Configuring NetFlow and NetFlow Data Export

First Published: June 19, 2006
Last Updated: January 21, 2011

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 application that provides statistics on packets flowing through the router. NetFlow is 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 for Configuring NetFlow and NetFlow Data Export” section on page 36.

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

Contents

- Prerequisites for Configuring NetFlow and NetFlow Data Export, page 2
- Restrictions for Configuring NetFlow and NetFlow Data Export, page 2
- Information About Configuring NetFlow and NetFlow Data Export, page 3
- How to Configure NetFlow and NetFlow Data Export, page 20
- Configuration Examples for Configuring NetFlow and NetFlow Data Export, page 31
- Additional References, page 34
- Feature Information for Configuring NetFlow and NetFlow Data Export, page 36
Prerequisites for Configuring NetFlow and NetFlow Data Export

Before you enable NetFlow, you must do the following:

- 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, distributed Cisco Express Forwarding, 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

NetFlow Data Capture

NetFlow consumes a significant amount of memory. If you have memory constraints, you might want to preset the size of the NetFlow cache so that it contains a lower number of entries. The default cache size depends on the platform. For example, the default cache size for the Cisco 7500 router is 65,536 (64K) entries.

**Memory Impact**

During times of heavy traffic, additional flows can fill up the global flow hash table. If you need to increase the size of the global flow hash table, increase the memory of the router.

**Cisco IOS Releases 12.2(14)S, 12.0(22)S, or 12.2(15)T**

If your router is running a version of Cisco IOS prior to releases 12.2(14)S, 12.0(22)S, or 12.2(15)T, the `ip route-cache flow` command is used to enable NetFlow on an interface.

If your router is running Cisco IOS Release 12.2(14)S, 12.0(22)S, 12.2(15)T, or a later release, use the `ip flow ingress` command to enable NetFlow on an interface.

**Cisco IOS Releases 12.4(20)T or Earlier Releases**

The `ip flow ingress` command behavior depends on the Cisco IOS release:

If your router is running a version earlier than Cisco IOS Release 12.4(20)T, and your router does not have a VPN Service Adapter (VSA)-enabled interface, enabling the `ip flow ingress` command will result in the ingress traffic being accounted for twice by the router.

If your router is running a version earlier than Cisco IOS Release 12.4(20)T, and your router has a VSA-enabled interface, enabling the `ip flow ingress` command will result in the encrypted ingress traffic being accounted for only once.

If your router is running a version of Cisco IOS Release 12.4(20)T or later, enabling the `ip flow ingress` command will result in the encrypted ingress traffic being accounted for only once.
Egress NetFlow Accounting in Cisco IOS 12.3T Releases, 12.3(11)T, or Later Releases

The Egress NetFlow Accounting feature captures NetFlow statistics for IP traffic only. Multiprotocol Label Switching (MPLS) statistics are not captured. The MPLS Egress NetFlow Accounting feature can be used on a provider edge (PE) router to capture IP traffic flow information for egress IP packets that arrive at the router as MPLS packets and undergo 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
In Cisco IOS 12.2S releases, egress NetFlow captures either IPv4 or MPLS packets as they leave the router.

NetFlow Data Export

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—The export bandwidth use increases for Version 9 (because of template flowsets) when compared to Version 5. The increase in bandwidth usage varies with the frequency with which template flowsets are sent. The default is to resend templates every 20 packets; this has a bandwidth cost of about 4 percent. If required, you can lower the resend rate with the ip flow-export template refresh-rate packets command.
- Performance impact—Version 9 slightly decreases the overall performance because generating and maintaining valid template flowsets requires additional processing.

Restrictions for NetFlow Version 8 Export Format

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

Restrictions for NetFlow Version 1 Export Format

The Version 1 format was the initially released version. Do not use the Version 1 format unless you are using a legacy collection system that requires it. Use Version 9 or Version 5 export format.

Information About Configuring NetFlow and NetFlow Data Export

- NetFlow Data Capture, page 4
- NetFlow Flows: Key Fields, page 4
- NetFlow Cache Management and Data Export, page 4
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 features:

- 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 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 flow. 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 efficient, with the amount of export data being about 1.5 percent of the switched traffic in the router. NetFlow accounts for every packet (nonsampled mode) and provides a highly condensed and detailed view of all network traffic that enters 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 whether a packet is part of an existing flow or whether the packet requires 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 or flow expiration.

The rules for expiring NetFlow cache entries include the following:

- Flows that 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 for 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.
- TCP connections that have reached the end of the byte stream (FIN) or have been reset (RST) are expired.

Expired flows are grouped into “NetFlow export” datagrams for export from the NetFlow-enabled device. NetFlow export datagrams can consist of up to 30 flow records for Version 5 or Version 9 flow export. 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. Figure 1 shows an example of NetFlow data export from the main and aggregation caches to a collector.
Overview

NetFlow exports data in UDP datagrams in one of the following formats: Version 9, Version 8, Version 7, Version 5, or Version 1:

- Version 9—A flexible and extensible format, which provides the versatility needed for support of new fields and record types. This format accommodates new NetFlow-supported technologies such as Multicast, MPLS, and Border Gateway Protocol (BGP) next hop. The Version 9 export format enables you to use the same version for main and aggregation caches, and the format is extensible, 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 BGP-AS information and flow sequence numbers. (Versions 2 through 4 were not released.) This is the most commonly used format.
- Version 1—The initially released export format that is rarely used today. Do not use the Version 1 export format unless the legacy collection system that you are using requires it. Use either the Version 9 export format or the Version 5 export format.

Details

The following sections provide more detailed information on NetFlow Data Export Formats:

- NetFlow Export Version Formats, page 7
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 sequence number, record count, and system uptime. The flow record contains flow information such as 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, and IP Version 6 (IPv6), IP Version 4 (IPv4), Multicast, and MPLS information. This new information allows new applications of export data and provides new views of 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.
- Netflow is “future proofed” because the Version 9 export format can be adapted to provide support for new and developing protocols and other non-NetFlow-based approaches to data collection.

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 1 export format was the original format supported in the initial Cisco IOS software releases containing the NetFlow functionality; it is rarely used today. The Version 5 export format is an enhancement that adds BGP autonomous system information and flow sequence numbers. Versions 2 through 4 and Version 6 export formats were either not released or not supported. The Version 8 export format is the NetFlow export format to use when you enable router-based NetFlow aggregation on Cisco IOS router platforms.
Figure 2 shows a typical datagram used for NetFlow fixed format export Versions 1, 5, 7, and 8.

### NetFlow Export Packet Header Format

In all the 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.

Table 1 lists the NetFlow Version 9 export packet header field names and descriptions.
Configuring NetFlow and NetFlow Data Export

Information About Configuring NetFlow and NetFlow Data Export

NetFlow Flow Record and Export Format Content Information

This section gives details about the Cisco export format flow record. Table 2 indicates which flow record format fields are available for Versions 5 and 9. (*Yes* indicates that the field is available. *No* indicates that the field is not available.)

### Table 1
**NetFlow Version 9 Export Packet Header Field Names and Descriptions**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>The version of NetFlow records exported in this packet; for Version 9, this value is 0x0009.</td>
</tr>
<tr>
<td>Count</td>
<td>Number of FlowSet records (both template and data) contained within this packet.</td>
</tr>
<tr>
<td>System Uptime</td>
<td>Time in milliseconds since this device was first booted.</td>
</tr>
<tr>
<td>UNIX Seconds</td>
<td>Seconds since 0000 Coordinated Universal Time (UTC) 1970.</td>
</tr>
<tr>
<td>Package Sequence</td>
<td>Incremental sequence counter of all export packets sent by this export device; this value is cumulative, and it can be used to learn 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.”</td>
</tr>
<tr>
<td>Source ID</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Table 2
**NetFlow Flow Record Format Fields for Format Versions 5, and 9**

<table>
<thead>
<tr>
<th>Field</th>
<th>Version 5</th>
<th>Version 9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP address</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Destination IP address</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Source TCP/UDP application port</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Destination TCP/UDP application port</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Next hop router IP address</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Input physical interface index</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Output physical interface index</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Packet count for this flow</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Byte count for this flow</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Start of flow timestamp</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>End of flow timestamp</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
**Table 2  NetFlow Flow Record Format Fields for Format Versions 5, and 9 (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Version 5</th>
<th>Version 9</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Protocol (for example, TCP=6; UDP=17)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Type of Service (ToS) byte</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>TCP Flags (cumulative OR of TCP flags)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Source AS number</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Destination AS number</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Source subnet mask</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Destination subnet mask</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Flags (indicates, among other things, which flows are invalid)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Other flow fields$^1$</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

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

**Figure 4  NetFlow Version 5 Export Record Format**

- **Usage**
  - Packet count
  - Byte count
  - Source IP address
  - Destination IP address

- **Time**
  - Start sysUpTime
  - End sysUpTime
  - Source TCP/UDP port
  - Destination TCP/UDP port

- **Port utilization**
  - Input ifIndex
  - Output ifIndex

- **QoS**
  - Type of Service
  - TCP flags
  - Protocol
  - Next hop address
  - Source AS number
  - Dest. AS number
  - Source prefix mask
  - Dest. prefix mask

**Table 3  NetFlow Version 5 Export Record Format Field Names and Descriptions**

<table>
<thead>
<tr>
<th>Content</th>
<th>Bytes</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>srcaddr</td>
<td>0–3</td>
<td>Source IP address</td>
</tr>
<tr>
<td>dstaddr</td>
<td>4–7</td>
<td>Destination IP address</td>
</tr>
<tr>
<td>nexthop</td>
<td>8–11</td>
<td>Next hop router’s IP address</td>
</tr>
<tr>
<td>input</td>
<td>12–13</td>
<td>Ingress interface Simple Network Management Protocol (SNMP) ifIndex</td>
</tr>
<tr>
<td>output</td>
<td>14–15</td>
<td>Egress interface SNMP ifIndex</td>
</tr>
<tr>
<td>dPks</td>
<td>16–19</td>
<td>Packets in the flow</td>
</tr>
<tr>
<td>dOctets</td>
<td>20–23</td>
<td>Octets (bytes) in the flow</td>
</tr>
</tbody>
</table>
Table 3  NetFlow Version 5 Export Record Format Field Names and Descriptions (continued)

<table>
<thead>
<tr>
<th>Content</th>
<th>Bytes</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>first</td>
<td>24–27</td>
<td>SysUptime at start of the flow</td>
</tr>
<tr>
<td>last</td>
<td>28–31</td>
<td>SysUptime at the time the last packet of the flow was received</td>
</tr>
<tr>
<td>srcport</td>
<td>32–33</td>
<td>Layer 4 source port number or equivalent</td>
</tr>
<tr>
<td>dstport</td>
<td>34–35</td>
<td>Layer 4 destination port number or equivalent</td>
</tr>
<tr>
<td>pad1</td>
<td>36</td>
<td>Unused (zero) byte</td>
</tr>
<tr>
<td>tcp_flags</td>
<td>37</td>
<td>Cumulative OR of TCP flags</td>
</tr>
<tr>
<td>prot</td>
<td>38</td>
<td>Layer 4 protocol (for example, 6=TCP, 17=UDP)</td>
</tr>
<tr>
<td>tos</td>
<td>39</td>
<td>IP type-of-service byte</td>
</tr>
<tr>
<td>src_as</td>
<td>40–41</td>
<td>Autonomous system number of the source, either origin or peer</td>
</tr>
<tr>
<td>dst_as</td>
<td>42–43</td>
<td>Autonomous system number of the destination, either origin or peer</td>
</tr>
<tr>
<td>src_mask</td>
<td>44</td>
<td>Source address prefix mask bits</td>
</tr>
<tr>
<td>dst_mask</td>
<td>45</td>
<td>Destination address prefix mask bits</td>
</tr>
<tr>
<td>pad2</td>
<td>46–47</td>
<td>PAD2 is unused (zero) bytes</td>
</tr>
</tbody>
</table>

Figure 5 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 in Version 9 and export format architecture is available in the NetFlow Version 9 Flow-Record Format document.
Figure 5  NetFlow Version 9 Export Packet Example

<table>
<thead>
<tr>
<th>Header</th>
<th>NetFlow Version 9 Header: 32 bits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Version 9 Count = 4 (FlowSets)</td>
</tr>
<tr>
<td>First Template FlowSet</td>
<td>System Uptime</td>
</tr>
<tr>
<td>Template Record</td>
<td>UNIX Seconds</td>
</tr>
<tr>
<td>First Record FlowSet (Template ID 256)</td>
<td>Package Sequence</td>
</tr>
<tr>
<td>First data Record</td>
<td>Source ID</td>
</tr>
<tr>
<td>Second Data Record</td>
<td></td>
</tr>
<tr>
<td>Second Template Flow Set</td>
<td></td>
</tr>
<tr>
<td>Template Record</td>
<td></td>
</tr>
<tr>
<td>Template Record</td>
<td></td>
</tr>
<tr>
<td>Second Record FlowSet (Template ID 257)</td>
<td></td>
</tr>
<tr>
<td>Data Record</td>
<td></td>
</tr>
<tr>
<td>Data Record</td>
<td></td>
</tr>
<tr>
<td>Data Record</td>
<td></td>
</tr>
<tr>
<td>Data Record</td>
<td></td>
</tr>
<tr>
<td>Data Record</td>
<td></td>
</tr>
</tbody>
</table>

For all export versions, you can specify a destination where NetFlow data export packets are sent, such as the workstation running NetFlow Collection Engine, when the number of recently expired flows reaches a predetermined maximum, or every second—whichever occurs first. For a Version 1 datagram, up to 24 flows can be sent in a single UDP datagram of approximately 1200 bytes; 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 Versions 1, 7, and 9 and platform-specific information when applicable, see Appendix 2 in the NetFlow Services Solutions Guide.

**NetFlow Data Export Format Selection**

NetFlow exports data in UDP datagrams in export format Version 9, 8, 5, or 1. Table 4 describes situations when you might select a particular NetFlow export format.
NetFlow Version 9 Data Export Format

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


Using Version 9 export, you can define new formats on the router and send these formats to the NetFlow Collection Engine (formerly called NetFlow FlowCollector) at set intervals. You can 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 Version 9 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 protocol (UDP, TCP, SCTP, and so on).

<table>
<thead>
<tr>
<th>Table 4</th>
<th>When to Select a Particular NetFlow Export Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export Format</td>
<td>Select When…</td>
</tr>
</tbody>
</table>
| Version 9 | You need to export data from various technologies, such as Multicast, DoS, IPv6, and BGP next hop. This format accommodates new NetFlow-supported technologies such as Multicast, MPLS, and BGP next hop.  
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.  
Version 5 export format does not support export from aggregation caches. |
| Version 1 | You need to export data to a legacy collection system that requires Version 1 export format. Otherwise, do not use Version 1 export format. Use Version 9 or Version 5 export format. |
NetFlow Version 9 Template-Based Flow Record Format

The main feature of NetFlow Version 9 export format is that it is template based. A template describes a NetFlow record format and attributes of 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 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. See 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 Figure 5.

NetFlow Export Templates

NetFlow implements a variety of templates, each exporting a different set of fields for a specific purpose. For example, the MPLS templates are different from the Optimized Edge Routing (OER) templates and the various option templates.

Table 5 lists the export templates and the specific set of fields the export pertains to.

<table>
<thead>
<tr>
<th>Number of Export Templates</th>
<th>Exports Fields Pertaining to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IPv4 main cache</td>
</tr>
<tr>
<td>8</td>
<td>MPLS labels 0 to 3</td>
</tr>
<tr>
<td>21</td>
<td>Aggregation caches with or without BGP subflows</td>
</tr>
<tr>
<td>3</td>
<td>BGP, BGP Next Hop (NH), and Multicast</td>
</tr>
<tr>
<td>4</td>
<td>OER</td>
</tr>
<tr>
<td>2</td>
<td>MAC and auxiliary information</td>
</tr>
<tr>
<td>11</td>
<td>Random sampler information, interface names, sampling option, and exporter status options</td>
</tr>
</tbody>
</table>
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 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 Cisco IOS Release 12.0(3)T for 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 introduced in Cisco IOS 12.0(15)S and integrated into Cisco IOS Releases 12.2(4)T and 12.2(14)S. Refer to the “Configuring NetFlow Aggregation Caches” module for information on 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.

Figure 6 displays the NetFlow Version 8 export packet header format.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Flow export format version number. In this case 8.</td>
</tr>
<tr>
<td>Count</td>
<td>Number of export records in the datagram.</td>
</tr>
<tr>
<td>System Uptime</td>
<td>Number of milliseconds since the router last booted.</td>
</tr>
<tr>
<td>UNIX Seconds</td>
<td>Number of seconds since 0000 UTC 1970.</td>
</tr>
<tr>
<td>UNIX NanoSeconds</td>
<td>Number of residual nanoseconds since 0000 UTC 1970.</td>
</tr>
<tr>
<td>Flow Sequence Number</td>
<td>Sequence counter of total flows sent for this export stream.</td>
</tr>
<tr>
<td>Engine Type</td>
<td>The type of switching engine. RP = 0 and LC = 1.</td>
</tr>
</tbody>
</table>

Table 6 lists the NetFlow Version 8 export packet header field names and definitions.
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 the Version 5 export format are in network byte order. Figure 7 shows the NetFlow Version 5 export packet header format.

Table 6  NetFlow Version 8 Export Packet Header Field Names and Descriptions (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engine ID</td>
<td>Slot number of the NetFlow engine.</td>
</tr>
<tr>
<td>Aggregation</td>
<td>Type of aggregation scheme being used.</td>
</tr>
<tr>
<td>Agg Version</td>
<td>Aggregation subformat version number. The current value is 2.</td>
</tr>
<tr>
<td>Sampling Interval</td>
<td>Interval value used if Sampled NetFlow is configured.</td>
</tr>
<tr>
<td>Reserved</td>
<td>Reserved.</td>
</tr>
</tbody>
</table>

Table 7 lists the NetFlow Version 5 export packet header field names and descriptions.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bytes Field</td>
<td>Description</td>
</tr>
<tr>
<td>0 to 1</td>
<td>Version</td>
</tr>
<tr>
<td>2 to 3</td>
<td>Count</td>
</tr>
</tbody>
</table>
NetFlow Version 1 Data Export Format

The NetFlow Version 1 data export format was the format supported in the initial Cisco IOS software releases containing the NetFlow functionality. It is rarely used today. Do not use the Version 1 export format unless the legacy collection system you are using requires it. Use either the Version 9 export format or the Version 5 export format.

Figure 8 shows the NetFlow Version 1 export packet header format.

Table 7: NetFlow Version 5 Export Packet Header Field Names and Descriptions (continued)

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

Table 8 lists the NetFlow Version 1 export packet header field names and descriptions.

Table 8: NetFlow Version 1 Packet Header Field Names and Descriptions

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Flow export format version number. In this case 1.</td>
</tr>
<tr>
<td>Count</td>
<td>Number of export records in the datagram.</td>
</tr>
<tr>
<td>System Uptime</td>
<td>Number of milliseconds since the router last booted.</td>
</tr>
<tr>
<td>UNIX Seconds</td>
<td>Number of seconds since 0000 UTC 1970.</td>
</tr>
<tr>
<td>UNIX NanoSeconds</td>
<td>Number of residual nanoseconds since 0000 UTC 1970.</td>
</tr>
</tbody>
</table>
Egress NetFlow Accounting Benefits: NetFlow Accounting Simplified

The Egress NetFlow Accounting feature can simplify the NetFlow configuration. The following example shows how.

In Figure 9 and Figure 10, 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.

Figure 9 shows how the flow traffic was tracked before the introduction of the Egress NetFlow Accounting feature. Figure 10 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 facilitates collection and tracking of 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 9 Ingress-Only NetFlow Example

A configuration such as the one used in Figure 9 requires that NetFlow statistics from three separate routers be added to obtain the flow statistics for the server.

In comparison, the example in Figure 10 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 Figure 10, 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 on 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 using the `show ip cache flow` command or the `show ip cache verbose flow` command for Router B.

**Figure 10  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, you can collect export records from just a few of them. 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.

**NetFlow on a Distributed VIP Interface**

On a Cisco 7500 series router with a Route Switch Processor (RSP) and with VIP controllers, the VIP hardware can be configured to switch packets received by the VIP interfaces with no per-packet intervention on the part of the RSP. This process is called distributed switching. When VIP distributed switching is enabled, the input VIP interface switches IP packets instead of forwarding them to the RSP for switching. Distributed switching decreases the demand on the RSP. VIP interfaces with distributed switching enabled can be configured for NetFlow.
How to Configure NetFlow and NetFlow Data Export

This section contains instructions for configuring NetFlow to capture and export network traffic data. Perform the following tasks to configure NetFlow to capture and export network traffic data:

- Configuring NetFlow, page 20 (required)
- Verifying that NetFlow Is Operational and Displaying NetFlow Statistics, page 21 (optional)
- Configuring NetFlow Data Export Using the Version 9 Export Format, page 23 (optional)
- Verifying that NetFlow Data Export Is Operational, page 26 (optional)
- Clearing NetFlow Statistics on the Router, page 27 (optional)
- Customizing the NetFlow Main Cache Parameters, page 28 (optional)

Configuring NetFlow

Perform the following task to enable NetFlow on an interface.

SUMMARY STEPS

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

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 interface type number</td>
<td>Specifies the interface that you want to enable NetFlow on and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface ethernet 0/0</td>
<td></td>
</tr>
</tbody>
</table>
Verifying that NetFlow Is Operational and Displaying NetFlow Statistics

Perform the following task to verify that NetFlow is operational and to display NetFlow statistics.

SUMMARY STEPS

1. show ip flow interface
2. show ip cache flow
3. show ip cache verbose flow

DETAILED STEPS

Step 1 show ip flow interface
Use this command to display the NetFlow configuration for an interface. The following is sample output from this command:

Router# show ip flow interface

Ethernet0/0
  ip flow ingress
Router#

Step 2 show ip cache flow
Use this command to verify that NetFlow is operational and to display a summary of NetFlow statistics. The following is sample output from this command:

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
Configuring NetFlow and NetFlow Data Export

Step 3  show ip cache verbose flow

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

Router# show ip cache verbose flow

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 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
35 active, 4061 inactive, 980 added
2992518 ager polls, 0 flow alloc failures
### 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.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Total Flows</th>
<th>Packets / Sec</th>
<th>Packets / Flow</th>
<th>Bytes / Sec</th>
<th>Packets Active / Sec</th>
<th>Idle / Sec</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP-FTP</td>
<td>108</td>
<td>0.0</td>
<td>1133</td>
<td>40</td>
<td>2.4</td>
<td>1799.6</td>
</tr>
<tr>
<td>TCP-FTPD</td>
<td>108</td>
<td>0.0</td>
<td>1133</td>
<td>40</td>
<td>2.4</td>
<td>1799.6</td>
</tr>
<tr>
<td>TCP-WWW</td>
<td>54</td>
<td>0.0</td>
<td>1133</td>
<td>40</td>
<td>1.2</td>
<td>1799.6</td>
</tr>
<tr>
<td>TCP-SMTP</td>
<td>54</td>
<td>0.0</td>
<td>1133</td>
<td>40</td>
<td>1.2</td>
<td>1799.6</td>
</tr>
<tr>
<td>TCP-BGP</td>
<td>27</td>
<td>0.0</td>
<td>1133</td>
<td>40</td>
<td>0.6</td>
<td>1799.6</td>
</tr>
<tr>
<td>TCP-NNTP</td>
<td>27</td>
<td>0.0</td>
<td>1133</td>
<td>40</td>
<td>0.6</td>
<td>1799.6</td>
</tr>
<tr>
<td>TCP-other</td>
<td>297</td>
<td>0.0</td>
<td>1133</td>
<td>40</td>
<td>6.6</td>
<td>1799.7</td>
</tr>
<tr>
<td>UDP-TFTP</td>
<td>27</td>
<td>0.0</td>
<td>1133</td>
<td>28</td>
<td>3.0</td>
<td>1799.6</td>
</tr>
<tr>
<td>UDP-other</td>
<td>108</td>
<td>0.0</td>
<td>1417</td>
<td>28</td>
<td>3.0</td>
<td>1799.6</td>
</tr>
<tr>
<td>ICMP</td>
<td>135</td>
<td>0.0</td>
<td>1133</td>
<td>427</td>
<td>3.0</td>
<td>1799.6</td>
</tr>
</tbody>
</table>

**Total:**

|          | 945         | 0.0           | 1166           | 91          | 21.9                 | 1799.6     | 0.8        |
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.

Prerequisites

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” section on page 20 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 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. ip 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip flow-export destination (ip-address</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# ip flow-export destination 172.16.10.2 99</td>
</tr>
<tr>
<td></td>
<td>Specifies the IP address, or hostname of the NetFlow collector, and the UDP port the NetFlow collector is listening on.</td>
</tr>
</tbody>
</table>
### Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Repeat Step 3 once to configure an additional NetFlow export destination.</td>
<td>(Optional) You can configure a maximum of two export destinations for NetFlow.</td>
</tr>
<tr>
<td>5</td>
<td><code>ip flow-export source interface-type interface-number</code></td>
<td>(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.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Router(config)# <code>ip flow-export source ethernet 0/0</code></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>`ip flow-export version 9 [origin-as</td>
<td>peer-as] [bgp-nexthop]`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Router(config)# <code>ip flow-export version 9</code></td>
<td>- The <strong>version 9</strong> keyword specifies that the export packet uses the Version 9 format.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Router(config)# <code>ip flow-export version 9</code></td>
<td>- The <strong>origin-as</strong> keyword specifies that export statistics include the originating autonomous system for the source and destination.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Router(config)# <code>ip flow-export version 9</code></td>
<td>- The <strong>peer-as</strong> keyword specifies that export statistics include the peer autonomous system for the source and destination.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Router(config)# <code>ip flow-export version 9</code></td>
<td>- The <strong>bgp-nexthop</strong> keyword specifies that export statistics include BGP next hop-related information.</td>
</tr>
<tr>
<td></td>
<td><strong>Caution</strong></td>
<td>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.</td>
</tr>
<tr>
<td>7</td>
<td><code>ip flow-export interface-names</code></td>
<td>Configures NetFlow data export to include the interface names from the flows when it exports the NetFlow cache entry to a destination system.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Router(config)# <code>ip flow-export interface-names</code></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td><code>ip flow-export template refresh-rate packets</code></td>
<td>(Optional) Enables the export of information in NetFlow cache entries.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Router(config)# <code>ip flow-export template refresh-rate 15</code></td>
<td>- The <strong>template</strong> keyword specifies template-specific configurations.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Router(config)# <code>ip flow-export template refresh-rate 15</code></td>
<td>- The <strong>refresh-rate packets</strong> 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.</td>
</tr>
</tbody>
</table>
### Command Purpose

**Step 9**

**Command:**
```
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**

**Command:**
```
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.

- 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**

**Command:**
```
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**

**Command:**
```
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**

**Command:**
```
end
```

**Example:**
```
Router(config)# end
```

Exits the current configuration mode and enters privileged EXEC mode.

---

**Verifying that NetFlow Data Export Is Operational**

Perform the steps in this optional task to verify that NetFlow data export is operational and to display the statistics for NetFlow data export.

**SUMMARY STEPS**

1. `show ip flow export`
2. show ip flow export template

DETAILED STEPS

Step 1 show ip flow export

Use this command to display 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:

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
Router#

Step 2 show ip flow export template

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

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#

Clearing NetFlow Statistics on the Router

Perform the steps in this optional task to clear NetFlow statistics on the router.

SUMMARY STEPS

1. enable
2. clear ip flow stats

DETAILED STEPS

**Step 1** enable

Use this command to enter privileged EXEC mode on the router:

```
Router> enable
Router#
```

**Step 2** clear ip flow stats

Use this command to clear the NetFlow statistics on the router. For example:

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

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 the IP address, interface, application, and ToS.

To customize the parameters for the main NetFlow cache, perform the steps in this optional task.

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:

- Flow transport is completed (TCP connections that have reached the end of the byte stream [FIN] or that have been reset [RST] are expired).
- The flow cache has become full.
- A flow becomes inactive. By default, a flow that is 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 from 10 to 600 seconds. You can configure the time interval for the active timer from 1 to 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), Cisco recommends a larger value such as 131072 (128K). To obtain information on your flow traffic, use the `show ip cache flow` command.

A NetFlow cache can be resized depending on the platform and the amount of DRAM on a line card. For example, the NetFlow cache size is configurable for software-based platforms such as Cisco 75xx and 72xx series routers. The amount of memory on a Cisco 12000 line card determines how many flows are possible in the cache.

Using the `ip flow-cache entries` command, configure the size of your NetFlow cache from 1024 entries to 524,288 entries. Use the `cache entries` command (after you configure NetFlow aggregation) to configure the size of the NetFlow aggregation cache from 1024 entries to 524,288 entries.

**Caution**

Cisco recommends 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.

**Restrictions**

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 type number`
4. `no ip flow {ingress | egress}`
5. `exit`
6. Repeat Steps 3 through 5 for every interface that has NetFlow enabled on it.
7. `ip flow-cache entries number`
8. `ip flow-cache timeout active minutes`
9. `ip flow-cache timeout inactive seconds`
10. `interface type number`
11. `ip flow {ingress | egress}`
12. `exit`
13. Repeat Steps 10 through 12 for every interface that previously had NetFlow enabled on it.
14. `end`
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type number</td>
<td>(Required if NetFlow is already enabled on the interface) Specifies the interface that you want to disable NetFlow on and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface ethernet 0/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> no ip flow (ingress</td>
<td>(Required if NetFlow is enabled on the interface) Disables NetFlow on the interface.</td>
</tr>
<tr>
<td>egress)</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# no ip flow ingress</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>ingress</strong>—Captures traffic that is being received by the interface</td>
</tr>
<tr>
<td></td>
<td>- <strong>egress</strong>—Captures traffic that is being transmitted by the interface</td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>(Optional) Exits interface configuration mode and returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# config-if)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You only need to use this command if you need to disable NetFlow on another interface.</td>
</tr>
<tr>
<td><strong>Step 6</strong> Repeat Steps 3 through 5 for every interface that has NetFlow enabled on it.</td>
<td>This step is required if NetFlow is enabled on any other interfaces. —</td>
</tr>
<tr>
<td><strong>Step 7</strong> ip flow-cache entries number</td>
<td>(Optional) Changes the number of entries maintained in the NetFlow cache.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# ip flow-cache entries 131072</td>
<td>The number argument is the number of entries to be maintained. The valid range is from 1024 to 524288 entries. The default is 65536 (64K).</td>
</tr>
<tr>
<td><strong>Step 8</strong> ip flow-cache timeout active minutes</td>
<td>(Optional) Specifies flow cache timeout parameters.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# ip flow-cache timeout active 20</td>
<td>The active keyword specifies the active flow timeout.</td>
</tr>
<tr>
<td></td>
<td>- The minutes argument 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.</td>
</tr>
<tr>
<td><strong>Step 9</strong> ip flow-cache timeout inactive seconds</td>
<td>(Optional) Specifies flow cache timeout parameters.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# ip flow-cache timeout inactive 130</td>
<td>The inactive keyword specifies the inactive flow timeout.</td>
</tr>
<tr>
<td></td>
<td>- The seconds argument 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.</td>
</tr>
</tbody>
</table>
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” section on page 18:

```
configure terminal
!
interface ethernet 0/0
  ip flow egress
!
```
Example: Configuring NetFlow Subinterface Support

The following examples show how to configure NetFlow Subinterface Support as described in the “NetFlow Subinterface Support Benefits: Fine-Tuning Your Data Collection” section on page 19:

- NetFlow Subinterface Support for Ingress (Received) Traffic on a Subinterface, page 32
- NetFlow SubInterface Support for Egress (Transmitted) Traffic on a Subinterface, page 32

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

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

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

```plaintext
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: Configuring NetFlow Multiple Export Destinations

The following example shows how to configure the NetFlow Multiple Export Destinations feature as described in the “NetFlow Multiple Export Destinations: Benefits” section on page 19:

```plaintext
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 autonomous system information:

```plaintext
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#
```

Example: Configuring NetFlow Version 1 Data Export

The following example shows how to configure the NetFlow data export using the Version 5 export format with the peer autonomous system information:

```plaintext
configure terminal
!
ip flow-export destination 172.16.10.2 99
exit

Router# show ip flow export

Flow export v1 is enabled for main cache
   Exporting flows to 172.16.10.2 (99)
   Exporting using source IP address 172.16.6.1
   Version 1 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#
```

Note

No autonomous system number or BGP next hop information is exported with the Version 1 export format.
## Additional References

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td><em>Cisco IOS Master Commands List, All Releases</em></td>
</tr>
<tr>
<td>NetFlow Commands</td>
<td><em>Cisco IOS NetFlow Command Reference</em></td>
</tr>
<tr>
<td>NetFlow Services Solutions Guide</td>
<td><em>NetFlow Services Solutions Guide</em></td>
</tr>
<tr>
<td>NetFlow Reliable Export With SCTP</td>
<td><em>NetFlow Reliable Export With SCTP</em></td>
</tr>
</tbody>
</table>
## Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>

## MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

## RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>

## Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
Feature Information for Configuring NetFlow and NetFlow Data Export

Table 9 lists the features in this module and provides links to specific configuration information. Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note

Table 9 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.

Table 9  Feature Information for Configuring NetFlow and NetFlow Data Export

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egress NetFlow Accounting</td>
<td>12.3(11)T</td>
<td>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 sections provide information about this feature:</td>
</tr>
<tr>
<td></td>
<td>15.0(1)S</td>
<td>• Egress NetFlow Accounting Benefits: NetFlow Accounting Simplified</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Example: Configuring Egress NetFlow Accounting</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>NetFlow Multiple Export</td>
<td>12.0(19)S</td>
<td>The NetFlow Multiple Export Destinations feature enables configuration of multiple destinations of the NetFlow data. The following sections provide information about this feature:</td>
</tr>
<tr>
<td>Destinations</td>
<td>12.2(2)T</td>
<td>• NetFlow Multiple Export Destinations: Benefits, page 19</td>
</tr>
<tr>
<td></td>
<td>12.2(14)S</td>
<td>• Example: Configuring NetFlow Multiple Export Destinations, page 32</td>
</tr>
<tr>
<td></td>
<td>15.0(1)S</td>
<td>The following commands were modified by this feature: ip flow-aggregation cache, ip flow-export destination, and show ip flow export.</td>
</tr>
</tbody>
</table>
### Table 9  Feature Information for Configuring NetFlow and NetFlow Data Export (continued)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| 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 sections provide information about this feature:  
  - NetFlow Subinterface Support Benefits: Fine-Tuning Your Data Collection, page 19  
  - Example: Configuring NetFlow Subinterface Support, page 32  
  The following command was introduced by this feature: *ip flow ingress*.  
  The following command was modified by this feature: *show ip interface*. |
| 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 sections provide information about this feature:  
  - NetFlow Export Format Versions 9, 8, 5, and 1, page 6  
  - Configuring NetFlow Data Export Using the Version 9 Export Format, page 23  
  The following commands were modified by this feature: *debug ip flow export, export, ip flow-export, show ip flow export*. |
| Support for interface names added to NetFlow data export\(^1\) | 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. |

\(^1\) This is a minor enhancement. Minor enhancements are not typically listed in Feature Navigator.
Glossary

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—A 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.

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

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

fast switching—A 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 with 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.

MPLS—Multiprotocol Label Switching. An industry standard for the forwarding of packets along a normally routed path (sometimes called MPLS hop-by-hop forwarding).

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

NetFlow Aggregation—A NetFlow feature that lets you summarize NetFlow export data on a 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 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.


RP—Route Processor. A processor module in the Cisco 7000 series routers that contains the CPU, system software, and most of the memory components that are used in the router. It is sometimes called a Supervisory Processor.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco’s trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)