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 feature information and caveats, see 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 document.

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

Before you enable NetFlow:

- Configure the router for IP routing.
- Ensure that one of the following is enabled on your router, and on the interfaces that you want to configure NetFlow on: Cisco Express Forwarding (CEF), distributed CEF, or fast switching.
- 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.
- Export bandwidth--Export bandwidth use increases for Version 9 (because of template flowsets). 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.
- Management Interface--NetFlow data export is not supported through the Management Interface port.

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

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

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

NetFlow 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 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 that is different from another packet, it is considered to belong to another flow. A flow might contain other accounting fields (such as the autonomous system 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.

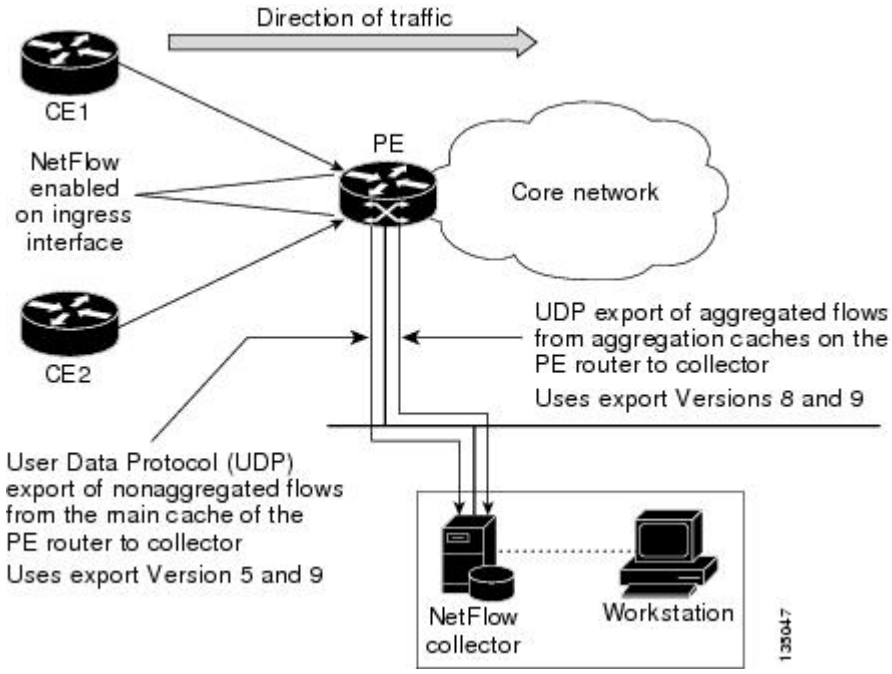
The key to NetFlow-enabled switching scalability and performance is highly intelligent flow cache management, especially for densely populated and busy edge routers handling large numbers of concurrent, short duration flows. The NetFlow cache management software contains a highly sophisticated set of 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 1: NetFlow Data Export from the Main and Aggregation Caches



NetFlow Export Format Version 9

The following section provides more detailed information on NetFlow Data Export Format Version 9:

Overview of NetFlow Export Format Version 9

NetFlow exports data in UDP datagrams in Version 9 format.

Version 9 is 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.

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.

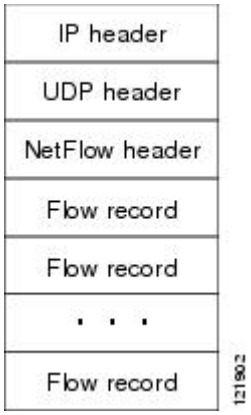
The use of templates with the NetFlow Version 9 export format provides several other key benefits:

- 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 figure below shows a typical datagram used for NetFlow fixed format export Version 7.

Figure 2: Typical Datagram for NetFlow Fixed Format Export Version 7

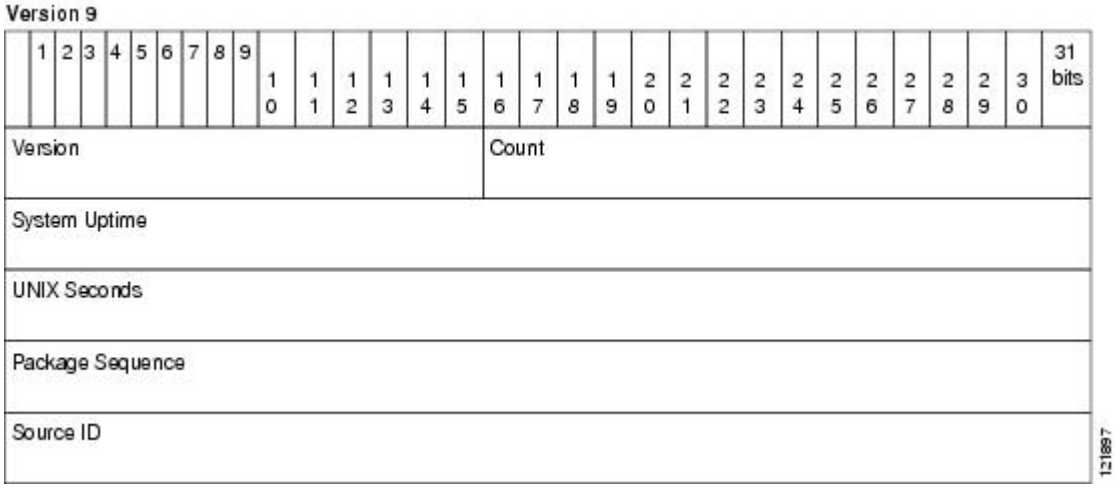


NetFlow Export Packet Header Format

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 Version 9 also includes 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 3: NetFlow Version 9 Export Packet Header Format



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

Table 1: 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.
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 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 9. (Y indicates that the field is available. N indicates that the field is not available.)

Table 2: NetFlow Flow Record Format Fields for Format Version 9

Field	Version 9
source IP address	Y
destination IP address	Y

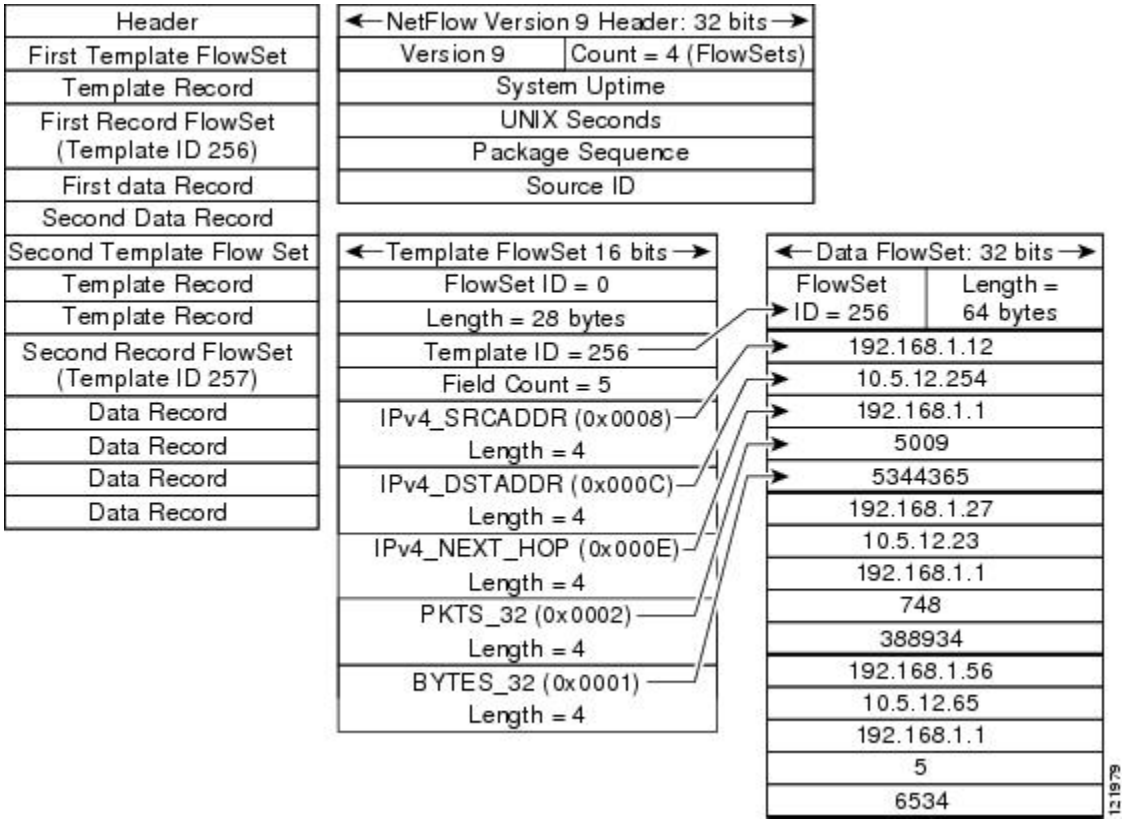
Field	Version 9
source TCP/UDP application port	Y
destination TCP/UDP application port	Y
next hop router IP address	Y
input physical interface index	Y
output physical interface index	Y
packet count for this flow	Y
byte count for this flow	Y
start of flow timestamp	Y
end of flow timestamp	Y
IP Protocol (for example, TCP=6; UDP=17)	Y
Type of Service (ToS) byte	Y
TCP Flags (cumulative OR of TCP flags)	Y
source AS number	Y
destination AS number	Y
source subnet mask	Y
destination subnet mask	Y
flags (indicates, among other things, which flows are invalid)	Y
Other flow fields[1]	Y

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

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 4: 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 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. You must 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.

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, on page 9 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, on page 9.

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.

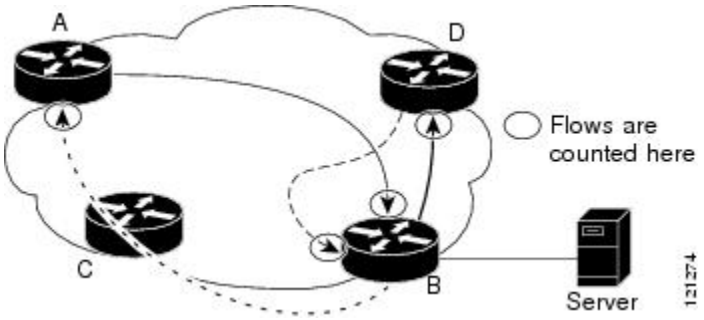
All traffic denoted by the arrows must be accounted for. The solid arrows represent IP traffic and the dotted arrows represent MPLS VPNs.

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 5: 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.

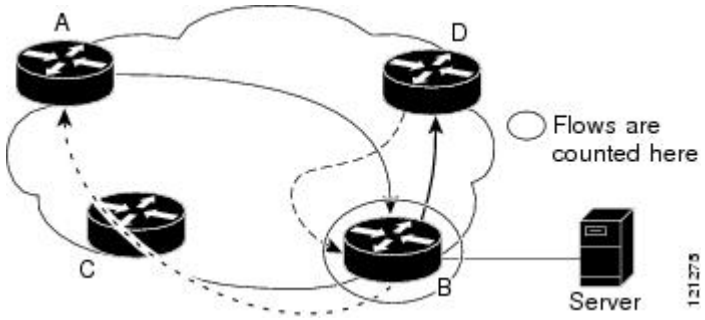
In the figure below, the following NetFlow configurations are applied to Router B:

- 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 6: 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.
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, on page 10.

	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 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

Perform the steps in this optional task to configure NetFlow Data Export using the Version 9 export format.

Note This task does not include instructions for configuring Reliable NetFlow Data Export using the Stream Control Transmission Protocol (SCTP). Refer to the NetFlow Reliable Export with SCTP module for information about and instructions for configuring Reliable NetFlow Data Export using SCTP.

Before You Begin

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 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 once to configure an additional NetFlow export destination.
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 interface-names**
8. **ip flow-export template refresh-rate** *packets*
9. **ip flow-export template timeout-rate** *minutes*
10. **i p flow-export template options export-stats**
11. **ip flow-export template options refresh-rate** *packets*
12. **ip flow-export template options timeout-rate** *minutes*
13. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**ip flow-export destination** {*ip-address* | *hostname*} *udp-port* **Example:** `Router(config)# ip flow-export destination 172.16.10.2 99`	Specifies the IP address, or hostname of the NetFlow collector, and the UDP port the NetFlow collector is listening on.
Step 4	Repeat Step 3 once to configure an additional NetFlow export destination.	(Optional) You can configure a maximum of two export destinations for NetFlow.
Step 5	**ip flow-export source** *interface-type interface-number* **Example:** `Router(config)# ip flow-export source ethernet 0/0`	(Optional) Specifies the IP address from the interface. The IP address is used as the source IP address for the UDP datagrams that are sent by NetFlow data export to the destination host.
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. • The **version 9** keyword specifies that the export packet uses the Version 9 format. • The **origin-as** keyword specifies that export statistics include the originating autonomous system for the source and destination. • The **peer-as** keyword specifies that export statistics include the peer autonomous system for the source and destination. • The **bgp-nexthop** keyword specifies that export statistics include BGP next hop-related information. **Caution** Entering this command on a Cisco 12000 series Internet router causes packet forwarding to stop for a few seconds while NetFlow reloads the RP and LC Cisco Express Forwarding tables. To avoid interruption of service to a live network, apply this command during a change window, or include it in the startup-config file to be executed during a router reboot.
Step 7	**ip flow-export interface-names** **Example:** `Router(config)# ip flow-export interface-names`	Configures NetFlow data export to include the interface names from the flows when it exports the NetFlow cache entry to a destination system.
Step 8	**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. • The **template** keyword specifies template-specific configurations. • The **refresh-rate** *packets*keyword-argument pair specifies the number of packets exported before the templates are re-sent. You can specify from 1 to 600 packets. The default is 20.

	Command or Action	Purpose
	Example:	
Step 9	**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. • The **template** keyword specifies that the **timeout-rate** keyword applies to the template. • The **timeout-rate** *minutes*keyword-argument pair specifies the time elapsed before the templates are re-sent. You can specify from 1 to 3600 minutes. The default is 30.
Step 10	**i p 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. • The **template** keyword specifies template-specific configurations. • The **options** keyword specifies template options. • The **export-stats**keyword specifies that the export statistics include the total number of flows exported and the total number of packets exported.
Step 11	**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. • The **template** keyword specifies template-specific configurations. • The **options** keyword specifies template options. • The **refresh-rate** *packets*keyword-argument pair specifies the number of packets exported before the templates are re-sent. You can specify from 1 to 600 packets. The default is 20.
Step 12	**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. • The **template** keyword specifies template-specific configurations. • The **options** keyword specifies template options. • The **timeout-rate** *minutes*keyword-argument pair specifies the time elapsed before the templates are re-sent. You can specify from 1 to 3600 minutes. The default is 30.
Step 13	**end** **Example:** `Router(config)# end`	Exits the current configuration mode and enters 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 step in this optional task.

SUMMARY STEPS

1. **show ip flow export**

DETAILED STEPS

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 Ethernet0/0
  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
```

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

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
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*	(Optional) Specifies flow cache timeout parameters.

	Command or Action	Purpose
	Example: `Router(config)# ip flow-cache timeout inactive 130`	• **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
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 as described in the Egress NetFlow Accounting Benefits NetFlow Accounting Simplified:

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

Example Configuring NetFlow Subinterface Support

NetFlow Subinterface Support For Ingress (Received) Traffic On a Subinterface

```
configure terminal
!
interface ethernet 0/0.1
 ip flow ingress
!
```

NetFlow SubInterface Support For Egress (Transmitted) Traffic On a Subinterface

```
configure terminal
!
interface ethernet 1/0.1
 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 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 NetFlow multiple export destinations:

```
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.

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

Table 3: Feature Information for Configuring NetFlow and NetFlow Data Export

Feature Name	Releases	Feature Information
Egress NetFlow Accounting	12.3(11)T 15.0(1)S	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 is entering the router. The following commands were introduced by this feature: **ip flow egress** and **ip flow-egress input-interface**. The following commands were modified by this feature: **flow-sampler**, **match**, **show ip cache flow**, **show ip cache verbose flow**, and **show ip flow interface**.
NetFlow Multiple Export Destinations	12.0(19)S 12.2(2)T 12.2(14)S 15.0(1)S	The NetFlow Multiple Export Destinations feature enables configuration of multiple destinations of the NetFlow data. The following commands were modified by this feature: **ip flow-aggregation cache**, **ip flow-export destination**, and **show ip flow export**.
NetFlow Subinterface Support	12.0(22)S 12.2(14)S 12.2(15)T 12.2(33)SB	The NetFlow Subinterface Support feature provides the ability to enable NetFlow on a per-subinterface basis. The following command was introduced by this feature: **ip flow ingress.** The following command was modified by this feature: **show ip interface**.

Feature Name	Releases	Feature Information
NetFlow v9 Export Format	12.0(24)S 12.2(18)S 12.2(27)SBC 12.2(18)SXF 12.3(1) 15.0(1)S	The NetFlow v9 Export Format, which is flexible and extensible, provides the versatility needed to support new fields and record types. This format accommodates new NetFlow-supported technologies such as Multicast, MPLS, NAT, and BGP next hop. The following commands were modified by this feature: **debug ip flow export**, **export**, **ip flow-export**, and **show ip flow export**.
Support for interface names added to NetFlow data export[2]	12.4(2)T	The **interface-names** keyword for the **ip flow-export** command configures NetFlow data export to include the interface names from the flows when it exports the NetFlow cache entry to a destination system.

2 This is a minor enhancement. Minor enhancements are not typically listed in Feature Navigator.

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.