 milli-seconds
restore time:   25 seconds
```

Verifying NetFlow Reliable Export With SCTP

The **show ip flow export sctp** [**verbose**]command provides information on the status and statistics of the options that you have configured for the NetFlow Reliable Export With SCTP feature.

Cisco IOS also provides commands for monitoring and troubleshooting the status and statistics for all of the SCTP features (including NetFlow Reliable Export With SCTP) that you have configured on the networking device. Refer to the Stream Control Transmission Protocol (SCTP) , Release 2 configuration guide http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_sctp2.htm for more information on interpreting the output from these commands, and the other commands that are available for monitoring and troubleshooting SCTP.

SUMMARY STEPS

1. **show ip sctp association list**
2. **show ip sctp association parameters** *association-id*
3. **show ip sctp errors**
4. **show ip sctp instances**
5. show ip sctp statistics

DETAILED STEPS

Step 1   **show ip sctp association list**
Shows the list of SCTP associations.

Example:

```
Router# show ip sctp association list
** SCTP Association List **
AssocID: 0,  Instance ID: 0
Current state: ESTABLISHED
Local port: 51882, Addrs: 172.16.6.2
Remote port: 100, Addrs: 172.16.12.200
AssocID: 1,  Instance ID: 1
Current state: ESTABLISHED
Local port: 59004, Addrs: 172.16.6.2
Remote port: 200, Addrs: 192.168.247.198
```

Step 2   **show ip sctp association parameters** *association-id*
Displays the current parameters for the association ID.

Example:

```
Router# show ip sctp association parameters 0
** SCTP Association Parameters **
AssocID: 0  Context: 1  InstanceID: 0
Assoc state: ESTABLISHED  Uptime: 00:19:44.504
Local port: 51882
Peers Adaption layer indication is NOT set
Local addresses: 172.16.6.2
Remote port: 100
Primary dest addr: 172.16.12.200
Effective primary dest addr: 172.16.12.200
Destination addresses:
```

```
172.16.12.200:   State:  ACTIVE(CONFIRMED)
  Heartbeats: Enabled   Timeout: 500 ms
  RTO/RTT/SRTT: 5000/0/3 ms   TOS: 0  MTU: 1500
  cwnd: 3000  ssthresh: 9000  outstand: 0
  Num retrans: 0  Max retrans: 2  Num times failed: 0
Local vertag: DAF7029F  Remote vertag: A3923131
Num inbound streams: 20  outbound streams: 20
Max assoc retrans: 2  Max init retrans: 2
CumSack timeout: 200 ms  Bundle timeout: 100 ms
Min RTO: 5000 ms  Max RTO: 5000 ms
Max Init RTO (T1): 1000 ms
LocalRwnd: 9000  Low: 9000   RemoteRwnd: 9000  Low: 8936
Congest levels: 0  current level: 0  high mark: 1
```

Step 3   **show ip sctp errors**

Shows any SCTP errors that have occurred.

Example:

```
Router# show ip sctp errors
** SCTP Error Statistics **
No SCTP errors logged.
```

Step 4   **show ip sctp instances**

Shows the details and status for the SCTP instances.

Example:

```
Router# show ip sctp instances
** SCTP Instances **
Instance ID: 0  Local port: 51882  State: available
Local addrs: 172.16.6.2
Default streams inbound: 20  outbound: 20
Adaption layer indication is not set
  Current associations:  (max allowed: 6)
  AssocID: 0  State: ESTABLISHED  Remote port: 100
    Dest addrs: 172.16.12.200
Instance ID: 1  Local port: 59004  State: available
Local addrs: 172.16.6.2
Default streams inbound: 20  outbound: 20
Adaption layer indication is not set
  Current associations:  (max allowed: 6)
  AssocID: 1  State: ESTABLISHED  Remote port: 200
    Dest addrs: 192.168.247.198
```

Step 5   show ip sctp statistics

Shows the SCTP overall statistics:

Example:

```
Router# show ip sctp statistics
** SCTP Overall Statistics **
Control Chunks
  Sent: 615  Rcvd: 699
Data Chunks Sent
  Total: 57  Retransmitted: 0
  Ordered: 57  Unordered: 0
  Total Bytes: 3648
Data Chunks Rcvd
  Total: 0  Discarded: 0
  Ordered: 0  Unordered: 0
  Total Bytes: 0
  Out of Seq TSN: 0
SCTP Dgrams
```

```
  Sent: 671  Rcvd: 699
ULP Dgrams
  Sent: 57  Ready: 0  Rcvd: 0
Additional Stats
  Assocs Currently Estab: 2
  Active Estab: 2  Passive Estab: 0
  Aborts: 0  Shutdowns: 0
  T1 Expired: 1  T2 Expired: 0
```

Configuration Examples for NetFlow Reliable Export With SCTP

The following example includes these NetFlow accounting and NetFlow SCTP export features:

- NetFlow ingress and egress accounting

- Multiple SCTP export destinations for the Main NetFlow cache with backup destinations

- Multiple SCTP export destinations for the NetFlow protocol-port aggregation cache using partial reliability and fail-over mode backup destinations

- Multiple SCTP export destinations for the NetFlow bgp-nexthop-tos aggregation cache with reliability disabled and redundant mode backup destinations

```
Router# show running-config
.
.
.
interface Ethernet0/0.1
 ip address 172.16.6.2 255.255.255.0
 ip flow ingress
!
!
interface Ethernet1/0.1
 ip address 172.16.7.1 255.255.255.0
 ip flow egress
!
ip flow-export destination 172.16.45.57 100 sctp
 reliability partial buffer-limit 3000
 backup destination 192.168.100.2 200
!
ip flow-export destination 172.16.12.200 100 sctp
 reliability partial buffer-limit 3000
 backup destination 192.168.247.198 200
!
ip flow-aggregation cache protocol-port
 export destination 172.16.12.200 100 sctp
 reliability partial buffer-limit 3000
 backup destination 192.168.247.198 200
 backup mode fail-over
 export destination 172.16.45.57 100 sctp
 reliability partial buffer-limit 3000
 backup destination 192.168.100.2 200
 backup mode fail-over
 enabled
!
ip flow-aggregation cache bgp-nexthop-tos
 export version 9
 export destination 172.16.12.200 100 sctp
 backup destination 192.168.247.198 200
 export destination 172.16.45.57 100 sctp
 backup destination 192.168.100.2 200
```

```
 enabled
!
```

The display output of the **show ip flow export sctp verbose** command shows the status and statistics for this configuration example:

```
Router# show ip flow export sctp verbose
IPv4 main cache exporting to 172.16.45.57, port 100, partial
status: connected
backup mode: redundant
104 flows exported in 84 sctp messages.
0 packets dropped due to lack of SCTP resources
fail-over time: 25 milli-seconds
restore time:   25 seconds
backup: 192.168.100.2, port 200
   status: connected
   fail-overs: 2
   0 flows exported in 0 sctp messages.
   0 packets dropped due to lack of SCTP resources
IPv4 main cache exporting to 172.16.12.200, port 100, partial
status: connected
backup mode: redundant
104 flows exported in 84 sctp messages.
0 packets dropped due to lack of SCTP resources
fail-over time: 25 milli-seconds
restore time:   25 seconds
backup: 192.168.247.198, port 200
   status: connected
   fail-overs: 1
   0 flows exported in 0 sctp messages.
   0 packets dropped due to lack of SCTP resources
protocol-port cache exporting to 172.16.12.200, port 100, partial
status: connected
backup mode: fail-over
19 flows exported in 18 sctp messages.
0 packets dropped due to lack of SCTP resources
fail-over time: 25 milli-seconds
restore time:   25 seconds
backup: 192.168.247.198, port 200
   status: connected
   fail-overs: 0
   0 flows exported in 0 sctp messages.
   0 packets dropped due to lack of SCTP resources
protocol-port cache exporting to 172.16.45.57, port 100, partial
status: connected
backup mode: fail-over
15 flows exported in 15 sctp messages.
0 packets dropped due to lack of SCTP resources
fail-over time: 25 milli-seconds
restore time:   25 seconds
backup: 192.168.100.2, port 200
   status: connected
   fail-overs: 0
   0 flows exported in 0 sctp messages.
   0 packets dropped due to lack of SCTP resources
bgp-nexthop-tos cache exporting to 172.16.12.200, port 100, full
status: connected
backup mode: redundant
20 flows exported in 10 sctp messages.
0 packets dropped due to lack of SCTP resources
fail-over time: 25 milli-seconds
restore time:   25 seconds
backup: 192.168.247.198, port 200
   status: connected
   fail-overs: 0
   0 flows exported in 0 sctp messages.
   0 packets dropped due to lack of SCTP resources
bgp-nexthop-tos cache exporting to 172.16.45.57, port 100, full
status: connected
backup mode: redundant
20 flows exported in 10 sctp messages.
0 packets dropped due to lack of SCTP resources
```

```
fail-over time: 25 milli-seconds
restore time:   25 seconds
backup: 192.168.100.2, port 200
   status: connected
   fail-overs: 0
   0 flows exported in 0 sctp messages.
   0 packets dropped due to lack of SCTP resources
```

Additional References

Related Documents

Related Topic	Document Title
Overview of Cisco IOS NetFlow	Cisco IOS NetFlow Overview
The minimum information about and tasks required for configuring NetFlow and NetFlow Data Export	Getting Started with Configuring NetFlow and NetFlow Data Export
Tasks for configuring NetFlow to capture and export network traffic data	Configuring NetFlow and NetFlow Data Export
Tasks for configuring Configuring MPLS Aware NetFlow	Configuring MPLS Aware NetFlow
Tasks for configuring MPLS egress NetFlow accounting	Configuring MPLS Egress NetFlow Accounting and Analysis
Tasks for configuring NetFlow input filters	Using NetFlow Filtering or Sampling to Select the Network Traffic to Track
Tasks for configuring Random Sampled NetFlow	Using NetFlow Filtering or Sampling to Select the Network Traffic to Track
Tasks for configuring NetFlow aggregation caches	Configuring NetFlow Aggregation Caches
Tasks for configuring NetFlow BGP next hop support	Configuring NetFlow BGP Next Hop Support for Accounting and Analysis
Tasks for configuring NetFlow multicast support	Configuring NetFlow Multicast Accounting
Tasks for detecting and analyzing network threats with NetFlow	Detecting and Analyzing Network Threats With NetFlow
Tasks for configuring NetFlow Layer 2 and Security Monitoring Exports	NetFlow Layer 2 and Security Monitoring Exports
Tasks for configuring the SNMP NetFlow MIB	Configuring SNMP and using the NetFlow MIB to Monitor NetFlow Data

Related Topic	Document Title
Tasks for configuring the NetFlow MIB and Top Talkers feature	Configuring NetFlow Top Talkers using Cisco IOS CLI Commands or SNMP Commands
Information for installing, starting, and configuring the CNS NetFlow Collection Engine	Cisco CNS NetFlow Collection Engine Documentation

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 3954	Cisco Systems NetFlow Services Export Version 9
RFC2690	Stream Control Transmission Protocol
RFC 3578	Stream Control Transmission Protocol-Partial Reliability Extension

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for NetFlow Reliable Transport Using SCTP

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2: Feature Information for NetFlow Reliable Transport Using SCTP

Feature Name	Releases	Feature Configuration Information
NetFlow Reliable Export With SCTP	12.4(4)T	The NetFlow Reliable Export With SCTP feature provides a more robust and flexible method for exporting NetFlow data to collectors than UDP, which was the only transport option prior to the introduction of this feature. NetFlow Reliable Export With SCTP has the following benefits: • Backup destinations--You can configure backup destinations for every SCTP export destination. The backup destinations can use redundant mode (always connected) and fail-over mode (connect as required). Fail-over mode is more suitable for backup destinations that are reachable over expensive dial-up links such as ISDN. • Reliability--NetFlow SCTP provides a very reliable level of transport that has error correction and flow control. You can modify the level of reliability for each SCTP export destination depending on the importance of the data that you are exporting. The following commands were introduced or modified by this feature: **ip flow export**, **show ip flow export**, and **export**.

Glossary

CEF --Cisco Express Forwarding. A Layer 3 IP switching technology that optimizes network performance and scalability for networks with large and dynamic traffic patterns.

BGP --Border Gateway Protocol. Interdomain routing protocol that replaces Exterior Border Gateway Protocol (EBGP). A BGP system exchanges reachability information with other BGP systems. BGP is defined by RFC 1163.

BGP next hop --IP address of the next hop to be used to reach a certain destination.

data record --Provides information about an IP flow that exists on the device that produced an export packet. Each group of data records (meaning each data flowset), refers to a previously transmitted template ID, which can be used to parse the data within the records.

dCEF --distributed Cisco Express Forwarding. A type of CEF switching in which line cards (such as Versatile Interface Processor (VIP) line cards) maintain identical copies of the forwarding information base (FIB) and adjacency tables. The line cards perform the express forwarding between port adapters; this relieves the Route Switch Processor of involvement in the switching operation.

export packet --A type of packet built by a device (for example, a router) with NetFlow services enabled. The packet is addressed to another device (for example, the NetFlow Collection Engine). The packet contains NetFlow statistics. The other device processes the packet (parses, aggregates, and stores information on IP flows).

fast switching --A Cisco feature in which a route cache is used to expedite packet switching through a router.

flow --A unidirectional stream of packets between a given source and destination, each of which is defined by a network-layer IP address and transport-layer source and destination port numbers.

flowset --A collection of flow records that follow the packet header in an export packet. A flowset contains information that must be parsed and interpreted by the NetFlow Collection Engine. There are two different types of flowsets: template flowsets and data flowsets. An export packet contains one or more flowsets, and both template and data flowsets can be mixed in the same export packet.

NetFlow --A Cisco IOS application that provides statistics on packets flowing through the router. It is emerging as a primary network accounting and security technology.

NetFlow Aggregation --A NetFlow feature that lets you summarize NetFlow export data on an IOS router before the data is exported to a NetFlow data collection system such as the NetFlow Collection Engine. This feature lowers bandwidth requirements for NetFlow export data and reduces platform requirements for NetFlow data collection devices.

NetFlow Collection Engine (formerly NetFlow FlowCollector)--A Cisco application that is used with NetFlow on Cisco routers and Catalyst 5000 series switches. The NetFlow Collection Engine collects packets from the router that is running NetFlow and decodes, aggregates, and stores them. You can generate reports on various aggregations that can be set up on the NetFlow Collection Engine.

NetFlow v9 --NetFlow export format Version 9. A flexible and extensible means of carrying 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.

options data record --A special type of data record used in the NetFlow process. It is based on an options template and has a reserved template ID that provides information about the NetFlow process itself.

options template --A type of template record used to communicate the format of data related to the NetFlow process.

packet header --First part of an export packet. It provides basic information about the packet (such as the NetFlow version, number of records contained in the packet, and sequence numbering) so that lost packets can be detected.

SCTP --Stream Control Transmission Protocol. The Stream Control Transmission Protocol (SCTP) is a transport layer protocol defined in 2000 by the IETF Signaling Transport (SIGTRAN) working group. The protocol is defined in RFC 2960, and an introductory text is provided by RFC 3286.

template flowset --A collection of template records that are grouped in an export packet.

template ID --A unique number that distinguishes a template record produced by an export device from other template records produced by the same export device. A NetFlow Collection Engine application can receive export packets from several devices. You should be aware that uniqueness is not guaranteed across export devices. The NetFlow Collection Engine should cache the address of the export device that produced the template ID in order to enforce uniqueness.

template record --Defines the format of subsequent data records that might be received in current or future export packets. A template record within an export packet does not necessarily indicate the format of data records within that same packet. A NetFlow Collection Engine application must cache any template records received and then parse any data records it encounters by locating the appropriate template record in the cache.