NetFlow Configuration Guide, Cisco IOS XE Release 3S (ASR 1000)

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Configuring NetFlow Aggregation Caches

This module contains information about and instructions for configuring NetFlow aggregation caches. The NetFlow main cache is the default cache used to store the data captured by NetFlow. By maintaining one or more extra caches, called aggregation caches, the NetFlow Aggregation feature allows limited aggregation of NetFlow data export streams on a router. The aggregation scheme that you select determines the specific kinds of data that are exported to a remote host.

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

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 Configuring NetFlow Aggregation Caches

Before you enable NetFlow you must:

- Configure the router for IP routing
- Ensure that either Cisco Express Forwarding or fast switching is enabled on your router and on the interfaces on which you want to configure NetFlow.
- Understand the resources required on your router because NetFlow consumes additional memory and CPU resources

If you intend to use Version 8 export format with an aggregation cache, configure Version 5 export format for the main cache.

If you need autonomous system (AS) information from the aggregation, make sure to specify either the **peer-as**or **origin-as** keyword in your export command if you have not configured an export format version.

You must explicitly enable each NetFlow aggregation cache by entering the **enabled** keyword from aggregation cache configuration mode.

Router-based aggregation must be enabled for minimum masking.

Restrictions for Configuring NetFlow Aggregation Caches

Performance Impact

Configuring Egress NetFlow accounting with the **ip flow egress** command might adversely affect network performance because of the additional accounting-related computation that occurs in the traffic-forwarding path of the router.

- NetFlow Data Export Restrictions, page 2

NetFlow Data Export Restrictions

Restrictions for NetFlow Version 9 Data Export

- Backward compatibility--Version 9 is not backward-compatible with Version 5 or Version 8. If you need Version 5 or Version 8, you must configure it.
- Export bandwidth--Export bandwidth use increases for Version 9 (because of template flowsets) versus Version 5. The increase in bandwidth usage versus Version 5 varies with the frequency with which template flowsets are sent. The default is to resend templates every 20 packets, which has a bandwidth cost of about 4 percent. If necessary, you can lower the resend rate with the **ip flow-export template refresh-rate** *packets* command.
- Performance impact--Version 9 slightly decreases overall performance, because generating and maintaining valid template flowsets require additional processing.

Restrictions for NetFlow Version 8 Export Format

Version 8 export format is available only for aggregation caches, and it cannot be expanded to support new features.

Information About Configuring NetFlow Aggregation Caches

- NetFlow Aggregation Caches, page 2
- NetFlow Data Export Format Versions 9 and 8 for NetFlow Aggregation Caches Overview, page 24

NetFlow Aggregation Caches

NetFlow Aggregation Cache Benefits

Aggregation of export data is typically performed by NetFlow collection tools on management workstations. Router-based aggregation allows limited aggregation of NetFlow export records to occur on the router. Thus, you can summarize NetFlow export data on the router before the data is exported to a NetFlow data collection system, which has the following benefits:

- Reduces the bandwidth required between the router and the workstations
- Reduces the number of collection workstations required
- Improves performance and scalability on high flow-per-second routers

NetFlow Aggregation Cache Schemes

Cisco IOS XE NetFlow aggregation maintains one or more extra caches with different combinations of fields that determine which flows are grouped together. These extra caches are called aggregation caches. The combinations of fields that make up an aggregation cache are referred to as schemes.

You can configure each aggregation cache with its individual cache size, cache ager timeout parameter, export destination IP address, and export destination UDP port. The normal flow ager process runs on each active aggregation cache the same way it runs on the main cache. On-demand aging is also supported. Each aggregation cache contains different field combinations that determine which data flows are grouped. The default aggregation cache size is 4096 bytes.

You configure a cache aggregation scheme through the use of arguments to the **ip flow-aggregation cache** command. NetFlow supports the following five non-ToS based cache aggregation schemes:

- Autonomous system (AS) aggregation scheme
- Destination prefix aggregation scheme
- Prefix aggregation scheme
- Protocol port aggregation scheme
- Source prefix aggregation scheme

The NetFlow Type of Service-Based Router Aggregation feature introduced support for additional cache aggregation schemes, all of which include the Type of Service (ToS) byte as one of the fields in the aggregation cache. The following are the six ToS-based aggregation schemes:

- AS-ToS aggregation scheme

- Destination prefix-ToS aggregation scheme
- Prefix-port aggregation scheme
- Prefix-ToS aggregation scheme
- Protocol-port-ToS aggregation scheme
- Source prefix-ToS aggregation scheme

Note NetFlow Aggregation Scheme Fields, page 4 through NetFlow Aggregation Cache Schemes, page 3 illustrate the Version 8 export formats of the aggregation schemes listed above. Additional export formats (for instance, Version 9) are also supported. If you are using Version 9, the formats will be different from those shown in the figures. For more information about Version 9 export formats, see the "Configuring NetFlow and NetFlow Data Export" module.

NetFlow Aggregation Scheme Fields

Each cache aggregation scheme contains field combinations that differ from any other cache aggregation scheme. The combination of fields determines which data flows are grouped and collected when a flow expires from the main cache. A flow is a set of packets that has common fields, such as the source IP address, destination IP address, protocol, source and destination ports, type-of-service, and the same interface on which the flow is monitored. To manage flow aggregation on your router, you need to configure the aggregation cache scheme that groups and collects the fields from which you want to examine data. The two tables below show the NetFlow fields that are grouped and collected for non-ToS and ToS based cache aggregation schemes.

The table below shows the NetFlow fields used in the non-ToS based aggregation schemes.

Table 1 NetFlow Fields Used in the Non-ToS Based Aggregations Schemes

Field	AS	Protocol Port	Source Prefix	Destination Prefix	Prefix
Source prefix			X		X
Source prefix mask			X		X
Destination prefix				X	X
Destination prefix mask				X	X
Source app port		X			
Destination app port		X			
Input interface	X		X		X
Output interface	X			X	X

Field	AS	Protocol Port	Source Prefix	Destination Prefix	Prefix
IP protocol		X			
Source AS	X		X		X
Destination AS	X			X	X
First time stamp	X	X	X	X	X
Last time stamp	X	X	X	X	X
Number of flows[1]	X	X	X	X	X
Number of packets	X	X	X	X	X
Number of bytes	X	X	X	X	X

The table below shows the NetFlow fields used in the ToS based aggregation schemes.

Table 2 NetFlow Fields Used in the ToS Based Aggregation Schemes

Field	AS-ToS	Protocol Port-ToS	Source Prefix-ToS	Destination Prefix-ToS	Prefix-ToS	Prefix-Port
Source prefix			X		X	X
Source prefix mask			X		X	X
Destination prefix				X	X	X
Destination prefix mask				X	X	X
Source app port		X				X
Destination app port		X				X
Input interface	X	X	X		X	X
Output interface	X	X		X	X	X

1 For the Cisco ASR 1000 series router, this value is always 0. This is because on the Cisco ASR 1000 series router, aggregation caches are managed not by extracting data from main cache flow records as they are aged out, but rather by examining each packet, independently of any main cache processing.

Field	AS-ToS	Protocol Port-ToS	Source Prefix-ToS	Destination Prefix-ToS	Prefix-ToS	Prefix-Port
IP protocol		X				X
Source AS	X		X		X	
Destination AS	X			X	X	
ToS	X	X	X	X	X	X
First time stamp	X	X	X	X	X	X
Last time stamp	X	X	X	X	X	X
Number of flows[2]	X	X	X	X	X	X
Number of packets	X	X	X	X	X	X
Number of bytes	X	X	X	X	X	X

NetFlow AS Aggregation Scheme

The NetFlow AS aggregation scheme reduces NetFlow export data volume substantially and generates AS-to-AS traffic flow data. The scheme groups data flows that have the same source BGP AS, destination BGP AS, input interface, and output interface.

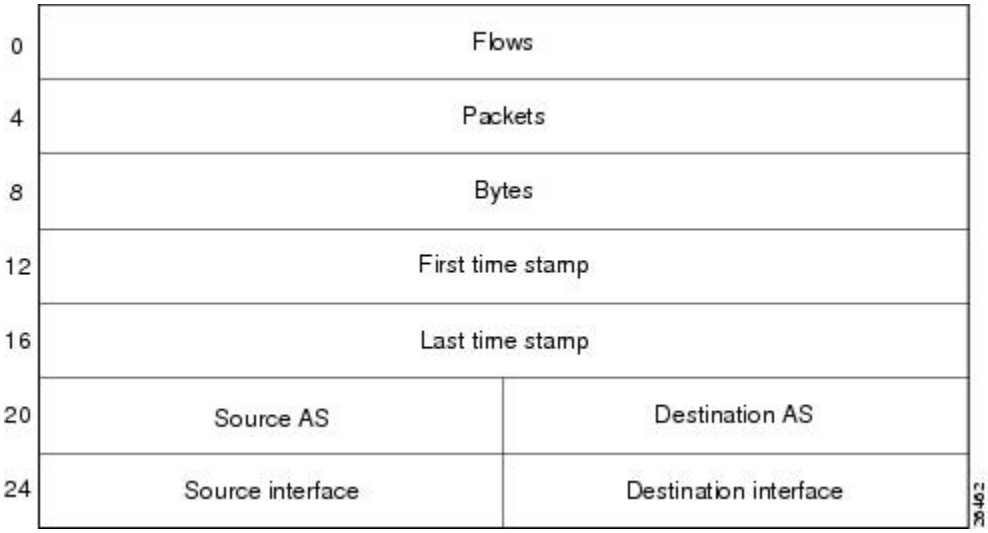
The aggregated NetFlow data export records report the following:

- Source and destination BGP AS
- Number of packets summarized by the aggregated record
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Source interface
- Destination interface
- Time stamp when the first packet was switched and time stamp when the last packet was switched

2 For the Cisco ASR 1000 series router, this value is always 0. This is because on the Cisco ASR 1000 series router, aggregation caches are managed not by extracting data from main cache flow records as they are aged out, but rather by examining each packet, independently of any main cache processing.

The figure below shows the data export format for the AS aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Figure 1 Data Export Format for AS Aggregation Scheme



The table below lists definitions for the data export record fields used in the AS aggregation scheme.

Table 3 Data Export Record Field Definitions for AS Aggregation Scheme

Field	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Source AS	Autonomous system of the source IP address (peer or origin)
Destination AS	Autonomous system of the destination IP address (peer or origin)
Source interface	SNMP index of the input interface
Destination interface	SNMP index of the output interface

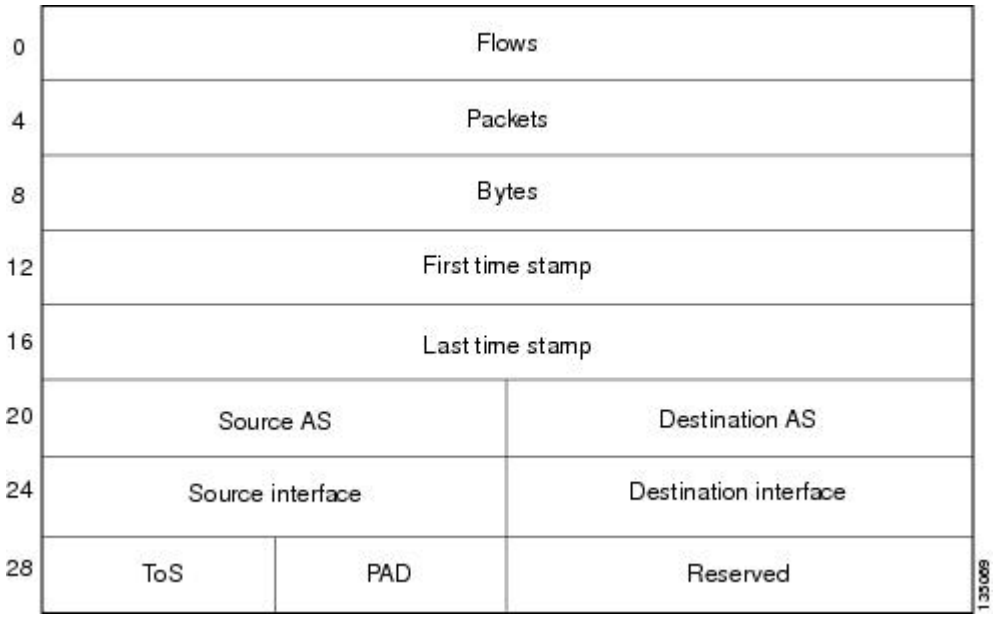
NetFlow AS-ToS Aggregation Scheme

The NetFlow AS-ToS aggregation scheme groups flows that have the same source BGP AS, destination BGP AS, source and destination interfaces, and ToS byte. The aggregated NetFlow export record based on the AS-ToS aggregation scheme reports the following:

- Source BGP AS
- Destination BGP AS
- ToS byte
- Number of flows summarized by the aggregated record
- Number of bytes summarized by this aggregated record
- Number of packets summarized by this aggregation record
- Source and destination interface
- Time stamp when the first packet was switched and time stamp when the last packet was switched

This aggregation scheme is particularly useful for generating AS-to-AS traffic flow data, and for reducing NetFlow export data volume substantially. The figure below shows the data export format for the AS-ToS aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Figure 2 Data Export Format for AS-ToS Aggregation Scheme



The table below lists definitions for the data export record terms used in the AS-ToS aggregation scheme.

Table 4 Data Export Record Term Definitions for AS-ToS Aggregation Scheme

Term	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched

Term	Definition
Source AS	Autonomous system of the source IP address (peer or origin)
Destination AS	Autonomous system of the destination IP address (peer or origin)
Source interface	SNMP index of the input interface
Destination interface	SNMP index of the output interface
ToS	Type of service byte
PAD	Zero field
Reserved	Zero field

NetFlow Destination Prefix Aggregation Scheme

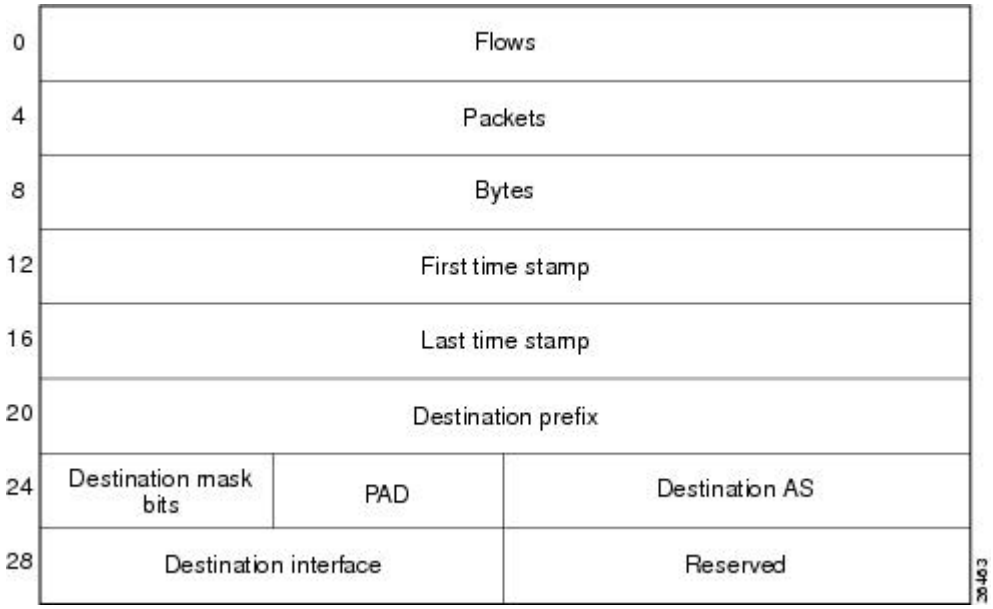
The destination prefix aggregation scheme generates data so that you can examine the destinations of network traffic passing through a NetFlow-enabled device. The scheme groups data flows that have the same destination prefix, destination prefix mask, destination BGP AS, and output interface.

The aggregated NetFlow data export records report the following:

- Destination prefix
- Destination prefix mask
- Destination BGP AS
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregated record
- Output interface
- Time stamp when the first packet was switched and time stamp when the last packet was switched

The figure below shows the data export format for the destination prefix aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Figure 3 Destination Prefix Aggregation Data Export Record Format



The table below lists definitions for the data export record terms used in the destination prefix aggregation scheme.

Table 5 Data Export Record Term Definitions for Destination Prefix Aggregation Scheme

Term	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Destination prefix	Destination IP address ANDed with the destination prefix mask
Destination mask bits	Number of bits in the destination prefix
PAD	Zero field
Destination AS	Autonomous system of the destination IP address (peer or origin)
Destination interface	SNMP index of the output interface

Term	Definition
Reserved	Zero field

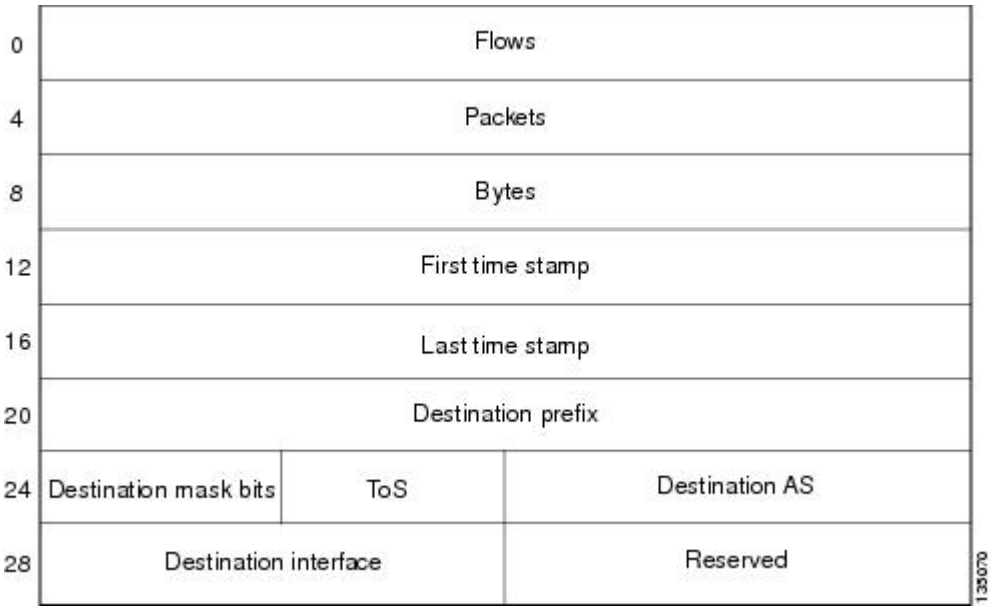
NetFlow Destination Prefix-ToS Aggregation Scheme

The NetFlow destination prefix-ToS aggregation scheme groups flows that have the same destination prefix, destination prefix mask, destination BGP AS, ToS byte, and output interface. The aggregated NetFlow export record reports the following:

- Destination IP address
- Destination prefix mask
- Destination AS
- ToS byte
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregated record
- Output interface
- Time stamp when the first packet was switched and time stamp when the last packet was switched

This aggregation scheme is particularly useful for capturing data with which you can examine the destinations of network traffic passing through a NetFlow-enabled device. The figure below shows the data export format for the Destination prefix-ToS aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Figure 4 Data Export Format for Destination Prefix-ToS Aggregation Scheme



The table below lists definitions for the data export record terms used in the destination prefix-ToS aggregation scheme.

Table 6 Data Export Record Term Definitions for Destination Prefix-ToS Aggregation Scheme

Term	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Destination prefix	Destination IP address ANDed with the destination prefix mask
Dest mask bits	Number of bits in the destination prefix
ToS	Type of service byte
Destination AS	Autonomous system of the destination IP address (peer or origin)
Destination interface	SNMP index of the output interface
Reserved	Zero field

NetFlow Prefix Aggregation Scheme

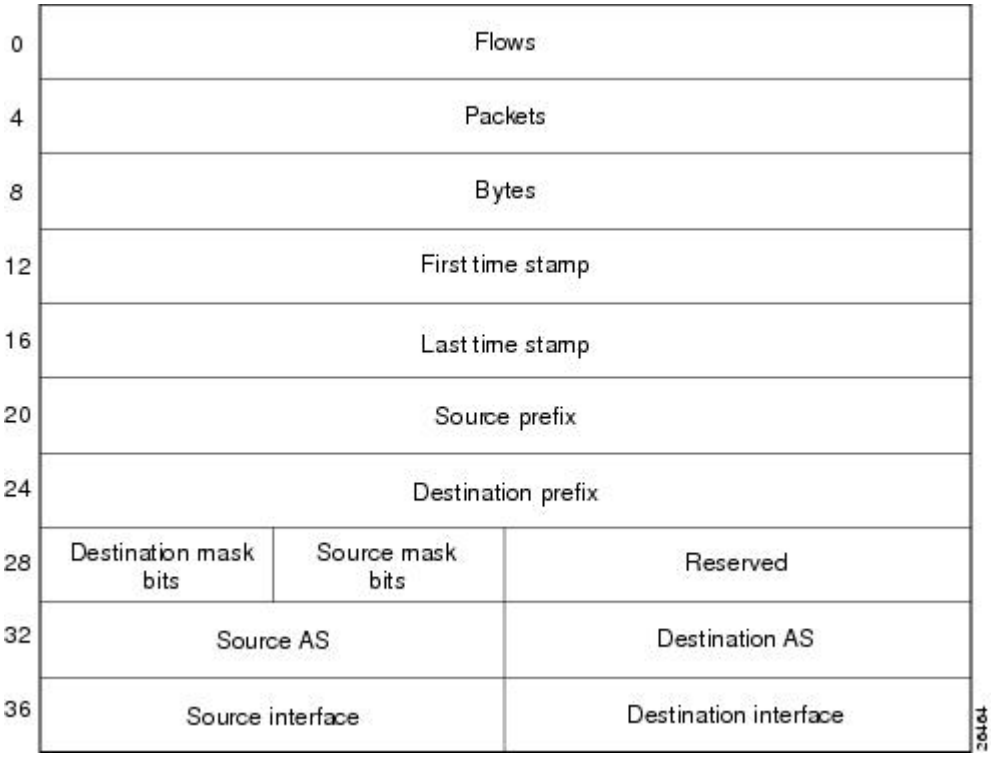
The NetFlow prefix aggregation scheme generates data so that you can examine the sources and destinations of network traffic passing through a NetFlow-enabled device. The scheme groups data flows that have the same source prefix, destination prefix, source prefix mask, destination prefix mask, source BGP AS, destination BGP AS, input interface, and output interface. See the figure below.

The aggregated NetFlow data export records report the following:

- Source and destination prefix
- Source and destination prefix mask
- Source and destination BGP AS
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregated record
- Input and output interfaces
- Time stamp when the first packet is switched and time stamp when the last packet is switched

The figure below shows the data export format for the prefix aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Figure 5 Data Export Format for Prefix Aggregation Scheme



The table below lists definitions for the data export record terms used in the prefix aggregation scheme.

Table 7 Data Export Record Terms and Definitions for Prefix Aggregation Scheme

Term	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Source prefix	Source IP address ANDed with the source prefix mask, or the prefix to which the source IP address of the aggregated flows belongs
Destination prefix	Destination IP address ANDed with the destination prefix mask

Term	Definition
Destination mask bits	Number of bits in the destination prefix
Source mask bits	Number of bits in the source prefix
Reserved	Zero field
Source AS	Autonomous system of the source IP address (peer or origin)
Destination AS	Autonomous system of the destination IP address (peer or origin)
Source interface	SNMP index of the input interface
Destination interface	SNMP index of the output interface

NetFlow Prefix-Port Aggregation Scheme

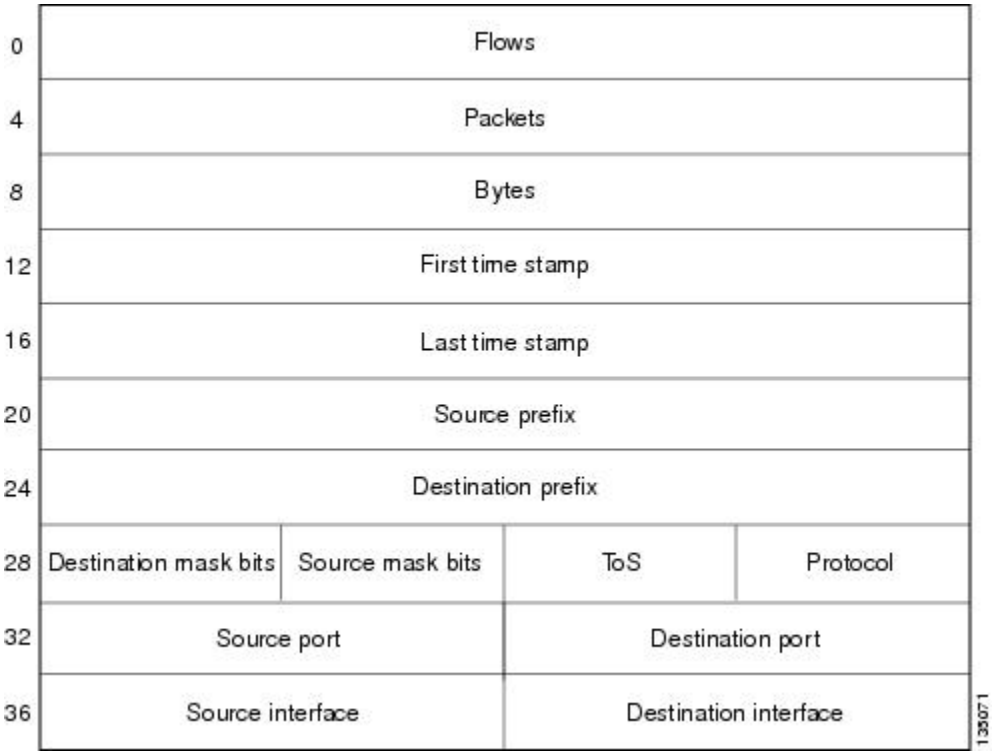
The NetFlow prefix-port aggregation scheme groups flows that have a common source prefix, source mask, destination prefix, destination mask, source port and destination port when applicable, input interface, output interface, protocol, and ToS byte. The aggregated NetFlow export record reports the following:

- Source prefix
- Source prefix mask
- Destination prefix
- Destination prefix mask
- Source port
- Destination port
- Source interface
- Destination interface
- Protocol
- ToS byte
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregation record
- Time stamp when the first packet was switched and time stamp when the last packet was switched

This aggregation scheme is particularly useful for capturing data with which you can examine the sources and destinations of network traffic passing through a NetFlow-enabled device. The figure below shows the

data export record for the prefix-port aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Figure 6 Data Export Record for Prefix-Port Aggregation Scheme



The table below lists definitions for the data export record terms used in the prefix-port aggregation scheme.

Table 8 Data Export Record Term Definitions for Prefix-Port Aggregation Scheme

Term	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Source prefix	Source IP address ANDed with the source prefix mask, or the prefix to which the source IP address of the aggregated flows belongs
Destination prefix	Destination IP address ANDed with the destination prefix mask

Term	Definition
Destination mask bits	Number of bits in the destination prefix
Source mask bits	Number of bits in the source prefix
ToS	Type of service byte
Protocol	IP protocol byte
Source port	Source UDP or TCP port number if applicable
Destination port	Destination User Datagram Protocol (UDP) or TCP port number
Source interface	SNMP index of the input interface
Destination interface	SNMP index of the output interface

NetFlow Prefix-ToS Aggregation Scheme

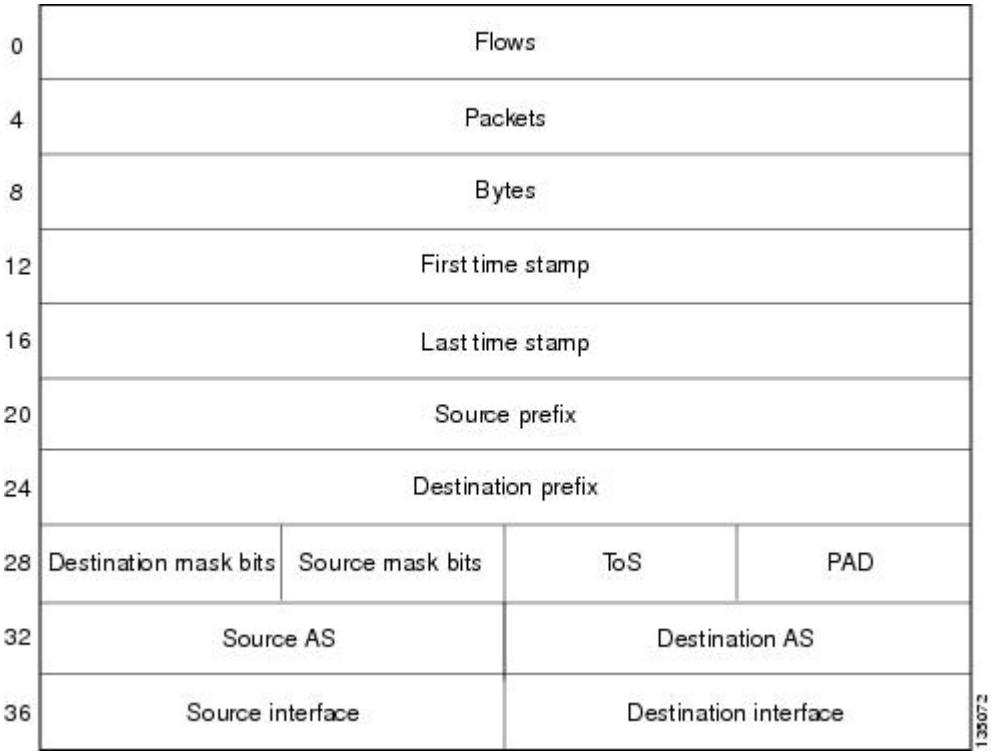
The NetFlow prefix-tos aggregation scheme groups together flows that have a common source prefix, source mask, destination prefix, destination mask, source BGP AS, destination BGP AS, input interface, output interface, and ToS byte. The aggregated NetFlow export record reports the following:

- Source prefix
- Source prefix mask
- Destination prefix
- Destination prefix mask
- Source AS
- Destination AS
- Source interface
- Destination interface
- ToS byte
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregated record
- Time stamp when the first packet was switched and time stamp when the last packet was switched

This aggregation scheme is particularly useful for capturing data so that you can examine the sources and destinations of network traffic passing through a NetFlow-enabled device. The figure below displays the

data export format for the prefix-tos aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Figure 7 Data Export Format for Prefix-ToS Aggregation Scheme



The table below lists definitions for the data export record terms used in the prefix-ToS aggregation scheme.

Table 9 Data Export Record Term Definitions for Prefix-ToS Aggregation Scheme

Term	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Source prefix	Source IP address ANDed with the source prefix mask, or the prefix to which the source IP address of the aggregated flows belongs
Destination prefix	Destination IP address ANDed with the destination prefix mask

Term	Definition
Destination mask bits	Number of bits in the destination prefix
Source mask bits	Number of bits in the source prefix
ToS	Type of service byte
Pad	Zero field
Source AS	Autonomous system of the source IP address (peer or origin)
Destination AS	Autonomous system of the destination IP address (peer or origin)
Source interface	SNMP index of the input interface
Destination interface	SNMP index of the output interface

NetFlow Protocol Port Aggregation Scheme

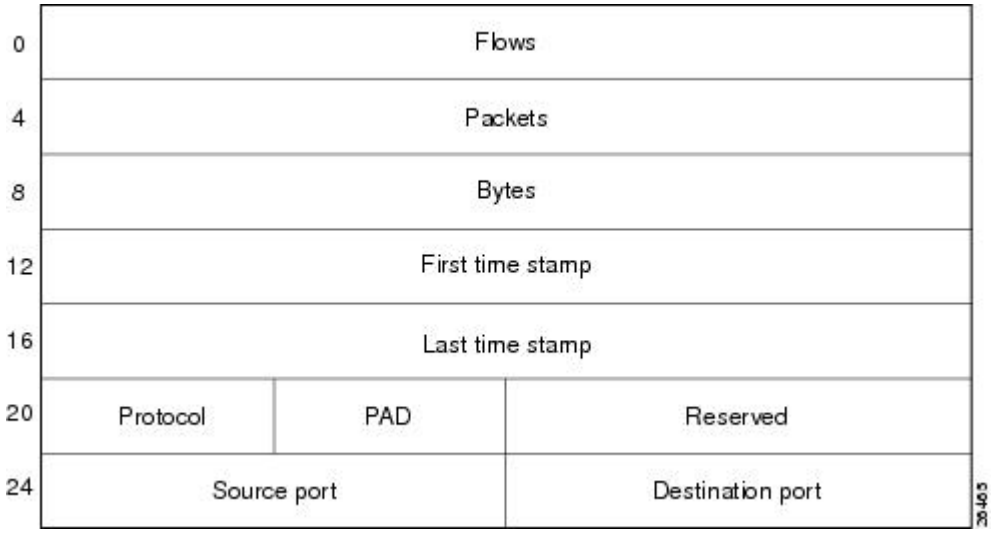
The NetFlow protocol port aggregation scheme captures data so that you can examine network usage by traffic type. The scheme groups data flows with the same IP protocol, source port number, and (when applicable) destination port number.

The aggregated NetFlow data export records report the following:

- Source and destination port numbers
- IP protocol (where 6 = TCP, 17 = UDP, and so on)
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregated record
- Time stamp when the first packet was switched and time stamp when the last packet was switched

The figure below shows the data export format for the protocol port aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Figure 8 Data Export Format for Protocol Port Aggregation Scheme



The table below lists definitions for the data export record terms used in the protocol port aggregation scheme.

Table 10 Data Export Record Term Definitions for Protocol Port Aggregation Scheme

Term	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Protocol	IP protocol byte
PAD	Zero field
Reserved	Zero field
Source port	Source UDP or TCP port number if applicable
Destination port	Destination User Datagram Protocol (UDP) or TCP port number

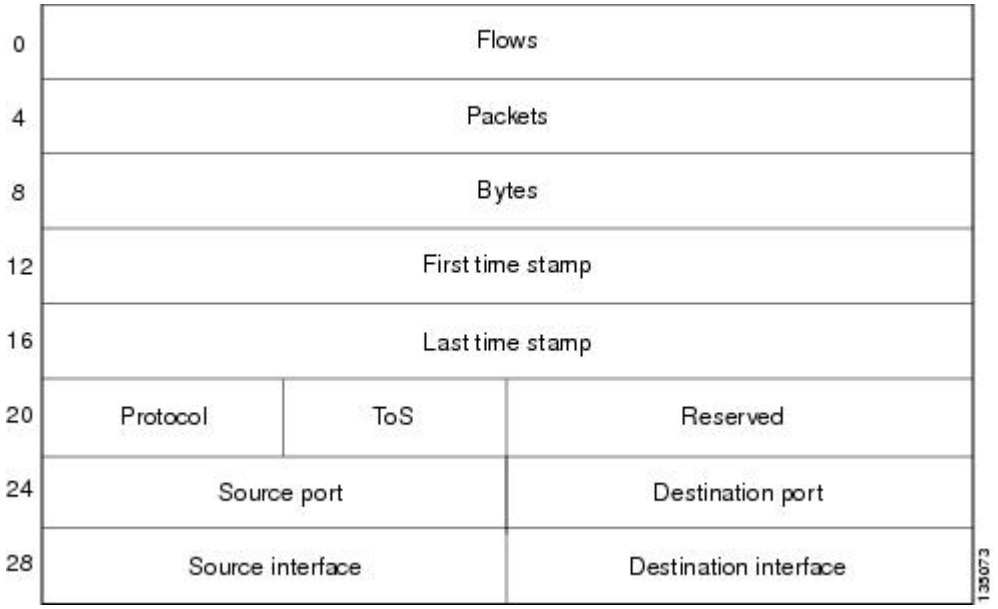
NetFlow Protocol-Port-ToS Aggregation Scheme

The NetFlow protocol-port-tos aggregation scheme groups flows that have a common IP protocol, ToS byte, source and (when applicable) destination port numbers, and source and destination interfaces. The aggregated NetFlow Export record reports the following:

- Source application port number
- Destination port number
- Source and destination interface
- IP protocol
- ToS byte
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregation record
- Time stamp when the first packet was switched and time stamp when the last packet was switched

This aggregation scheme is particularly useful for capturing data so that you can examine network usage by type of traffic. The figure below shows the data export format for the protocol-port-tos aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Figure 9 Data Export Format for Protocol-Port-ToS Aggregation Scheme



The table below lists definitions for the data export record terms used in the protocol-port-ToS aggregation scheme.

Table 11 Data Export Record Term Definitions for Protocol-Port-ToS Aggregation Scheme

Term	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Protocol	IP protocol byte
ToS	Type of service byte
Reserved	Zero field
Source port	Source UDP or TCP port number if applicable
Destination port	Destination User Datagram Protocol (UDP) or TCP port number

Term	Definition
Source interface	SNMP index of the input interface
Destination interface	SNMP index of the output interface

NetFlow Source Prefix Aggregation Scheme

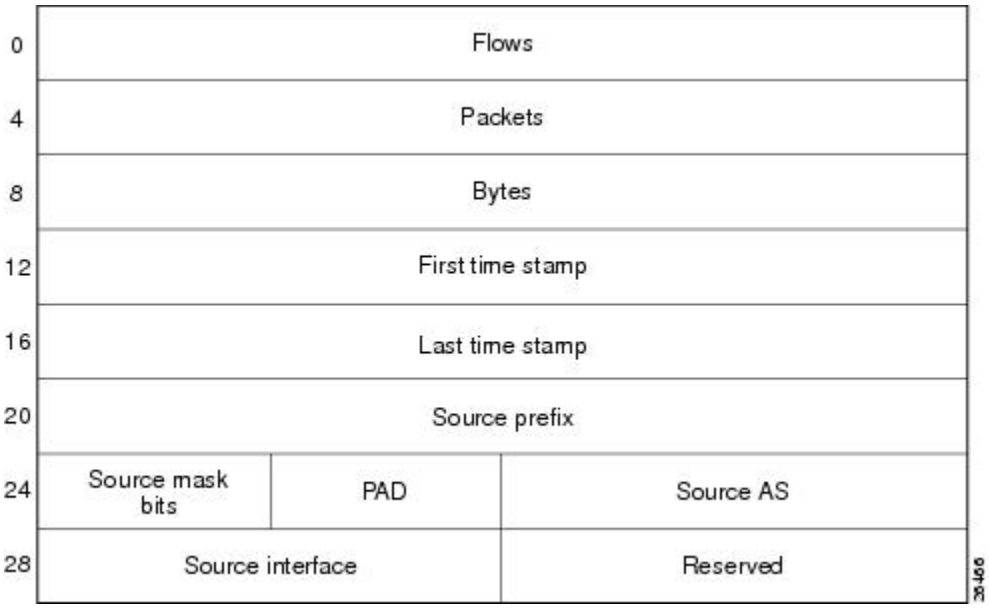
The NetFlow source prefix aggregation scheme captures data so that you can examine the sources of network traffic passing through a NetFlow-enabled device. The scheme groups data flows that have the same source prefix, source prefix mask, source BGP AS, and input interface.

The aggregated NetFlow data export records report the following:

- Source prefix
- Source prefix mask
- Source BGP AS
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregated record
- Input interface
- Time stamp when the first packet was switched and time stamp when the last packet was switched

The figure below shows the data export format for the source prefix aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Figure 10 Data Export Format for Source Prefix Aggregation Scheme



The table below lists definitions for the data export record terms used in the source prefix aggregation scheme.

Table 12 Data Export Record Term Definitions for Source Prefix Aggregation Scheme

Term	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Source prefix	Source IP address ANDed with the source prefix mask, or the prefix to which the source IP address of the aggregated flows belongs
Source mask bits	Number of bits in the source prefix
PAD	Zero field
Source AS	Autonomous system of the source IP address (peer or origin)
Source interface	SNMP index of the input interface
Reserved	Zero field

NetFlow Source Prefix-ToS Aggregation Scheme

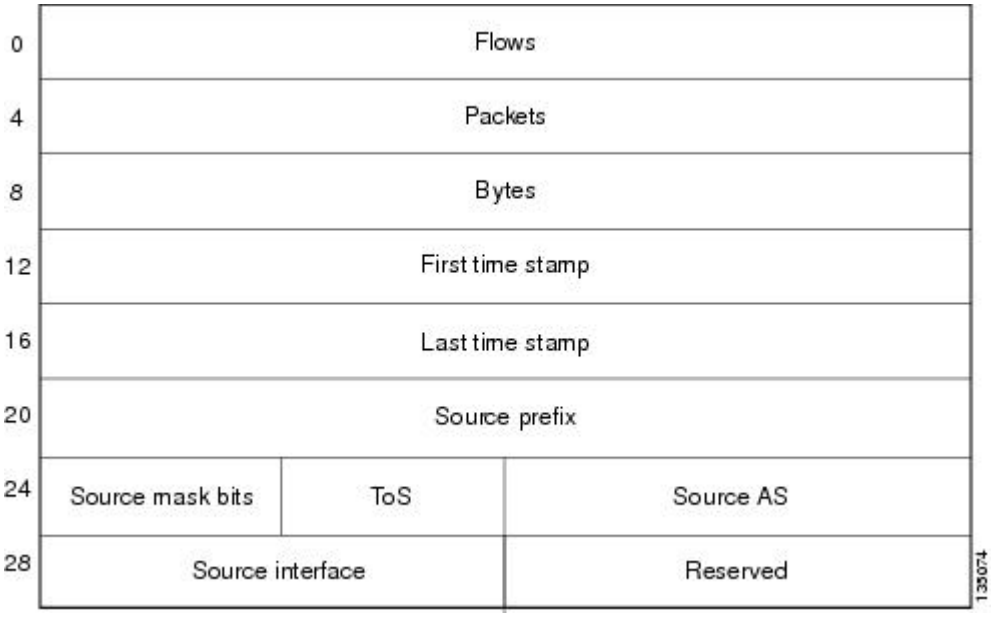
The NetFlow source prefix-ToS aggregation scheme groups flows that have a common source prefix, source prefix mask, source BGP AS, ToS byte, and input interface. The aggregated NetFlow export record reports the following:

- Source prefix
- Source prefix mask
- Source AS
- ToS byte
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregation record
- Input interface
- Time stamp when the first packet was switched and time stamp when the last packet was switched

This aggregation scheme is particularly useful for capturing data so that you can examine the sources of network traffic passing through a NetFlow-enabled device. The figure below shows the data export format for the source prefix-ToS aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Note When a router does not have a prefix for the source IP address in the flow, NetFlow uses 0.0.0.0 with 0 mask bits rather than making /32 entries. This prevents DOS attacks that use random source addresses from thrashing the aggregation caches. This is also done for the destination in the destination prefix-ToS, the prefix-ToS, and prefix-port aggregation schemes.

Figure 11 Data Export Format for Source Prefix-ToS Aggregation Scheme



The table below lists definitions for the data export record terms used in the source prefix-ToS aggregation scheme.

Table 13 Data Export Record Term Definitions for Source Prefix-ToS Aggregation Scheme

Term	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Source prefix	Source IP address ANDed with the source prefix mask, or the prefix to which the source IP address of the aggregated flows belongs
Source mask bits	Number of bits in the source prefix

Term	Definition
ToS	Type of service byte
Source AS	Autonomous system of the source IP address (peer or origin)
Source interface	SNMP index of the input interface
Reserved	Zero field

NetFlow Data Export Format Versions 9 and 8 for NetFlow Aggregation Caches Overview

Export formats available for NetFlow aggregation caches are the Version 9 export format and the Version 8 export format.

- Version 9--A flexible and extensible format, which provides the versatility needed for support of new fields and record types. Version 9 export format enables you to use the same version for main and aggregation caches, and the format is extendable, so you can use the same export format with future features.
- Version 8--A format added to support data export from aggregation caches. Export datagrams contain a subset of the usual Version 5 export data, which is valid for the particular aggregation cache scheme. Version 8 is the default export version for aggregation caches when data export is configured.

The Version 9 export format is flexible and extensible, which provides the versatility needed for the support of new fields and record types. You can use the Version 9 export format for both main and aggregation caches.

The Version 8 export format was added to support data export from aggregation caches. This format allows export datagrams to contain a subset of the Version 5 export data that is valid for the cache aggregation scheme.

See the "NetFlow Data Export" section of the "Configuring NetFlow Aggregation Caches" module for more details on NetFlow Data Export Formats.

How to Configure NetFlow Aggregation Caches

Configuring NetFlow Aggregation Caches

Perform this task to enable NetFlow and configure a NetFlow aggregation cache.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-aggregation cache** {**as** | **as-tos** | **destination-prefix** | **destination-prefix-tos** | **prefix** | **prefix-port** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos**}
4. **cache entries** *number*
5. **cache timeout active** *minutes*
6. **cache timeout inactive** *seconds*
7. **export destination** {{*ip-address* | *hostname*} *udp-port*}
8. Repeat Step 7 to configure a second export destination.
9. **export version** [**9** | **8**]
10. **enabled**
11. **exit**
12. **interface** *interface-type interface-number*
13. **ip flow** {**ingress** | **egress**}
14. **exit**
15. Repeat Steps 12 through 14 to enable NetFlow on other interfaces
16. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip flow-aggregation cache** {**as** | **as-tos** | **destination-prefix** | **destination-prefix-tos** | **prefix** | **prefix-port** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos**} **Example:** **Example:** `Router(config)# ip flow-aggregation cache destination-prefix`	(Required) Specifies the aggregation cache scheme and enables aggregation cache configuration mode. • The **as** keyword configures the AS aggregation cache. • The **as-tos**keyword configures the AS ToS aggregation cache. • The **destination-prefix** keyword configures the destination prefix aggregation cache. • The **destination-prefix-tos** keyword configures the destination prefix ToS aggregation cache. • The **prefix** keyword configures the prefix aggregation cache. • The **prefix-port** keyword configures the prefix port aggregation cache. • The **prefix-tos** keyword configures the prefix ToS aggregation cache. • The **protocol-port** keyword configures the protocol port aggregation cache. • The **protocol-port-tos** keyword configures the protocol port ToS aggregation cache. • The **source-prefix** keyword configures the source prefix aggregation cache. • The **source-prefix-tos** keyword configures the source prefix ToS aggregation cache.
Step 4	**cache entries** *number* **Example:** `Router(config-flow-cache)# cache entries 2048`	(Optional) Configures aggregation cache operational parameters. • The **entries** *number* keyword-argument pair is the number of cached entries allowed in the aggregation cache. The range is from 1024 to 2000000. The default is 4096.
Step 5	**cache timeout active** *minutes* **Example:** `Router(config-flow-cache)# cache timeout active 15`	(Optional) Configures aggregation cache operational parameters. • The **timeout** keyword dissolves the session in the aggregation cache. • The **active** *minutes* keyword-argument pair specifies the number of minutes that an entry is active. The range is from 1 to 60 minutes. The default is 30 minutes.
Step 6	**cache timeout inactive** *seconds* **Example:** `Router(config-flow-cache)# cache timeout inactive 300`	(Optional) Configures aggregation cache operational parameters. • The **timeout** keyword dissolves the session in the aggregation cache. • The **inactive** *seconds*keyword-argument pair specifies the number of seconds that an inactive entry stays in the aggregation cache before the entry times out. The range is from 10 to 600 seconds. The default is 15 seconds.

	Command or Action	Purpose
Step 7	**export destination** {{*ip-address* | *hostname*} *udp-port*} **Example:** `Router(config-flow-cache)# export destination 172.30.0.1 991`	(Optional) Enables the exporting of information from NetFlow aggregation caches. • The *ip-address* | *hostname*argument is the destination IP address or hostname. • The *port* argument is the destination UDP port.
Step 8	Repeat Step 7 to configure a second export destination.	(Optional) You can configure a maximum of two export destinations for each NetFlow aggregation cache.
Step 9	**export version** [**9** | **8**] **Example:** `Router(config-flow-cache)# export version 9`	(Optional) Specifies data export format Version. • The **version 9** keyword specifies that the export packet uses the Version 9 format.
Step 10	**enabled** **Example:** `Router(config-flow-cache)# enabled`	(Required) Enables the aggregation cache.
Step 11	**exit** **Example:** `Router(config-if)# exit`	(Required) Exits NetFlow aggregation cache configuration mode and returns to global configuration mode.
Step 12	**interface** *interface-type interface-number* **Example:** `Router(config)# interface fastethernet 0/0/0`	(Required) Specifies the interface that you want to enable NetFlow on and enters interface configuration mode.
Step 13	**ip flow** {**ingress** | **egress**} **Example:** `Router(config-if)# ip flow ingress`	(Required) Enables NetFlow on the interface. • **ingress** --captures traffic that is being received by the interface • **egress** --captures traffic that is being transmitted by the interface.

	Command or Action	Purpose
Step 14	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode and returns to global configuration mode. **Note** You only need to use this command if you want to enable NetFlow on another interface.
Step 15	Repeat Steps 12 through 14 to enable NetFlow on other interfaces	(Optional) --
Step 16	**end** **Example:** `Router(config-if)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Verifying the Aggregation Cache Configuration

To verify the aggregation cache configuration, use the following show commands. These commands allow you to:

- Verify that the NetFlow aggregation cache is operational.
- Verify that NetFlow Data Export for the aggregation cache is operational.
- View the aggregation cache statistics.

SUMMARY STEPS

1. **enable**
2. **show ip cache flow aggregation** {**as** | **as-tos** | **destination-prefix** | **destination-prefix-tos** | **prefix** | **prefix-port** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos**}
3. **show ip flow export**
4. **end**

DETAILED STEPS

Step 1 **enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
```

Router#

Step 2 **show ip cache flow aggregation** {**as** | **as-tos** | **destination-prefix** | **destination-prefix-tos** | **prefix** | **prefix-port** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos**}

Use the **show ip cache flow aggregation destination-prefix** command to verify the configuration of an destination-prefix aggregation cache. For example:

Example:

```
Router# show ip cache flow aggregation destination-prefix
IP Flow Switching Cache, 139272 bytes
  5 active, 2043 inactive, 9 added
  841 ager polls, 0 flow alloc failures
  Active flows timeout in 15 minutes
  Inactive flows timeout in 300 seconds
IP Sub Flow Cache, 11144 bytes
  5 active, 507 inactive, 9 added, 9 added to flow
  0 alloc failures, 0 force free
  1 chunk, 2 chunks added
Dst If         Dst Prefix      Msk  AS    Flows  Pkts B/Pk  Active
Null           0.0.0.0         /0   0        5    13    52   138.9
Et0/0.1        172.16.6.0      /24  0        1     1    56     0.0
Et1/0.1        172.16.7.0      /24  0        3    31K 1314   187.3
Et0/0.1        172.16.1.0      /24  0       16   104K 1398   188.4
Et1/0.1        172.16.10.0     /24  0        9    99K 1412   183.3
Router#
```

Use the **show ip cache verbose flow aggregation source-prefix** command to verify the configuration of a source-prefix aggregation cache. For example:

Example:

```
Router# show ip cache verbose flow aggregation source-prefix
IP Flow Switching Cache, 278544 bytes
  4 active, 4092 inactive, 4 added
  51 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  4 active, 1020 inactive, 4 added, 4 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
Src If         Src Prefix      Msk  AS    Flows  Pkts B/Pk  Active
FEt1/0/0.1      172.16.10.0     /24  0        4    35K 1391    67.9
FEt0/0/0.1      172.16.6.0      /24  0        2     5    88    60.6
FEt1/0/0.1      172.16.7.0      /24  0        2  3515  1423    58.6
FEt0/0/0.1      172.16.1.0      /24  0        2    20K 1416    71.9
Router#
```

Use the **show ip cache verbose flow aggregation protocol-port** command to verify the configuration of a protocol-port aggregation cache. For example:

Example:

```
Router# show ip cache verbose flow aggregation protocol-port
IP Flow Switching Cache, 278544 bytes
  4 active, 4092 inactive, 4 added
  158 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
Protocol  Source Port  Dest Port  Flows  Packets  Bytes/Packet  Active
  0x01       0x0000      0x0000      6       52K     1405        104.3
  0x11       0x0208      0x0208      1        3        52         56.9
  0x01       0x0000      0x0800      2      846      1500         59.8
  0x01       0x0000      0x0B01      2       10        56         63.0
Router#
```

Step 3 **show ip flow export**

Use the **show ip flow export** command to verify that NetFlow Data Export is operational for the aggregation cache. For example:

Example:

```
Router# show ip flow export
Flow export v1 is disabled for main cache
  Version 9 flow records
  Cache for protocol-port aggregation:
    Exporting flows to 172.16.20.4 (991) 172.30.0.1 (991)
    Exporting using source IP address 172.16.6.2
  Cache for source-prefix aggregation:
    Exporting flows to 172.16.20.4 (991) 172.30.0.1 (991)
    Exporting using source IP address 172.16.6.2
  Cache for destination-prefix aggregation:
    Exporting flows to 172.16.20.4 (991) 172.30.0.1 (991)
    Exporting using source IP address 172.16.6.2
  40 flows exported in 20 udp datagrams
  0 flows failed due to lack of export packet
  20 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
Router#
```

Step 4 **end**

Use this command to exit privileged EXEC mode.

Example:

```
Router# end
```

Configuration Examples for Configuring NetFlow Aggregation Caches

Configuring an AS Aggregation Cache Example

The following example shows how to configure an AS aggregation cache with a cache size of 2046, an inactive timeout of 200 seconds, a cache active timeout of 45 minutes, an export destination IP address of 10.42.42.1, and a destination port of 9992:

```
configure terminal
!
ip flow-aggregation cache as
 cache entries 2046
 cache timeout inactive 200
 cache timeout active 45
 export destination 10.42.42.1 9992
 enabled
!
interface Fastethernet0/0/0
 ip flow ingress
!
 end
```

Configuring a Destination Prefix Aggregation Cache Example

The following example shows how to configure a destination prefix aggregation cache with a cache size of 2046, an inactive timeout of 200 seconds, a cache active timeout of 45 minutes, an export destination IP address of 10.42.42.1, and a destination port of 9992:

```
configure terminal

!

ip flow-aggregation cache destination-prefix
 cache entries 2046
 cache timeout inactive 200
 cache timeout active 45
 export destination 10.42.42.1 9992
 enabled
!
interface Fastethernet0/0/0
 ip flow ingress
!
 end
```

Configuring a Prefix Aggregation Cache Example

The following example shows how to configure a prefix aggregation cache with a cache size of 2046, an inactive timeout of 200 seconds, a cache active timeout of 45 minutes, an export destination IP address of 10.42.42.1, and a destination port of 9992:

```
configure terminal

!

ip flow-aggregation cache prefix
 cache entries 2046
 cache timeout inactive 200
 cache timeout active 45
 export destination 10.42.42.1 9992
 enabled
!
interface Fastethernet0/0/0
 ip flow ingress
```

```
!
 end
```

Configuring a Protocol Port Aggregation Cache Example

The following example shows how to configure a protocol port aggregation cache with a cache size of 2046, an inactive timeout of 200 seconds, a cache active timeout of 45 minutes, an export destination IP address of 10.42.42.1, and a destination port of 9992:

```
configure terminal

!

ip flow-aggregation cache protocol-port
 cache entries 2046
 cache timeout inactive 200
 cache timeout active 45
 export destination 10.42.42.1 9992
 enabled
!
interface Fastethernet0/0/0
 ip flow ingress
!
 end
```

Configuring a Source Prefix Aggregation Cache Example

The following example shows how to configure a source prefix aggregation cache with a cache size of 2046, an inactive timeout of 200 seconds, a cache active timeout of 45 minutes, an export destination IP address of 10.42.42.1, and a destination port of 9992:

```
configure terminal

!

ip flow-aggregation cache source-prefix
 cache entries 2046
 cache timeout inactive 200
 cache timeout active 45
 export destination 10.42.42.1 9992
 enabled
!
interface Fastethernet0/0/0
 ip flow ingress
!
 end
```

Configuring an AS-ToS Aggregation Cache Example

The following example shows how to configure an AS-ToS aggregation cache with a cache active timeout of 20 minutes, an export destination IP address of 10.2.2.2, and a destination port of 9991:

```
configure terminal

!

ip flow-aggregation cache as-tos
 cache timeout active 20
 export destination 10.2.2.2 9991
 enabled
```

```
!
interface Fastethernet0/0/0
 ip flow ingress
!
 end
```

Configuring a Prefix-ToS Aggregation Cache Example

The following example shows how to configure a prefix-ToS aggregation cache with an export destination IP address of 10.4.4.4 and a destination port of 9995:

```
configure terminal

!

ip flow-aggregation cache prefix-tos
 export destination 10.4.4.4 9995
 enabled
!
interface Fastethernet0/0/0
 ip flow ingress
!
 end
```

Configuring the Minimum Mask of a Prefix Aggregation Scheme Example

The following example shows how to configure the minimum mask for a prefix aggregation scheme:

```
configure terminal

!

ip flow-aggregation cache prefix
 mask source minimum 24
 mask destination minimum 28
 enabled
!
interface Fastethernet0/0/0
 ip flow ingress
!
 end
```

Configuring the Minimum Mask of a Destination Prefix Aggregation Scheme Example

The following example shows how to configure the minimum mask for a destination prefix aggregation scheme:

```
configure terminal

!

ip flow-aggregation cache destination-prefix
 mask destination minimum 32
 enabled
!
interface Fastethernet0/0/0
 ip flow ingress
!
 end
```

Configuring the Minimum Mask of a Source Prefix Aggregation Scheme Example

The following example shows how to configure the minimum mask for a source prefix aggregation scheme:

```
configure terminal

!

ip flow-aggregation cache source-prefix
 mask source minimum 30
 enabled
!
interface Fastethernet0/0/0
 ip flow ingress
!
 end
```

Configuring NetFlow Version 9 Data Export for Aggregation Caches Example

The following example shows how to configure NetFlow Version 9 data export for an AS aggregation cache scheme:

```
configure terminal
!
ip flow-aggregation cache as
 export destination 10.42.42.2 9991
 export template refresh-rate 10
 export version 9
 export template timeout-rate 60
 enabled
!
interface Ethernet0/0
 ip flow ingress
!
 end
```

Configuring NetFlow Version 8 Data Export for Aggregation Caches Example

The following example shows how to configure NetFlow Version 8 data export for an AS aggregation cache scheme:

```
configure terminal
!
ip flow-aggregation cache as
 export destination 10.42.42.2 9991
 export destination 10.42.41.1 9991
 export version 8
 enabled
!
interface Fastethernet0/0/0
 ip flow ingress
!
 end
```

Additional References

Related Documents

Related Topic	Document Title
NetFlow commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS NetFlow Command Reference*
Tasks for configuring NetFlow to capture and export network traffic data	"Configuring NetFlow and NetFlow Data Export"
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"
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 XE releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

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

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring NetFlow Aggregation Caches

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 14 Feature Information for Configuring NetFlow Aggregation Caches

Feature Name	Releases	Feature Configuration Information
NetFlow ToS-Based Router Aggregation	Cisco IOS XE Release 2.1	The NetFlow ToS-Based Router Aggregation feature enables you to limit router-based type of service (ToS) aggregation of NetFlow export data. The aggregation of export data provides a summarized NetFlow export data that can be exported to a collection device. The result is lower bandwidth requirements for NetFlow export data and reduced platform requirements for NetFlow data collection devices. In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. The following commands were modified by this feature: **ip flow-aggregation cache**, **show ip cache verbose flow aggregation**, **show ip flow export**.
NetFlow Minimum Prefix Mask for Router-Based Aggregation	Cisco IOS XE Release 2.1	The NetFlow Minimum Prefix Mask for Router-Based Aggregation feature allows you to set a minimum mask size for prefix aggregation, destination prefix aggregation, and source prefix aggregation schemes. In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers. The following commands were modified by this feature: **ip flow-aggregation cache**, **mask destination**, **mask source**, **show ip cache flow aggregation**.

Glossary

AS --autonomous system. A collection of networks under a common administration sharing a common routing strategy. Autonomous systems are subdivided by areas. An autonomous system must be assigned a unique 16-bit number by the Internet Assigned Numbers Authority (IANA).

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

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

flow --A set of packets with the same source IP address, destination IP address, protocol, source/destination ports, and type-of-service, and the same interface on which flow is monitored. Ingress flows are associated with the input interface, and egress flows are associated with the output interface.

flowset --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 --Cisco IOS XE accounting feature that maintains per-flow information.

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)--Cisco application that is used with NetFlow on Cisco routers and Catalyst 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 for 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.

QoS --quality of service. A measure of performance for a transmission system that reflects its transmission quality and service availability.

template flowset --One or more template records that are grouped in an export packet.

ToS --type of service. The second byte in the IP header. It indicates the desired quality of service (QoS) for a particular datagram.

Configuring NetFlow and NetFlow Data Export

This module contains information about and instructions for configuring NetFlow to capture and export network traffic data. NetFlow capture and export are performed independently on each internetworking device on which NetFlow is enabled. NetFlow need not be operational on each router in the network. NetFlow is a Cisco IOS XE application that provides statistics on packets flowing through the router. NetFlow is emerging as a primary network accounting and security technology.

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 Configuring NetFlow and NetFlow Data Export

- Configure the router for IP routing.
- Ensure that either Cisco Express Forwarding or fast switching is enabled on your router and on the interfaces on which you want to configure NetFlow.
- Understand the resources required on your router because NetFlow consumes additional memory and CPU resources.

Restrictions for Configuring NetFlow and NetFlow Data Export

Preset Size of NetFlow Cache

NetFlow consumes additional memory. If you have memory constraints, you might want to preset the size of the NetFlow cache so that it contains a smaller number of entries. The default cache size depends on the platform.

Egress NetFlow Accounting in Cisco IOS XE Release 2.1 or Later Releases

The Egress NetFlow Accounting feature captures NetFlow statistics for IP traffic only. Multiprotocol Label Switching (MPLS) statistics are not captured. The Egress NetFlow Accounting feature can be used on a provider edge (PE) router to capture IP traffic flow information for egress IP packets that arrived at the router as MPLS packets and underwent label disposition.

Egress NetFlow accounting might adversely affect network performance because of the additional accounting-related computation that occurs in the traffic-forwarding path of the router.

Locally generated traffic (traffic that is generated by the router on which the Egress NetFlow Accounting feature is configured) is not counted as flow traffic for the Egress NetFlow Accounting feature.

Note Egress NetFlow captures IPv4 packets as they leave the router.

Restrictions for NetFlow Version 9 Data Export

- Backward compatibility--Version 9 is not backward-compatible with Version 5 or Version 8. If you need Version 5 or Version 8, you must configure it.
- Export bandwidth--Export bandwidth use increases for Version 9 (because of template flowsets) versus Version 5. The increase in bandwidth usage versus Version 5 varies with the frequency with which template flowsets are sent. The default is to resend templates every 20 packets, which has a bandwidth cost of about 4 percent. If necessary, you can lower the resend rate with the **ip flow-export template refresh-rate** *packets* command.
- Performance impact--Version 9 slightly decreases overall performance, because generating and maintaining valid template flowsets require additional processing.

Restrictions for NetFlow Version 8 Export Format

Version 8 export format is available only for aggregation caches, and it cannot be expanded to support new features.

Restrictions for NetFlow Version 5 Export Format

Version 5 export format is suitable only for the main cache, and it cannot be expanded to support new features.

Policy-Based Routing and NetFlow Data Export

If a local policy is configured, an Aggregation Services Router (ASR) checks the injected packet and applies policy-based routing (PBR) to the packet. When NetFlow Data Export (NDE) packets are injected

in the data path during Cisco Express Forwarding lookup, the PBR local policy is not applied to the NDE packets. Therefore, NDE features on ASR cannot work with PBR.

Information About Configuring NetFlow and NetFlow Data Export

NetFlow Data Capture

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

- IP-to-IP packets
- IP-to-MPLS packets
- Frame Relay-terminated packets
- ATM-terminated packets

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

- Egress NetFlow Accounting--NetFlow gathers statistics for all egress packets for IP traffic only.

NetFlow Flows Key Fields

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

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Layer 3 protocol type
- Type of service (ToS)
- 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 contain other accounting fields (such as the autonomous system (AS) number in the NetFlow export Version 5 flow format) that depend on the export record version that you configure. Flows are stored in the NetFlow cache.

NetFlow Cache Management and Data Export

The key components of NetFlow are the NetFlow cache or data source 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. A flow record is maintained within the NetFlow cache for each active flows. Each flow record in the NetFlow cache contains fields that can later be exported to a collection device, such as the NetFlow Collection Engine.

NetFlow is very efficient with the amount of export data being about 1.5 percent of the switched traffic in the router. NetFlow accounts for every packet (non-sampled mode) and provides a highly condensed and detailed view of all network traffic that entered the router or switch.

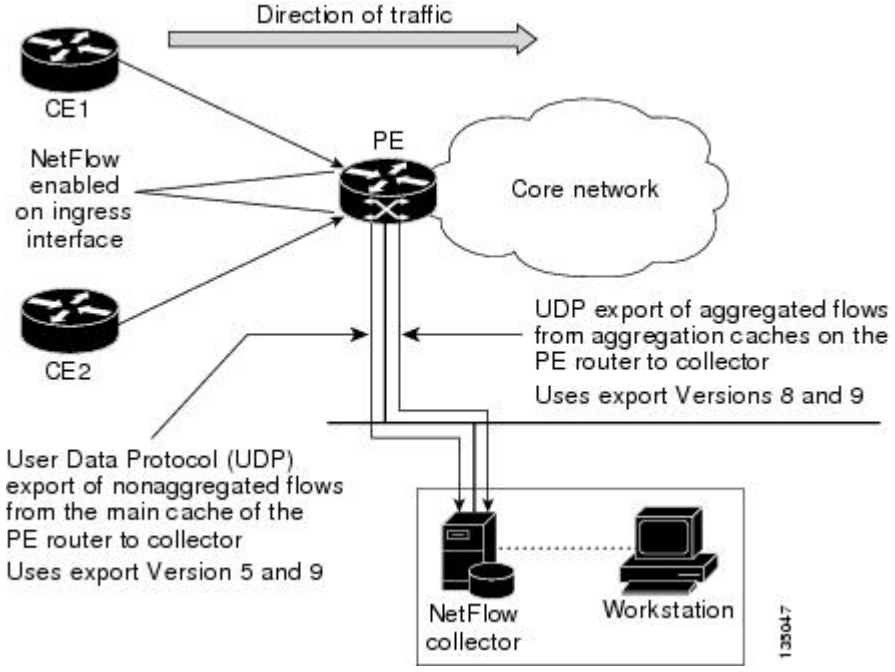
The key to NetFlow-enabled switching scalability and performance is highly intelligent flow cache management, especially for densely populated and busy edge routers handling large numbers of concurrent, short duration flows. The NetFlow cache management software contains a highly sophisticated set of algorithms for efficiently determining if a packet is part of an existing flow or should generate a new flow cache entry. The algorithms are also capable of dynamically updating the per-flow accounting measurements that reside in the NetFlow cache, and determining cache aging/flow expiration.

Rules for expiring NetFlow cache entries include:

- Flows which have been idle for a specified time are expired and removed from the cache.
- Long-lived flows are expired and removed from the cache. (Flows are not allowed to live more than 30 minutes by default; the underlying packet conversation remains undisturbed.)
- As the cache becomes full, a number of heuristics are applied to aggressively age groups of flows simultaneously.

Expired flows are grouped together into "NetFlow export" datagrams for export from the NetFlow- enabled device. The NetFlow functionality is configured on a per-interface basis. To configure NetFlow export capabilities, you need to specify the IP address and application port number of the Cisco NetFlow or third-party flow collector. The flow collector is a device that provides NetFlow export data filtering and aggregation capabilities. The figure below shows an example of NetFlow data export from the main and aggregation caches to a collector.

Figure 12 NetFlow Data Export from the Main and Aggregation Caches



NetFlow Export Format Versions 9 8 and 5

The following sections provide more detailed information on NetFlow Data Export Formats Versions 9, 8, and 5:

Overview of NetFlow Export Format Versions 9 8 and 5

NetFlow exports data in UDP datagrams in one of the following formats: Version 9, Version 8, Version 7, or Version 5.

- Version 9--A flexible and extensible format, which provides the versatility needed for support of new fields and record types. The version 9 export format enables you to use the same version for main and aggregation caches, and the format is extendable, so you can use the same export format with future features.
- Version 8--A format added to support data export from aggregation caches. Export datagrams contain a subset of the usual Version 5 export data, which is valid for the particular aggregation cache scheme.
- Version 5--A later enhanced version that adds Border Gateway Protocol (BGP) AS information and flow sequence numbers. (Versions 2 through 4 were not released.) This is the most commonly used format.

NetFlow Export Version Formats

For all export versions, the NetFlow export datagram consists of a header and a sequence of flow records. The header contains information such as the sequence number, record count, and system uptime. The flow record contains flow information, for example, IP addresses, ports, and routing information.

The NetFlow Version 9 export format is the newest NetFlow export format. The distinguishing feature of the NetFlow Version 9 export format is that it is template based. Templates make the record format extensible. This feature allows future enhancements to NetFlow without requiring concurrent changes to the basic flow-record format.

The use of templates with the NetFlow Version 9 export format provides several other key benefits:

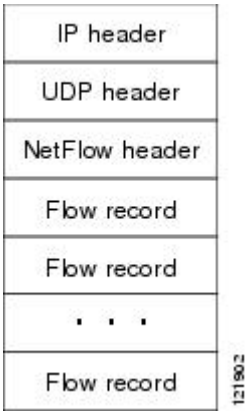
- You can export almost any information from a router or switch including Layer 2 through 7 information, routing information, IP Version 6 (IPv6), IP Version 4 (IPv4), and multicast information. This new information allows new applications for export data and new views of the network behavior.
- Third-party business partners who produce applications that provide collector or display services for NetFlow are not required to recompile their applications each time a new NetFlow export field is added. Instead, they might be able to use an external data file that documents the known template formats.
- New features can be added to NetFlow more quickly, without breaking current implementations.

The work of the IETF IP Information Export (IPFIX) Working Group (WG) and the IETF Pack Sampling (PSAMP) WG are based on the NetFlow Version 9 export format.

The Version 5 export format adds BGP autonomous system information and flow sequence numbers. the Version 8 export format is the NetFlow export format to use when you enable router-based NetFlow aggregation on Cisco IOS XE router platforms.

The figure below shows a typical datagram used for NetFlow fixed format export Versions 5, 7, and 8.

Figure 13 Typical Datagram for NetFlow Fixed Format Export Versions 5, 7, and 8

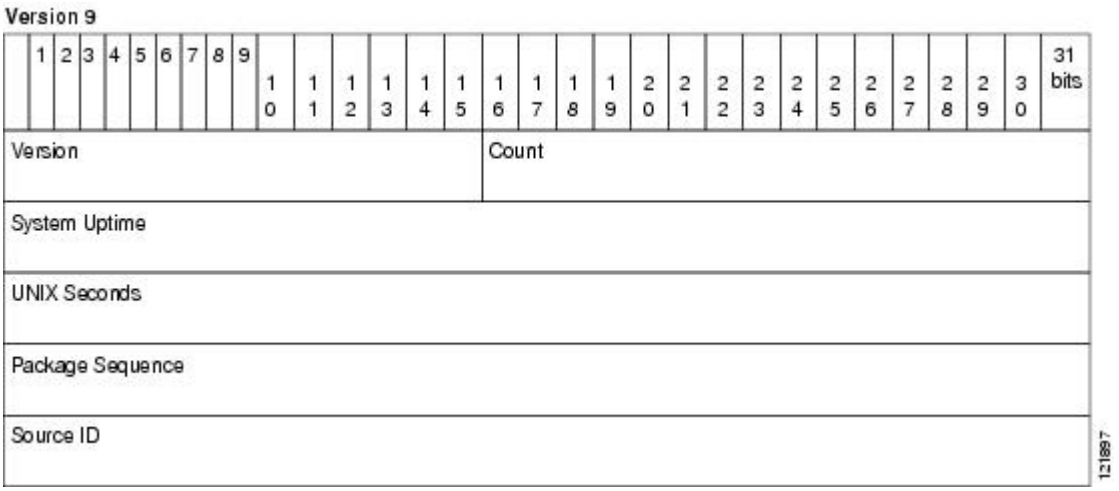


NetFlow Export Packet Header Format

In all five export versions, the datagram consists of a header and one or more flow records. The first field of the header contains the version number of the export datagram. Typically, a receiving application that accepts any of the format versions allocates a buffer large enough for the largest possible datagram from any of the format versions, and then uses the header to determine how to interpret the datagram. The second field in the header contains the number of records in the datagram (indicating the number of expired flows represented by this datagram). Datagram headers for NetFlow Export Versions 5, 8, and 9 also include a "sequence number" field used by NetFlow collectors to check for lost datagrams.

The NetFlow Version 9 export packet header format is shown in Figure 3 .

Figure 14 NetFlow Version 9 Export Packet Header Format



The table below lists the NetFlow Version 9 export packet header field names and descriptions.

Table 15 NetFlow Version 9 Export Packet Header Field Names and Descriptions

Field Name	Description
Version	The version of NetFlow records exported in this packet; for Version 9, this value is 0x0009.
Count	Number of FlowSet records (both template and data) contained within this packet.
System Uptime	Time in milliseconds since this device was first booted.
UNIX Seconds	Seconds since 0000 Coordinated Universal Time (UTC) 1970.
Package Sequence	Incremental sequence counter of all export packets sent by this export device; this value is cumulative, and it can be used to find out whether any export packets have been missed. This is a change from the NetFlow Version 5 and Version 8 headers, where this number represented "total flows."
Source ID	The Source ID field is a 32-bit value that is used to guarantee uniqueness for each flow exported from a particular device. (The Source ID field is the equivalent of the engine type and engine ID fields found in the NetFlow Version 5 and Version 8 headers.) The format of this field is vendor-specific. In Cisco's implementation, the first two bytes are reserved for future expansion, and are always zero. Byte 3 provides uniqueness with respect to the routing engine on the exporting device. Byte 4 provides uniqueness with respect to the particular line card or Versatile Interface Processor on the exporting device. Collector devices should use the combination of the source IP address and the source ID field to associate an incoming NetFlow export packet with a unique instance of NetFlow on a particular device.

NetFlow Flow Record and Export Format Content Information

This section gives details about the Cisco export format flow record. The table below indicates which flow record format fields are available for Version 5, and 9. (Y indicates that the field is available. N indicates that the field is not available.)

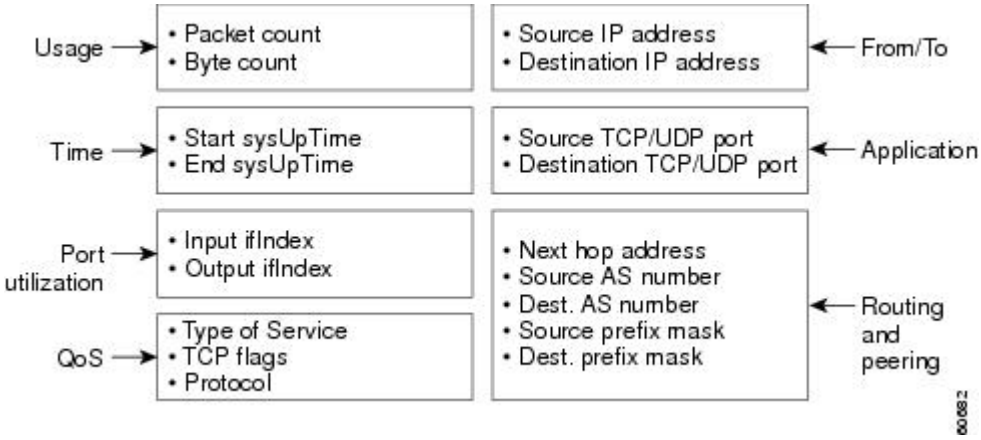
Table 16 NetFlow Flow Record Format Fields for Format Versions 5 and 9

Field	Version 5	Version 9
source IP address	Y	Y
destination IP address	Y	Y
source TCP/UDP application port	Y	Y
destination TCP/UDP application port	Y	Y
next hop router IP address	Y	Y
input physical interface index	Y	Y
output physical interface index	Y	Y
packet count for this flow	Y	Y
byte count for this flow	Y	Y
start of flow timestamp	Y	Y
end of flow timestamp	Y	Y
IP Protocol (for example, TCP=6; UDP=17)	Y	Y
Type of Service (ToS) byte	Y	Y
TCP Flags (cumulative OR of TCP flags)	Y	Y
source AS number	Y	Y
destination AS number	Y	Y
source subnet mask	Y	Y
destination subnet mask	Y	Y
flags (indicates, among other things, which flows are invalid)	Y	Y
Other flow fields[3]	N	Y

3 For a list of other flow fields available in Version 9 export format, see Figure 5 .

The figure below is an example of the NetFlow Version 5 export record format, including the contents and description of byte locations. The terms in **bold** indicate values that were added for the Version 5 format.

Figure 15 NetFlow Version 5 Export Record Format



The table below shows the field names and descriptions for the NetFlow Version 5 export record format.

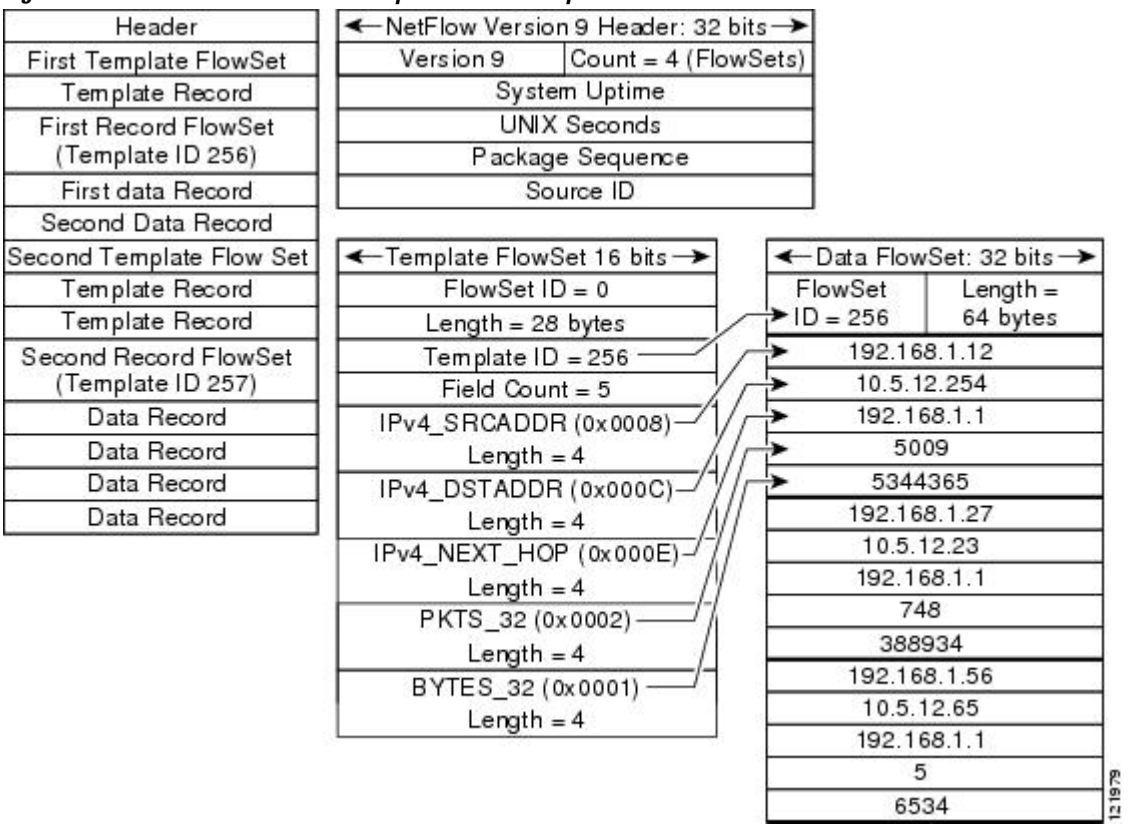
Table 17 NetFlow Version 5 Export Record Format Field Names and Descriptions

Content	Bytes	Descriptions
srcaddr	0-3	Source IP address
dstaddr	4-7	Destination IP address
nexthop	8-11	Next hop router's IP address
input	12-13	Ingress interface SNMP ifIndex
output	14-15	Egress interface SNMP ifIndex
dPkts	16-19	Packets in the flow
dOctets	20-23	Octets (bytes) in the flow
first	24-27	SysUptime at start of the flow
last	28-31	SysUptime at the time the last packet of the flow was received
srcport	32-33	Layer 4 source port number or equivalent
dstport	34-35	Layer 4 destination port number or equivalent
pad1	36	Unused (zero) byte
tcp_flags	37	Cumulative OR of TCP flags

Content	Bytes	Descriptions
prot	38	Layer 4 protocol (for example, 6=TCP, 17=UDP)
tos	39	IP type-of-service byte
src_as	40-41	Autonomous system number of the source, either origin or peer
dst_as	42-43	Autonomous system number of the destination, either origin or peer
src_mask	44	Source address prefix mask bits
dst_mask	45	Destination address prefix mask bits
pad2	46-47	Packet Assembler/Disassembler (PAD) 2 is unused (zero) bytes

The figure below shows a typical flow record for the Version 9 export format. The NetFlow Version 9 export record format is different from the traditional NetFlow fixed format export record. In NetFlow Version 9, a template describes the NetFlow data and the flow set contains the actual data. This allows for flexible export. Detailed information about the fields currently in Version 9 and the export format architecture are available in the NetFlow Version 9 Flow-Record Format document.

Figure 16 NetFlow Version 9 Export Packet Example



For all export versions, you specify a destination where NetFlow data export packets are sent, such as the workstation running NetFlow Collection Engine, either when the number of recently expired flows reaches a predetermined maximum, or every second--whichever occurs first. For a Version 5 datagram, up to 30 flows can be sent in a single UDP datagram of approximately 1500 bytes.

For detailed information on the flow record formats, data types, and export data fields for Version 9 and platform-specific information when applicable, see Appendix 2 in the NetFlow Solutions Service Guide.

NetFlow Data Export Format Selection

NetFlow exports data in UDP datagrams in export format Version 9, 8, or 5. The table below describes situations when you might select a particular NetFlow export format.

Table 18 When to Select a Particular NetFlow Export Format

Export Format	Select When...
Version 9	You need to export data from various technologies, such as Multicast, DoS, IPv6 and so on. The Version 9 export format supports export from the main cache and from aggregation caches.
Version 8	You need to export data from aggregation caches. The Version 8 export format is available only for export from aggregation caches.
Version 5	You need to export data from the NetFlow main cache, and you are not planning to support new features. The Version 5 export format does not support export from aggregation caches.

NetFlow Version 9 Data Export Format

NetFlow Version 9 data export supports Cisco Express Forwarding switching and fast switching.

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.

Using Version 9 export, you define new formats on the router that you can send to the NetFlow Collection Engine (formerly called NetFlow FlowCollector) at set intervals. You enable the features that you want, and the field values corresponding to those features are sent to the NetFlow Collection Engine.

Third-party business partners, who produce applications that provide NetFlow Collection Engine or display services for NetFlow need not recompile their applications each time a new NetFlow technology is added. Instead, with the NetFlow v9 Export Format feature, they can use an external data file that documents the known template formats and field types.

In NetFlow Version 9:

- 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, Stream Control Transmission Protocol (SCTP), and so on).

NetFlow Version 9 Template-Based Flow Record Format

The main feature of the NetFlow Version 9 export format is that it is template based. A template describes a NetFlow record format and attributes of the fields (such as type and length) within the record. The router assigns each template an ID, which is communicated to the NetFlow Collection Engine, along with the template description. The template ID is used for all further communication from the router to the NetFlow Collection Engine.

NetFlow Version 9 Export Flow Records

The basic output of NetFlow is a flow record. In the NetFlow Version 9 export format, a flow record follows the same sequence of fields as found in the template definition. The template to which NetFlow flow records belong is determined by the prefixing of the template ID to the group of NetFlow flow records that belong to a template. For a complete discussion of existing NetFlow flow-record formats, see the NetFlow Services Solutions Guide.

NetFlow Version 9 Export Packet

In NetFlow Version 9, an export packet consists of the packet header and flowsets. The packet header identifies the new version and provides other NetFlow Version 9 Data Export Format, page 49 Figure 3 for Version 9 export packet header details. Flowsets are of two types: template flowsets and data flowsets. The template flowset describes the fields that will be in the data flowsets (or flow records). Each data flowset contains the values or statistics of one or more flows with the same template ID. When the NetFlow Collection Engine receives a template flowset, it stores the flowset and export source address so that subsequent data flowsets that match the flowset ID and source combination are parsed according to the field definitions in the template flowset. Version 9 supports NetFlow Collection Engine Version 4.0. For an example of a Version 9 export packet, see NetFlow Version 9 Data Export Format, page 49.

NetFlow Version 8 Data Export Format

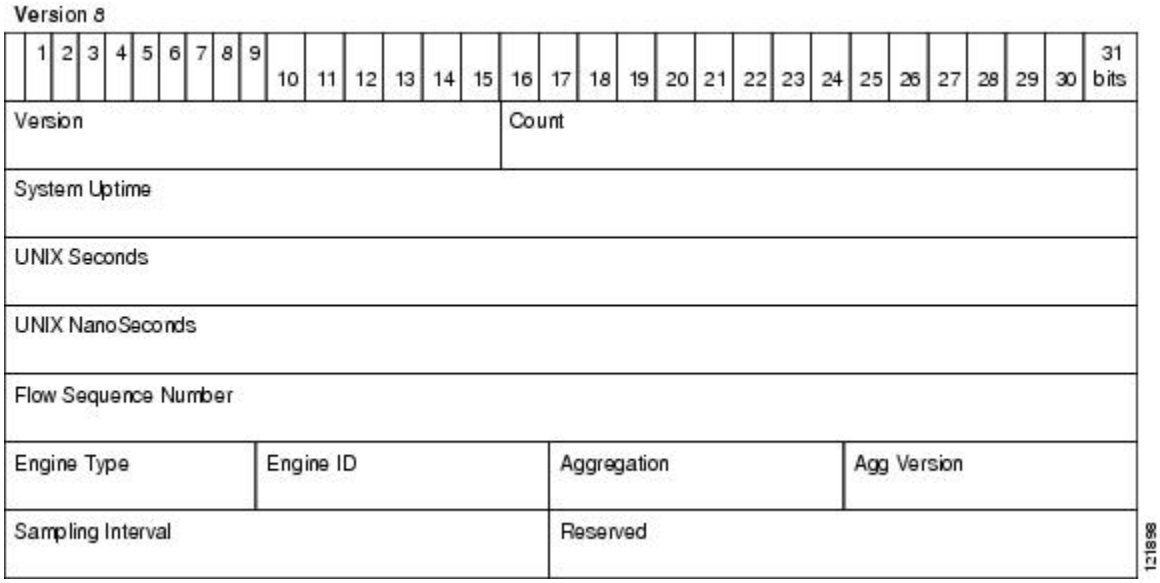
The Version 8 data export format is the NetFlow export format used when the router-based NetFlow aggregation feature is enabled on Cisco IOS XE router platforms. The Version 8 format allows for export datagrams to contain a subset of the Version 5 export data that is based on the configured aggregation cache scheme. For example, a certain subset of the Version 5 export data is exported for the destination prefix aggregation scheme, and a different subset is exported for the source-prefix aggregation scheme.

The Version 8 export format was introduced in the Cisco IOS NetFlow Aggregation feature. An additional six aggregation schemes that also use Version 8 format were defined for the NetFlow ToS-Based Router Aggregation feature. Refer to the Configuring NetFlow Aggregation Caches module for information about configuring Version 8 data export for aggregation caches.

The Version 8 datagram consists of a header with the version number (which is 8) and time stamp information, followed by one or more records corresponding to individual entries in the NetFlow cache.

The figure below displays the NetFlow Version 8 export packet header format.

Figure 17 NetFlow Version 8 Export Packet Header Format



The table below lists the NetFlow Version 8 export packet header field names and definitions.

Table 19 NetFlow Version 8 Export Packet Header Field Names and Descriptions

Field Name	Description
Version	Flow export format version number. In this case 8.
Count	Number of export records in the datagram.
System Uptime	Number of milliseconds since the router last booted.
UNIX Seconds	Number of seconds since 0000 UTC 1970.
UNIX NanoSeconds	Number of residual nanoseconds since 0000 UTC 1970.
Flow Sequence Number	Sequence counter of total flows sent for this export stream.
Engine Type	The type of switching engine. Route Processor (RP) = 0 and linecard (LC) = 1.
Engine ID	Slot number of the NetFlow engine.
Aggregation	Type of aggregation scheme being used.
Agg Version	Aggregation subformat version number. The current value is "2."

Field Name	Description
Sampling Interval	Interval value used if Sampled NetFlow is configured.
Reserved	Reserved.

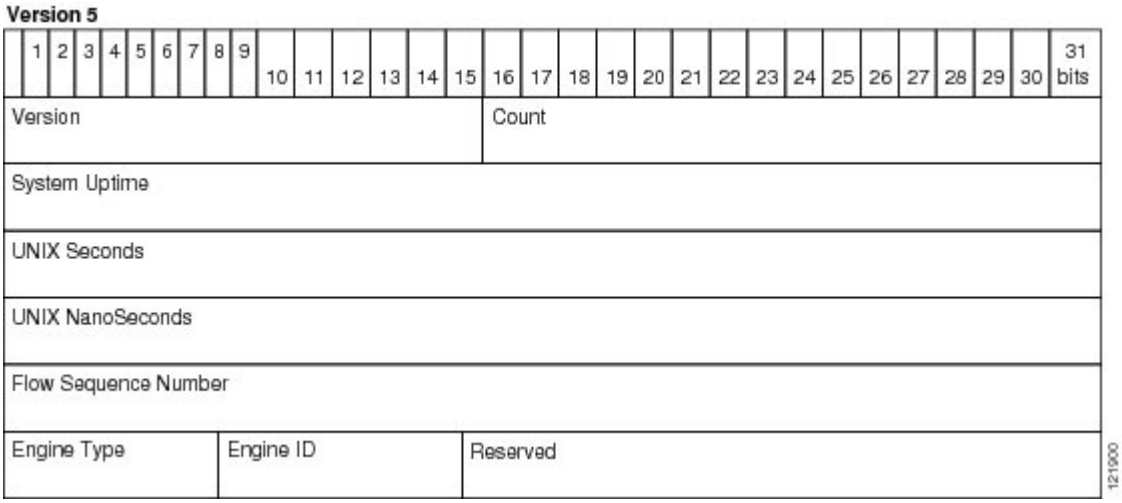
NetFlow Version 5 Data Export Format

The Version 5 data export format adds support for BGP autonomous system information and flow sequence numbers.

Because NetFlow uses UDP to send export datagrams, datagrams can be lost. The Version 5 header format contains a flow sequence number to find out whether flow export information has been lost. The sequence number is equal to the sequence number of the previous datagram plus the number of flows in the previous datagram. After receiving a new datagram, the receiving application can subtract the expected sequence number from the sequence number in the header to get the number of missed flows.

All fields in Version 5 export format are in network byte order. The figure below shows the NetFlow Version 5 export packet header format.

Figure 18 NetFlow Version 5 Export Packet Header Format



The table below lists the NetFlow Version 5 export packet header field names and descriptions.

Table 20 NetFlow Version 5 Export Packet Header Field Names and Descriptions

Bytes	Field	Description
0 to 1	Version	Flow export format version number. In this case 5.
2 to 3	Count	Number of export records in the datagram.

Bytes	Field	Description
4 to 7	System Uptime	Number of milliseconds since the router last booted.
8 to 11	UNIX Seconds	Number of seconds since 0000 UTC 1970.
12 to 15	UNIX NanoSeconds	Number of residual nanoseconds since 0000 UTC 1970.
16 to 19	Flow Sequence Number	Sequence counter of total flows sent for this export stream.
20	Engine Type	The type of switching engine. RP = 0 and LC = 1.
21	Engine ID	Slot number of the NetFlow engine.
22 to 23	Reserved	Reserved.

The table below lists the byte definitions for the Version 5 flow record format.

Table 21 Version 5 Flow Record Format

Bytes	Content	Description
0 to 3	srcaddr	Source IP address.
4 to 7	dstaddr	Destination IP address.
8 to 11	nexthop	IP address of the next hop router.
12 to 15	input and output	SNMP index of the input and output interfaces.
16 to 19	dPkts	Packets in the flow.
20 to 23	dOctets	Total number of Layer 3 bytes in the flow's packets.
24 to 27	First	SysUptime at start of flow.
28 to 31	Last	SysUptime at the time the last packet of flow was received.
32 to 35	srcport and dstport	TCP/UDP source and destination port number or equivalent.
36 to 39	pad1, tcp_flags, prot, and tos	Unused (zero) byte, cumulative OR of TCP flags, IP protocol (for example, 6 = TCP, 17 = UDP), and IP ToS.

Bytes	Content	Description
40 to 43	src_as and dst_as	Autonomous system of the source and destination, either origin or peer.
44 to 47	src_mask, dst_mask, and pad2	Source and destination address prefix mask bits. PAD 2 is unused (zero) bytes.

Egress NetFlow Accounting Benefits NetFlow Accounting Simplified

The Egress NetFlow Accounting feature can simplify NetFlow configuration, which is illustrated in the following example.

In the figures below, both incoming and outgoing (ingress and egress) flow statistics are required for the server. The server is attached to Router B. The "cloud" in the figure represents the core of the network and includes MPLS VPNs.

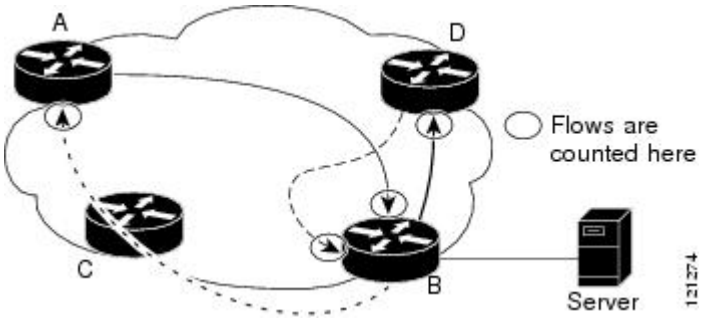
All traffic denoted by the arrows must be accounted for. The solid arrows represent IP traffic and the dotted arrows represent MPLS VPNs.

The first figure below shows how the flow traffic was tracked before the introduction of the Egress NetFlow Accounting feature. The second figure below shows how the flow traffic is tracked after the introduction of the Egress NetFlow Accounting feature. The Egress NetFlow Accounting feature simplifies configuration tasks and makes it easier for you to collect and track incoming and outgoing flow statistics for the server in this example.

Because only ingress flows could be tracked before the Egress NetFlow Accounting feature was introduced, the following NetFlow configurations had to be implemented for the tracking of ingress and egress flows from Router B:

- Enable NetFlow on an interface on Router B to track ingress IP traffic from Router A to Router B.
- Enable NetFlow on an interface on Router D to track ingress IP traffic from Router B to Router D.
- Enable NetFlow on an interface on Router A to track ingress traffic from the MPLS VPN from Router B to Router A.
- Enable NetFlow on an interface on Router B to track ingress traffic from the MPLS VPN from Router D to Router B.

Figure 19 Ingress-Only NetFlow Example



A configuration such as the one used in the figure above requires that NetFlow statistics from three separate routers be added together to obtain the flow statistics for the server.

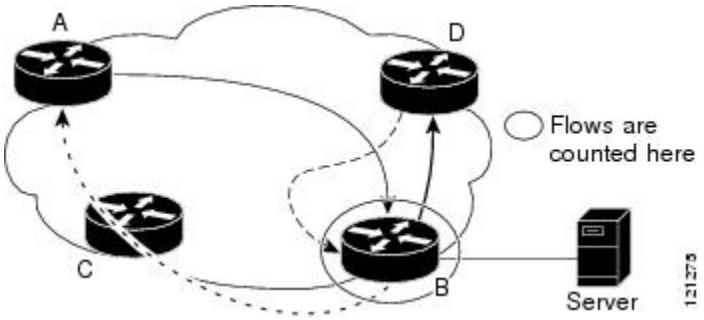
In comparison, the example in the figure below shows NetFlow, the Egress NetFlow Accounting feature, and the MPLS Egress NetFlow Accounting feature being used to capture ingress and egress flow statistics for Router B, thus obtaining the required flow statistics for the server.

In the figure below, the following NetFlow configurations are applied to Router B:

- Enable NetFlow on an interface on Router B to track ingress IP traffic from Router A to Router B.
- Enable the Egress NetFlow Accounting feature on an interface on Router B to track egress IP traffic from Router B to Router D.
- Enable NetFlow an interface on Router B to track ingress traffic from the MPLS VPN from Router B to Router D.
- Enable NetFlow on an interface on Router B to track ingress traffic from the MPLS VPN from Router B to Router A.

After NetFlow is configured on Router B, you can display all NetFlow statistics for the server by entering the **show ip cache flow** command or the **show ip cache verbose flow** command for Router B.

Figure 20 Egress NetFlow Accounting Example



NetFlow Subinterface Support Benefits Fine-Tuning Your Data Collection

You can configure NetFlow on a per-subinterface basis. If your network contains thousands of subinterfaces and you want to collect export records from only a few subinterfaces, you can do that. The result is lower bandwidth requirements for NetFlow data export and reduced platform requirements for NetFlow data-collection devices.

The configuration of NetFlow on selected subinterfaces provides the following benefits:

- Reduced bandwidth requirement between routing devices and NetFlow management workstations.
- Reduced NetFlow workstation requirements; the number of flows sent to the workstation for processing is reduced.

NetFlow Multiple Export Destinations Benefits

The NetFlow Multiple Export Destinations feature enables configuration of multiple destinations for the NetFlow data. With this feature enabled, two identical streams of NetFlow data are sent to the destination host. Currently, the maximum number of export destinations allowed is two.

The NetFlow Multiple Export Destinations feature improves the chances of receiving complete NetFlow data because it provides redundant streams of data. Because the same export data is sent to more than one NetFlow collector, fewer packets are lost.

How to Configure NetFlow and NetFlow Data Export

Configuring NetFlow

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-type interface-number*
4. **ip flow** {**ingress** | **egress**}
5. **exit**
6. Repeat Steps 3 through 5 to enable NetFlow on other interfaces
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.
Step 3	**interface** *interface-type interface-number* **Example:** `Router(config)# interface fastethernet 0/0/0`	(Required) Specifies the interface that you want to enable NetFlow on and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**ip flow** {**ingress** | **egress**} **Example:** `Router(config-if)# ip flow ingress`	(Required) Enables NetFlow on the interface. • **ingress** --Captures traffic that is being received by the interface. • **egress** --Captures traffic that is being transmitted by the interface. This is the Egress NetFlow Accounting feature that is described in the Egress NetFlow Accounting Benefits NetFlow Accounting Simplified, page 54.
Step 5	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode and returns to global configuration mode. **Note** You only need to use this command if you want to enable NetFlow on another interface.
Step 6	Repeat Steps 3 through 5 to enable NetFlow on other interfaces	(Optional) --
Step 7	**end** **Example:** `Router(config-if)# end`	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Verifying That NetFlow Is Operational and Viewing NetFlow Statistics

To verify that NetFlow is operational and to view the NetFlow statistics, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **show ip cache flow**
3. **show ip cache verbose flow**
4. **end**

DETAILED STEPS

Step 1 **enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
Router#
```

Step 2 **show ip cache flow**

Use this command to verify that NetFlow is operational and to display a summary of the NetFlow statistics. The following is sample output from this command:

Example:

```
Router# show ip cache flow
IP packet size distribution (1103746 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .249 .694 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .027 .000 .027 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 278544 bytes
  35 active, 4061 inactive, 980 added
  2921778 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-FTP            108      0.0      1133    40      2.4    1799.6       0.9
TCP-FTPD           108      0.0      1133    40      2.4    1799.6       0.9
TCP-WWW             54      0.0      1133    40      1.2    1799.6       0.8
TCP-SMTP            54      0.0      1133    40      1.2    1799.6       0.8
TCP-BGP             27      0.0      1133    40      0.6    1799.6       0.7
TCP-NNTP            27      0.0      1133    40      0.6    1799.6       0.7
TCP-other          297      0.0      1133    40      6.8    1799.7       0.8
UDP-TFTP            27      0.0      1133    28      0.6    1799.6       1.0
UDP-other          108      0.0      1417    28      3.1    1799.6       0.9
ICMP               135      0.0      1133   427      3.1    1799.6       0.8
Total:             945      0.0      1166    91     22.4    1799.6       0.8
SrcIf         SrcIPaddress    DstIf          DstIPaddress    Pr SrcP DstP  Pkts
FEt0/0/0      192.168.67.6    FEt1/0/0.1     172.16.10.200   01 0000 0C01    51
FEt0/0/0      10.10.18.1      Null           172.16.11.5     11 0043 0043    51
FEt0/0/0      10.10.18.1      Null           172.16.11.5     11 0045 0045    51
FEt0/0/0      10.234.53.1     FEt1/0/0.1     172.16.10.2     01 0000 0800    51
FEt0/0/0      10.10.19.1      Null           172.16.11.6     11 0044 0044    51
FEt0/0/0      10.10.19.1      Null           172.16.11.6     11 00A2 00A2    51
FEt0/0/0      192.168.87.200  FEt1/0/0.1     172.16.10.2     06 0014 0014    50
FEt0/0/0      192.168.87.200  FEt1/0/0.1     172.16.10.2     06 0015 0015    52
.
.
.
FEt0/0/0      172.16.1.84     FEt1/0.1       172.16.10.19    06 0087 0087    50
FEt0/0/0      172.16.1.84     FEt1/0.1       172.16.10.19    06 0050 0050    51
FEt0/0/0      172.16.1.85     FEt1/0.1       172.16.10.20    06 0089 0089    49
FEt0/0/0      172.16.1.85     FEt1/0.1       172.16.10.20    06 0050 0050    50
FEt0/0/0      10.251.10.1     FEt1/0.1       172.16.10.2     01 0000 0800    51
FEt0/0/0      10.162.37.71    Null           172.16.11.3     06 027C 027C    49
Router#
```

Step 3 **show ip cache verbose flow**

Use this command to verify that NetFlow is operational and to display a detailed summary of the NetFlow statistics. The following is sample output from this command:

Example:

```
Router# show ip cache verbose flow
ToS
IP packet size distribution (1130681 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .249 .694 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
```

```
   .000 .000 .027 .000 .027 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 278544 bytes
  35 active, 4061 inactive, 980 added
  2992518 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-FTP            108      0.0      1133    40      2.4    1799.6       0.9
TCP-FTPD           108      0.0      1133    40      2.4    1799.6       0.9
TCP-WWW             54      0.0      1133    40      1.2    1799.6       0.8
TCP-SMTP            54      0.0      1133    40      1.2    1799.6       0.8
TCP-BGP             27      0.0      1133    40      0.6    1799.6       0.7
TCP-NNTP            27      0.0      1133    40      0.6    1799.6       0.7
TCP-other          297      0.0      1133    40      6.6    1799.7       0.8
UDP-TFTP            27      0.0      1133    28      0.6    1799.6       1.0
UDP-other          108      0.0      1417    28      3.0    1799.6       0.9
ICMP               135      0.0      1133   427      3.0    1799.6       0.8
Total:             945      0.0      1166    91     21.9    1799.6       0.8
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
FEt0/0/0        192.168.67.6    FEt1/0.1       172.16.10.200   01 00  10     799
0000 /0  0                     0C01 /0  0     0.0.0.0                28  1258.1
FEt0/0/0        10.10.18.1      Null           172.16.11.5     11 00  10     799
0043 /0  0                     0043 /0  0     0.0.0.0                28  1258.0
FEt0/0/0        10.10.18.1      Null           172.16.11.5     11 00  10     799
0045 /0  0                     0045 /0  0     0.0.0.0                28  1258.0
FEt0/0/0        10.234.53.1     FEt1/0.1       172.16.10.2     01 00  10     799
0000 /0  0                     0800 /0  0     0.0.0.0                28  1258.1
FEt0/0/0        10.10.19.1      Null           172.16.11.6     11 00  10     799
0044 /0  0                     0044 /0  0     0.0.0.0                28  1258.1
.
.
.
FEt0/0/0       172.16.1.84     FEt1/0/0.1     172.16.10.19    06 00  00     799
0087 /0  0                     0087 /0  0     0.0.0.0                40  1258.1
FEt0/0/0       172.16.1.84     FEt1/0/0.1     172.16.10.19    06 00  00     799
0050 /0  0                     0050 /0  0     0.0.0.0                40  1258.0
FEt0/0/0       172.16.1.85     FEt1/0/0.1     172.16.10.20    06 00  00     798
0089 /0  0                     0089 /0  0     0.0.0.0                40  1256.5
FEt0/0/0       172.16.1.85     FEt1/0/0.1     172.16.10.20    06 00  00     799
0050 /0  0                     0050 /0  0     0.0.0.0                40  1258.0
FEt0/0/0        10.251.10.1    FEt1/0/0.1     172.16.10.2     01 00  10     799
0000 /0  0                     0800 /0  0     0.0.0.0              1500  1258.1
FEt0/0/0        10.162.37.71   Null           172.16.11.3     06 00  00     798
027C /0  0                     027C /0  0     0.0.0.0                40  1256.4
Router#
```

Step 4 **end**

Use this command to exit privileged EXEC mode.

Example:

```
Router# end
```

Configuring NetFlow Data Export Using the Version 9 Export Format

This task does not include the steps for configuring NetFlow. You must configure NetFlow by enabling it on at least one interface in the router in order to export traffic data with NetFlow Data Export. Refer to the Configuring NetFlow, page 56 for information about configuring NetFlow.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-export destination** {{*ip-address* | *hostname*} *udp-port*}
4. Repeat Step 3 to configure a second NetFlow export destination, if desired.
5. **ip flow-export source** *interface-type interface-number*
6. **ip flow-export version 9 [origin-as | peer-as] [bgp-nexthop]**
7. **ip flow-export template refresh-rate** *packets*
8. **ip flow-export template timeout-rate** *minutes*
9. **ip flow-export template options export-stats**
10. **ip flow-export template options refresh-rate** *packets*
11. **ip flow-export template options timeout-rate** *minutes*
12. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enters privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.
Step 3	**ip flow-export destination** {{*ip-address* | *hostname*} *udp-port*} **Example:** `Router(config)# ip flow-export destination 172.16.10.2 99`	(Required) Specifies the IP address or hostname of the NetFlow collector, and the UDP port the NetFlow collector is listening on.

	Command or Action	Purpose
Step 4	Repeat Step 3 to configure a second NetFlow export destination, if desired.	(Optional) You can configure a maximum of two export destinations for NetFlow. This is the NetFlow Multiple Export Destinations feature that is described in the NetFlow Multiple Export Destinations Benefits, page 55.
Step 5	**ip flow-export source** *interface-type interface-number* **Example:** `Router(config)# ip flow-export source fastethernet 0/0/0`	(Optional) The IP address of the interface specified is used as the source IP address for the UDP datagrams that are sent by NetFlow data export to the destination host. **Note** Do not use the IP address or interface name of the Management Interface on the router as the source address.
Step 6	**ip flow-export version 9 [origin-as | peer-as] [bgp-nexthop]** **Example:** `Router(config)# ip flow-export version 9`	(Optional) Enables the export of information in NetFlow cache entries. • **version 9** --Specifies that the export packet uses the Version 9 format. • **origin-as** --Specifies that export statistics include the originating AS for the source and destination. • **peer-as** --Specifies that export statistics include the peer AS for the source and destination. • **bgp-nexthop** --Specifies that export statistics include BGP next hop-related information.
Step 7	**ip flow-export template refresh-rate** *packets* **Example:** `Router(config)# ip flow-export template refresh-rate 15`	(Optional) Enables the export of information in NetFlow cache entries. • **template** --Specifies template-specific configurations. • **refresh-rate** *packets* --Specifies the number of packets exported before the templates are resent. You can specify from 1 to 600 packets. The default is 20 packets.
Step 8	**ip flow-export template timeout-rate** *minutes* **Example:** `Router(config)# ip flow-export template timeout-rate 90`	(Optional) Enables the export of information in NetFlow cache entries. • **template** --Specifies that the **timeout-rate** keyword applies to the template. • **timeout-rate** *minutes* --Specifies the time elapsed before the templates are resent. You can specify from 1 to 3600 minutes. The default is 30 minutes.
Step 9	**ip flow-export template options export-stats** **Example:** `Router(config)# ip flow-export template options export-stats`	(Optional) Enables the export of information in NetFlow cache entries. • **template** --Specifies template-specific configurations. • **options** --Specifies template options. • **export-stats** --Specifies that the export statistics include the total number of flows exported and the total number of packets exported.

	Command or Action	Purpose
Step 10	**ip flow-export template options refresh-rate** *packets* **Example:** `Router(config)# ip flow-export template options refresh-rate 25`	(Optional) Enables the export of information in NetFlow cache entries. • **template** --Specifies template-specific configurations. • **options** --Specifies template options. • **refresh-rate** *packets* --Specifies the number of packets exported before the templates are resent. You can specify from 1 to 600 packets. The default is 20 packets.
Step 11	**ip flow-export template options timeout-rate** *minutes* **Example:** `Router(config)# ip flow-export template options timeout-rate 120`	(Optional) Enables the export of information in NetFlow cache entries. • **template** --Specifies template-specific configurations. • **options** --Specifies template options. • **timeout-rate** *minutes* --Specifies the time elapsed before the templates are resent. You can specify from 1 to 3600 minutes. The default is 30 minutes.
Step 12	**end** **Example:** `Router(config)# end`	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Verifying That NetFlow Data Export Is Operational

To verify that NetFlow data export is operational and to view the statistics for NetFlow data export, perform the following task.

SUMMARY STEPS

1. **enable**
2. **show ip flow export**
3. **show ip flow export template**
4. **end**

DETAILED STEPS

Step 1 **enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
```

Router#

Step 2 **show ip flow export**

Use this command to display the statistics for the NetFlow data export, including statistics for the main cache and for all other enabled caches. The following is sample output from this command:

Example:

```
Router# show ip flow export
Flow export v9 is enabled for main cache
  Exporting flows to 172.16.10.2 (99)
  Exporting using source interface FastEthernet0/0/0
  Version 9 flow records
  0 flows exported in 0 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
Router#
```

Step 3 **show ip flow export template**

Use this command to display the statistics for the NetFlow data export (such as the template timeout rate and the refresh rate) for the template-specific configurations. The following is sample output from this command:

Example:

```
Router# show ip flow export template
   Template Options Flag = 1
   Total number of Templates added = 1
   Total active Templates = 1
   Flow Templates active = 0
   Flow Templates added = 0
   Option Templates active = 1
   Option  Templates added = 1
   Template ager polls = 0
   Option Template ager polls = 140
Main cache version 9 export is enabled
 Template export information
   Template timeout = 90
   Template refresh rate = 15
 Option export information
   Option timeout = 120
   Option refresh rate = 25
Router#
```

Step 4 **end**

Use this command to exit privileged EXEC mode.

Example:

```
Router# end
```

Clearing NetFlow Statistics on the Router

To clear NetFlow statistics on the router, perform the following task.

SUMMARY STEPS

1. **enable**
2. **clear ip flow stats**
3. **end**

DETAILED STEPS

Step 1 **enable**
Use this command to enable privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
Router#
```

Step 2 **clear ip flow stats**
Use this command to clear the NetFlow statistics on the router. For example:

Example:

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

Step 3 **end**
Use this command to exit privileged EXEC mode.

Example:

```
Router# end
```

Customizing the NetFlow Main Cache Parameters

NetFlow operates by creating a NetFlow cache entry (a flow record) for each active flow. A flow record is maintained within the NetFlow cache for all active flows. Each flow record in the NetFlow cache contains fields that can later be exported to a collection device, such as the NetFlow Collection Engine. NetFlow enables the accumulation of data on flows. Each flow is identified by unique characteristics such as IP address, interface, application, and ToS.

To customize the parameters for the main NetFlow cache, perform the following steps.

- NetFlow Cache Entry Management on a Routing Device, page 64
- NetFlow Cache Size, page 65

NetFlow Cache Entry Management on a Routing Device

The routing device checks the NetFlow cache once per second and causes the flow to expire in the following instances:

- The flow cache has become full.
- A flow becomes inactive. By default, a flow unaltered in the last 15 seconds is classified as inactive.
- An active flow has been monitored for a specified number of minutes. By default, active flows are flushed from the cache when they have been monitored for 30 minutes.

Routing device default timer settings are 15 seconds for the inactive timer and 30 minutes for the active timer. You can configure your own time interval for the inactive timer between 10 and 600 seconds. You can configure the time interval for the active timer between 1 and 60 minutes.

NetFlow Cache Size

After you enable NetFlow on an interface, NetFlow reserves memory to accommodate a number of entries in the NetFlow cache. Normally, the size of the NetFlow cache meets the needs of your NetFlow traffic rates. The cache default size is 64K flow cache entries. Each cache entry requires 64 bytes of storage. About 4 MB of DRAM are required for a cache with the default number of entries. You can increase or decrease the number of entries maintained in the cache, if required. For environments with a large amount of flow traffic (such as an Internet core router), we recommend a larger value such as 131072 (128K). To obtain information on your flow traffic, use the **show ip cache flow** command.

Using the **ip flow-cache entries** command, you can configure the size of your NetFlow cache between 1024 entries and 524,288 entries. Using the **cache entries** command (after you configure NetFlow aggregation), you can configure the size of the NetFlow aggregation cache from 1024 entries to 2,000,000 entries.

Caution We recommend that you not change the values for NetFlow cache entries. Improper use of this feature could cause network problems. To return to the default value for NetFlow cache entries, use the **no ip flow-cache entries** global configuration command.

Note If you modify any parameters for the NetFlow main cache after you enable NetFlow, the changes will not take effect until you reboot the router or disable NetFlow on every interface it is enabled on, and then re-enable NetFlow on the interfaces.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-type* interface-number
4. **no ip flow** {**ingress** | **egress**}
5. **exit**
6. Repeat Steps 3 through 5 for any remaining interfaces on which NetFlow has been enabled.
7. **ip flow-cache entries** *number*
8. **ip flow-cache timeout active** *minutes*
9. **ip flow-cache timeout inactive** *seconds*
10. **interface** *interface-type interface-number*
11. **ip flow** {**ingress** | **egress**}
12. **exit**
13. Repeat Steps 10 through 12 for the remaining interfaces on which you disabled NetFlow (Steps 3 through 5).
14. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.
Step 3	**interface** *interface-type* interface-number **Example:** `Router(config)# interface fastethernet 0/0/0`	(Required if NetFlow is already enabled on the interface.) Specifies the interface that you want to disable NetFlow on, and enters interface configuration mode.
Step 4	**no ip flow** {**ingress**	**egress**} **Example:** `Router(config-if)# no ip flow ingress`	(Required if NetFlow is enabled on the interface.) Disables NetFlow on the interface. • **ingress** --Captures traffic that is being received by the interface • **egress** --Captures traffic that is being transmitted by the interface

	Command or Action	Purpose
Step 5	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode and returns to global configuration mode. **Note** You only need to use this command if you need to disable NetFlow on another interface.
Step 6	Repeat Steps 3 through 5 for any remaining interfaces on which NetFlow has been enabled.	(Required if NetFlow is enabled on any other interfaces.) --
Step 7	**ip flow-cache entries** *number* **Example:** `Router(config)# ip flow-cache entries 131072`	(Optional) Changes the number of entries maintained in the NetFlow cache. • *number* --is the number of entries to be maintained. The valid range is from 1024 to 2000000 entries. The default is 200000.
Step 8	**ip flow-cache timeout active** *minutes* **Example:** `Router(config)# ip flow-cache timeout active 20`	(Optional) Specifies flow cache timeout parameters. • **active** --Specifies the active flow timeout. • *minutes* --Specifies the number of minutes that an active flow remains in the cache before the flow times out. The range is from 1 to 60. The default is 30.
Step 9	**ip flow-cache timeout inactive** *seconds* **Example:** `Router(config)# ip flow-cache timeout inactive 130`	(Optional) Specifies flow cache timeout parameters. • **inactive** --Specifies the inactive flow timeout. • *seconds* --Specifies 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 is 15.
Step 10	**interface** *interface-type interface-number* **Example:** `Router(config)# interface fastethernet 0/0/0`	(Required) Specifies the interface that you want to enable NetFlow on, and enters interface configuration mode.
Step 11	**ip flow** {**ingress** | **egress**} **Example:** `Router(config-if)# ip flow ingress`	(Required) Enables NetFlow on the interface. • **ingress** --captures traffic that is being received by the interface • **egress** --captures traffic that is being transmitted by the interface

	Command or Action	Purpose
Step 12	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode and returns to global configuration mode. **Note** You only need to use this command if you need to enable NetFlow on another interface.
Step 13	Repeat Steps 10 through 12 for the remaining interfaces on which you disabled NetFlow (Steps 3 through 5).	(Required for any other interfaces that you need to enable NetFlow on.) --
Step 14	**end** **Example:** `Router(config-if)# end`	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Configuration Examples for NetFlow and NetFlow Data Export

Example Configuring Egress NetFlow Accounting

The following example shows how to configure Egress NetFlow Accounting:

```
configure terminal
!
interface fastethernet 0/0/0
 ip flow egress
!
```

Example Configuring NetFlow Subinterface Support

This section contains examples for configuring NetFlow Subinterface Support, and contains the following examples:

Example NetFlow Subinterface Support for Ingress (Received) Traffic on a Subinterface

```
configure terminal
!
```

```
interface fastethernet 0/0/0.1
 ip flow ingress
!
```

Example NetFlow SubInterface Support for Egress (Transmitted) Traffic on a Subinterface

```
configure terminal
!
interface fastethernet 1/0/0.1
 ip flow egress
!
```

Note NetFlow performs additional checks for the status of each subinterface that requires more CPU processing time and bandwidth. If you have several subinterfaces configured and you want to configure NetFlow data capture on all of them, we recommend that you configure NetFlow on the main interface instead of on the individual subinterfaces.

Example Configuring NetFlow Multiple Export Destinations

The following example shows how to configure the NetFlow Multiple Export Destinations feature:

```
configure terminal
!
ip flow-export destination 10.10.10.10 9991
ip flow-export destination 172.16.10.2 9991
!
```

Note You can configure a maximum of two export destinations for the main cache and for each aggregation cache.

Example Configuring NetFlow Version 5 Data Export

The following example shows how to configure the NetFlow data export using the Version 5 export format with the peer AS information.

```
configure terminal

!

ip flow-export version 5 peer-as
ip flow-export destination 172.16.10.2 99
exit
Router# show ip flow export
Flow export v5 is enabled for main cache
  Exporting flows to 172.16.10.2 (99)
  Exporting using source IP address 172.16.6.1
  Version 5 flow records, peer-as
  0 flows exported in 0 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
```

```
  0 export packets were dropped due to encapsulation fixup failures
Router#
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
NetFlow commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS NetFlow Command Reference*
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
Information for installing, starting, and configuring the CNS NetFlow Collection Engine	Cisco CNS NetFlow Collection Engine Documentation
Discussion of NetFlow flow-record formats	NetFlow Services Solutions Guide

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 software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

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

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring NetFlow and NetFlow Data Export

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 22 Feature Information for Configuring NetFlow and NetFlow Data Export

Feature Name	Releases	Feature Configuration Information
Egress NetFlow Accounting	Cisco IOS XE Release 2.1	The Egress NetFlow Accounting feature allows NetFlow statistics to be gathered on egress traffic that is exiting the router. Previous versions of NetFlow allow statistics to be gathered only on ingress traffic that enters the router. In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers. The following commands were modified by this feature: **flow-sampler**, **ip flow egress, ip flow-egress input-interface**, **match**, **show ip cache flow**, **show ip cache verbose flow**, **show ip flow interface**.
NetFlow	Cisco IOS XE Release 2.1	NetFlow is a Cisco IOS XE application used to capture network traffic data. It provides statistics on packets flowing through the router, and is emerging as a primary network accounting and security technology. In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. The following commands were modified by this feature: **flow-sampler**, **ip flow egress, ip flow-egress input-interface**, **match**, **show ip cache flow**, **show ip cache verbose flow**, **show ip flow interface**.

Feature Name	Releases	Feature Configuration Information
NetFlow Multiple Export Destinations	Cisco IOS XE Release 2.1	The NetFlow Multiple Export Destinations feature enables configuration of multiple destinations of the NetFlow data. In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers. The following commands were modified by this feature: **ip flow-aggregation cache**, **ip flow-export destination**, **show ip flow export**.
NetFlow Subinterface Support	Cisco IOS XE Release 2.1	The NetFlow Subinterface Support feature provides the ability to enable NetFlow on a per-subinterface basis. In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers. The following commands were introduced or modified by this feature: **ip flow ingress, show ip interface**.
NetFlow v9 Export Format (Netflow Data Export [NDE] Version 5) (Netflow Data Export [NDE] Version 8)	Cisco IOS XE Release 2.1	The NetFlow v9 Export Format is flexible and extensible, which provides the versatility needed to support new fields and record types. This format accommodates new NetFlow-supported technologies such as Multicast and Network Address Translation (NAT). In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers. The following commands were modified by this feature: **debug ip flow export**, **export**, **ip flow-export**, **show ip flow export**.

Glossary

AS --autonomous system. A collection of networks under a common administration sharing a common routing strategy. Autonomous systems are subdivided by areas. An autonomous system must be assigned a unique 16-bit number by the Internet Assigned Numbers Authority (IANA).

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

BGP --Border Gateway Protocol. An interdomain routing protocol that replaces Exterior Gateway Protocol (EGP). 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 by a router to reach a certain destination.

export packet --Type of packet built by a device (for example, a router) with NetFlow services enabled that 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 --Cisco feature in which a route cache is used to expedite packet switching through a router.

flow --A set of packets with the same source IP address, destination IP address, protocol, source/destination ports, and type-of-service, and the same interface on which the flow is monitored. Ingress flows are associated with the input interface, and egress flows are associated with the output interface.

NetFlow --A Cisco IOS XE 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 Cisco 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 v9 --NetFlow export format Version 9. A flexible and extensible means for 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.

Using NetFlow Sampling to Select the Network Traffic to Track

This module contains information about and instructions for selecting the network traffic to track through the use of NetFlow sampling. The Random Sampled NetFlow feature, described in this module, allows you to collect data from specific subsets of traffic. The Random Sampled NetFlow feature provides NetFlow data for a subset of traffic in a Cisco router by processing only one randomly selected packet out of *n* sequential packets (*n* is a user-configurable parameter).

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

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 Using NetFlow Sampling to Select Network Traffic to Track

Before you can configure the Random Sampled NetFlow feature, you must:

- Configure the router for IP routing

- Configure Cisco Express Forwarding on your router and on the interfaces on which you want to configure Random Sampled NetFlow. Fast switching is not supported.
- Configure NetFlow Version 5 or Version 9 data export if you want to export NetFlow data (otherwise, NetFlow data is visible in the cache, but is not exported)
- Configure NetFlow Version 9 if you want to use sampler option templates or view NetFlow sampler IDs

Restrictions for Using NetFlow Sampling to Select Network Traffic to Track

If full NetFlow is enabled on an interface, it takes precedence over Random Sampled NetFlow (which will thus have no effect). This means that you should disable full NetFlow on an interface before enabling Random Sampled NetFlow on that interface.

Enabling Random Sampled NetFlow on a physical interface does not automatically enable Random Sampled NetFlow on subinterfaces; you must explicitly configure it on subinterfaces. Also, disabling Random Sampled NetFlow on a physical interface (or a subinterface) does not enable full NetFlow. This restriction prevents the transition to full NetFlow from overwhelming the physical interface (or subinterface). If you want full NetFlow, you must explicitly enable it.

If you enable Random Sampled NetFlow with Version 5 data export, sampler option templates are not exported. Use NetFlow Version 9 if you want to use sampler option templates.

Information About Using NetFlow Sampling to Select Network Traffic to Track

Sampling of NetFlow Traffic

NetFlow provides highly granular per-flow traffic statistics in a Cisco router. A flow is a unidirectional stream of packets that arrive at the router on the same subinterface, have the same source and destination IP addresses, Layer 4 protocol, TCP/UDP source and destination ports, and the same ToS (type of service) byte in the IP headers. The router accumulates NetFlow statistics in a NetFlow cache and can export them to an external device (such as the Cisco Networking Services (CNS) NetFlow Collection Engine) for further processing.

Full NetFlow accounts for all traffic entering the subinterface on which it is enabled. But in some cases, you might gather NetFlow data on only a subset of this traffic. The Random Sampled NetFlow feature provides a way to limit incoming traffic to only traffic of interest for NetFlow processing. Random Sampled NetFlow provides NetFlow data for a subset of traffic in a Cisco router by processing only one randomly selected packet out of *n* sequential packets.

Note Random Sampled NetFlow is more statistically accurate than Sampled NetFlow. NetFlow's ability to sample packets was first provided by a feature named Sampled NetFlow. The methodology that the Sampled NetFlow feature uses is *deterministic* sampling, which selects every nth packet for NetFlow processing on a per-interface basis. For example, if you set the sampling rate to 1 out of 100 packets, then Sampled NetFlow samples the 1st, 101st, 201st, 301st, and so on packets. Sampled NetFlow does not allow random sampling and thus can make statistics inaccurate when traffic arrives in fixed patterns.

Random Sampled NetFlow Sampling Mode

Sampling mode makes use of an algorithm that selects a subset of traffic for NetFlow processing. In the random sampling mode that the Random Sampled NetFlow feature uses, incoming packets are randomly selected so that one out of each n sequential packets is selected *on average* for NetFlow processing. For example, if you set the sampling rate to 1 out of 100 packets, then NetFlow might sample the 5th packet and then the 120th, 199th, 302nd, and so on. This sample configuration provides NetFlow data on 1 percent of total traffic. The n value is a parameter from 1 to 65535 packets that you can configure.

Random Sampled NetFlow The NetFlow Sampler

A NetFlow sampler map defines a set of properties (such as the sampling rate and NetFlow sampler name) for NetFlow sampling. Each NetFlow sampler map can be applied to one or many subinterfaces as well as physical interfaces. You can define up to eight NetFlow sampler maps.

For example, you can create a NetFlow sampler map named mysampler1 with the following properties: random sampling mode and a sampling rate of 1 out of 100 packets. This NetFlow sampler map can be applied to any number of subinterfaces, each of which would refer to mysampler1 to perform NetFlow sampling. Traffic from these subinterfaces is merged (from a sampling point of view). This introduces even more "randomness" than random per-subinterface NetFlow sampling does, but statistically it provides the same sampling rate of 1 out of 100 packets for each participating subinterface.

The sampling in random sampled NetFlow is done by NetFlow samplers. A NetFlow sampler is defined as an instance of a NetFlow sampler map that has been applied to a physical interface or subinterface. If full NetFlow is configured on a physical interface, it overrides random sampled NetFlow on all subinterfaces of this physical interface.

How to Configure NetFlow Sampling

Configuring Random Sampled NetFlow to Reduce the Impact of NetFlow Data Export

To configure and verify the configuration for the Random Sampled NetFlow feature, perform the following tasks:

- Verifying the Configuration of Random Sampled NetFlow, page 80

Defining a NetFlow Sampler Map

To define a NetFlow sampler map, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow-sampler-map** *sampler-map-name*
4. **mode random one-out-of** *sampling-rate*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.
Step 3	**flow-sampler-map** *sampler-map-name* **Example:** `Router(config)# flow-sampler-map mysampler1`	(Required) Defines a NetFlow sampler map and enters flow sampler map configuration mode. • The *sampler-map-name* argument is the name of the NetFlow sampler map to be defined.
Step 4	**mode random one-out-of** *sampling-rate* **Example:** `Router(config-sampler)# mode random one-out-of 100`	(Required) Enables random mode and specifies a sampling rate for the NetFlow sampler. • The **random** keyword specifies that sampling uses the random mode. • The **one-out-of** *sampling-rate* keyword-argument pair specifies the sampling rate (one out of every *n* packets) from which to sample. For *n*, you can specify from 1 to 65535 (packets).

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-sampler)# end`	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Applying a NetFlow Sampler Map to an Interface

To apply a NetFlow sampler map to an interface, perform the following steps.

You can apply a NetFlow sampler map to a physical interface (or a subinterface) to create a NetFlow sampler.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-type interface-number*
4. **flow-sampler** *sampler-map-name*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.
Step 3	**interface** *interface-type interface-number* **Example:** `Router(config)# fastethernet 1/0/0.2`	(Required) Specifies the interface and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**flow-sampler** *sampler-map-name* **Example:** `Router(config-if)# flow-sampler mysampler1`	(Required) Applies a NetFlow sampler map to the interface to create the NetFlow sampler. • The *sampler-map-name* argument is the name of the NetFlow sampler map to apply to the interface.
Step 5	**end** **Example:** `Router(config-if)# end`	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Verifying the Configuration of Random Sampled NetFlow

To verify the configuration of random sampled NetFlow, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **show flow-sampler**
3. **show ip cache verbose flow**
4. **show ip flow export template**
5. **end**

DETAILED STEPS

Step 1 **enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
```

Router#

Step 2 **show flow-sampler**

Use this command to display attributes (including mode, sampling rate, and number of sampled packets) of one or all Random Sampled NetFlow samplers to verify the sampler configuration. For example:

Example:

```
Router# show flow-sampler
Sampler : mysampler1, id : 1, packets matched : 10, mode : random sampling mode
  sampling interval is : 100
 Sampler : myflowsampler2, id : 2, packets matched : 5, mode : random sampling mode
  sampling interval is : 200
```

To verify attributes for a particular NetFlow sampler, use the **show flow-sampler** *sampler-map-name*command. For example, enter the following for a NetFlow sampler named mysampler1:

Example:

```
Router# show flow-sampler mysampler1
Sampler : mysampler1, id : 1, packets matched : 0, mode : random sampling mode
  sampling interval is : 100
```

Step 3 **show ip cache verbose flow**

Use this command to display additional NetFlow fields in the header when Random Sampled NetFlow is configured. For example:

Example:

```
Router# show ip cache verbose flow
...
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
BGP: BGP NextHop
Fet1/0/0        8.8.8.8        FEt0/0/0*      9.9.9.9         01 00  10       3
0000 /8  302                   0800 /8  300   3.3.3.3               100     0.1
BGP: 2.2.2.2         Sampler: 1  Class: 1  FFlags: 01
```

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

NetFlow flags (FFlags) that might appear in the **show ip cache verbose flow** command output are:

- FFlags: 01 (#define FLOW_FLAGS_OUTPUT 0x0001)--Egress flow
- FFlags: 02 (#define FLOW_FLAGS_DROP 0x0002)--Dropped flow (for example, dropped by an ACL)
- FFlags: 08 (#define FLOW_FLAGS_IPV6 0x0008)--IPv6 flow
- FFlags: 10 (#define FLOW_FLAGS_RSVD 0x0010)--Reserved

IPv6 and RSVD FFlags are seldom used. If FFlags is zero, the line is omitted from the output. If multiple flags are defined (logical ORed together), then both sets of flags are displayed in hexadecimal format.

Step 4 **show ip flow export template**

Use this command to display the statistics for the NetFlow data export (such as template timeout and refresh rate) for the template-specific configurations. For example:

Example:

```
Router# show ip flow export template
Template Options Flag = 0
   Total number of Templates added = 0
   Total active Templates = 0
   Flow Templates active = 0
   Flow Templates added = 0
   Option Templates active = 0
   Option Templates added = 0
   Template ager polls = 0
   Option Template ager polls = 0
Main cache version 9 export is enabled
 Template export information
   Template timeout = 30
   Template refresh rate = 20
```

```
 Option export information
   Option timeout = 30
   Option refresh rate = 20
```

Step 5 **end**

Use this command to exit privileged EXEC mode.

Example:

```
Router# end
```


- Troubleshooting Tips, page 82

Troubleshooting Tips

Use the **debug flow-sampler**command to display debugging output for Random Sampled NetFlow.

Configuration Examples for Configuring NetFlow Sampling

- Configuring Random Sampled NetFlow to Reduce the Impact of NetFlow Data Export Examples, page 82

Configuring Random Sampled NetFlow to Reduce the Impact of NetFlow Data Export Examples

- Defining a NetFlow Sampler Map Example, page 82
- Applying a NetFlow Sampler Map to an Interface Example, page 82

Defining a NetFlow Sampler Map Example

The following example shows how to define a NetFlow sampler map named mysampler1:

```
configure terminal
!
flow-sampler-map mysampler1
 mode random one-out-of 100
 end
```

Applying a NetFlow Sampler Map to an Interface Example

The following example shows how to enable Cisco Express Forwarding switching and apply a NetFlow sampler map named mysampler1 to Fastethernet interface 1/0/0 to create a NetFlow sampler on that interface:

```
configure terminal
!
ip cef
!
```

```
interface fastethernet 1/0/0
 flow-sampler mysampler1
 end
```

Additional References

Related Documents

Related Topic	Document Title
NetFlow commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS NetFlow Command Reference*
Tasks for configuring NetFlow to capture and export network traffic data	"Configuring NetFlow and NetFlow Data Export"
Tasks for configuring Random Sampled NetFlow	"Using NetFlow Sampling to Select the Network Traffic to Track"
Tasks for configuring NetFlow aggregation caches	Configuring NetFlow Aggregation Caches"
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 XE releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

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

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Using NetFlow Sampling to Select Network Traffic to Track

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 23 Feature Information for Using NetFlow Sampling to Select Network Traffic to Track

Feature Name	Releases	Feature Configuration Information
Random Sampled NetFlow	Cisco IOS XE Release 2.1	Random Sampled NetFlow provides NetFlow data for a subset of traffic in a Cisco router by processing only one randomly selected packet out of n sequential packets (n is a user-configurable parameter). Packets are sampled as they arrive (before any NetFlow cache entries are made for those packets). Statistical traffic sampling substantially reduces consumption of router resources (especially CPU resources) while providing valuable NetFlow data. The main uses of Random Sampled NetFlow are traffic engineering, capacity planning, and applications where full NetFlow is not needed for an accurate view of network traffic. In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified by this feature: **debug flow-sampler**, **flow-sampler**, **flow-sampler-map**, **ip flow-export, mode** (**flow sampler map configuration**), **show flow-sampler**.

Glossary

ACL --Access control list. A roster of users and groups of users kept by a router. The list is used to control access to or from the router for a number of services.

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

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

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

flow --Unidirectional stream of packets between a given source and destination. Source and destination are each defined by a network-layer IP address and transport-layer source and destination port numbers.

MQC --Modular Quality of Service (QoS) Command-line Interface (CLI). A CLI structure that lets you create traffic polices and attach them to interfaces. A traffic policy contains a traffic class and one or more QoS features. The QoS features in the traffic policy determine how the classified traffic is treated.

NBAR --Network-Based Application Recognition. A classification engine in Cisco IOS software that recognizes a wide variety of applications, including web-based applications and client/server applications that dynamically assign Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port numbers. After the application is recognized, the network can invoke specific services for that application. NBAR is a key part of the Cisco Content Networking architecture and works with QoS features to let you use network bandwidth efficiently.

NetFlow --Cisco IOS XE security and accounting feature that maintains per-flow information.

NetFlow sampler --A set of properties that are defined in a NetFlow sampler map that has been applied to at least one physical interface or subinterface.

NetFlow sampler map --The definition of a set of properties (such as the sampling rate) for NetFlow sampling.

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

ToS --type of service. Second byte in the IP header that indicates the desired quality of service for a specific datagram.