Configuring Cisco IOS Flexible NetFlow with Predefined Records

Last Updated: November 7, 2011

This module contains information about and instructions for configuring Flexible NetFlow using predefined records. Many of the Flexible NetFlow predefined records use the same key and nonkey fields as the aggregation caches available in original NetFlow. However, the predefined Flexible NetFlow records do not perform aggregation.

NetFlow is a Cisco IOS technology that provides statistics on packets flowing through a router. NetFlow is the standard for acquiring IP operational data from IP networks. NetFlow provides data to support network and security monitoring, network planning, traffic analysis, and IP accounting.

Flexible NetFlow improves on original NetFlow by adding the capability to customize the traffic analysis parameters for your specific requirements. Flexible NetFlow facilitates the creation of more complex configurations for traffic analysis and data export through the use of reusable configuration components.

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.

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

Prerequisites for Flexible NetFlow with Predefined Records

- You are familiar with the information in the " Cisco IOS Flexible NetFlow Overview " module.
- The networking device must be running a Cisco IOS release that supports Flexible NetFlow.

IPv4 Traffic

- The networking device must be configured for IPv4 routing.
- One of the following must be enabled on your router and on any interfaces on which you want to enable Flexible NetFlow: Cisco Express Forwarding or distributed Cisco Express Forwarding.

IPv6 Traffic

- The networking device must be configured for IPv6 routing.
- One of the following must be enabled on your router and on any interfaces on which you want to enable Flexible NetFlow: Cisco Express Forwarding IPv6 or distributed Cisco Express Forwarding IPv6.

Restrictions for Flexible NetFlow with Predefined Records

Cisco IOS Release 12.2(50)SY

- Predefined records specifying mask and prefix are not supported.

Information About Configuring Flexible NetFlow with Predefined Records

Flexible NetFlow Predefined Records

Flexible NetFlow predefined records are based on the original NetFlow ingress and egress caches and the aggregation caches. The difference between the original NetFlow aggregation caches and the corresponding predefined Flexible NetFlow records is that the predefined records do not perform aggregation. Flexible NetFlow predefined records are associated with a Flexible NetFlow flow monitor the same way that you associate a user-defined (custom) record.

Benefits of Flexible NetFlow Predefined Records

If you have been using original NetFlow or original NetFlow with aggregation caches you can continue to capture the same traffic data for analysis when you migrate to Flexible NetFlow by using the predefined records available with Flexible NetFlow. Many users will find that the preexisting Flexible NetFlow records are suitable for the majority of their traffic analysis requirements.

NetFlow Original and NetFlow IPv4 Original Input Predefined Records

The Flexible NetFlow "NetFlow original" and "NetFlow IPv4 original input" predefined records can be used interchangeably because they have the same key and nonkey fields. The key and nonkey fields and the counters for the Flexible NetFlow "NetFlow original" and "NetFlow IPv4 original input" predefined records are shown in the table below.

Table 1 *Key and Nonkey Fields Used by the Flexible NetFlow NetFlow Original and NetFlow IPv4 Original Input Predefined Records*

Field	Key or Nonkey Field	Definition
IP ToS	Key	Value in the type of service (ToS) field.
IP Protocol	Key	Value in the IP protocol field.
IP Source Address	Key	IP source address.
IP Destination Address	Key	IP destination address.
Transport Source Port	Key	Value of the transport layer source port field.
Transport Destination Port	Key	Value of the transport layer destination port field.
Interface Input	Key	Interface on which the traffic is received.
Flow Sampler ID	Key	ID number of the flow sampler (if flow sampling is enabled).

Field	Key or Nonkey Field	Definition
IP Source AS	Nonkey	Source autonomous system number.
IP Destination AS	Nonkey	Destination autonomous system number.
IP Next Hop Address	Nonkey	IP address of the next hop.
IP Source Mask	Nonkey	Mask for the IP source address.
IP Destination Mask	Nonkey	Mask for the IP destination address.
TCP Flags	Nonkey	Value in the TCP flag field.
Interface Output	Nonkey	Interface on which the traffic is transmitted.
Counter Bytes	Nonkey	Number of bytes seen in the flow.
Counter Packets	Nonkey	Number of packets seen in the flow.
Time Stamp System Uptime First	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched.
Time Stamp System Uptime Last	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched.

The configuration in the How to Get Started with Configuring Flexible NetFlow uses the predefined Flexible NetFlow "NetFlow original" record.

NetFlow IPv4 Original Output Predefined Record

The Flexible NetFlow "NetFlow IPv4 original output" predefined record is used to emulate the original NetFlow Egress NetFlow Accounting feature that was released in Cisco IOS Release 12.3(11)T. The key and nonkey fields and the counters for the Flexible NetFlow "NetFlow IPv4 original output" predefined record are shown in the table below.

Table 2 *Key and Nonkey Fields Used by the Flexible NetFlow NetFlow IPv4 Original Output Predefined Record*

Field	Key or Nonkey Field	Definition
IP ToS	Key	Value in the ToS field.
IP Protocol	Key	Value in the IP protocol field.

Field	Key or Nonkey Field	Definition
IP Source Address	Key	IP source address.
IP Destination Address	Key	IP destination address.
Transport Source Port	Key	Value of the transport layer source port field.
Transport Destination Port	Key	Value of the transport layer destination port field.
Interface Output	Key	Interface on which the traffic is transmitted.
Flow Sampler ID	Key	ID number of the flow sampler (if flow sampling is enabled).
IP Source AS	Nonkey	Source autonomous system number.
IP Destination AS	Nonkey	Destination autonomous system number.
IP Next Hop Address	Nonkey	IP address of the next hop.
IP Source Mask	Nonkey	Mask for the IP source address.
IP Destination Mask	Nonkey	Mask for the IP destination address.
TCP Flags	Nonkey	Value in the TCP flag field.
Interface Input	Nonkey	Interface on which the traffic is received.
Counter Bytes	Nonkey	Number of bytes seen in the flow.
Counter Packets	Nonkey	Number of packets seen in the flow.
Time Stamp System Uptime First	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched.
Time Stamp System Uptime Last	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched.

The configuration in the Example Configuring Flexible NetFlow Egress Accounting for IPv4 and IPv6 Traffic uses the predefined Flexible NetFlow "NetFlow original output" record.

NetFlow IPv6 Original Input Predefined Record

The key and nonkey fields and the counters for the Flexible NetFlow "NetFlow IPv6 original input" predefined record are shown in the table below.

Table 3   Key and Nonkey Fields Used by the Flexible NetFlow NetFlow IPv6 Original Input Predefined Record

Field	Key or NonKey Field	Definition
Traffic Class	Key	Value in the traffic class field.
Flow Label	Key	Flow label.
Protocol	Key	Value in the protocol field.
Extension Map	Key	Value in the extension map bitmap.
IP Source Address	Key	IP source address.
IP Destination Address	Key	IP destination address.
Transport Source Port	Key	Value of the transport layer source port field.
Transport Destination Port	Key	Value of the transport layer destination port field.
Interface Input	Key	Interface on which the traffic is received.
Flow Direction	Key	The direction of the flow.
Flow Sampler	Key	ID number of the flow sampler (if flow sampling is enabled).
Routing Source AS	Nonkey	Source autonomous system number.
Routing Destination AS	Nonkey	Destination autonomous system number.
Routing Next-hop Address	Nonkey	IP address of the next hop.
IP Source Mask	Nonkey	Mask for the IP source address.
IP Destination Mask	Nonkey	Mask for the IP destination address.
Transport TCP Flags	Nonkey	Value in the TCP flag field.
Interface Output	Nonkey	Interface over which the traffic is transmitted.
Counter Bytes	Nonkey	Number of bytes seen in the flow.

Field	Key or NonKey Field	Definition
Counter Packets	Nonkey	Number of packets seen in the flow.
Time Stamp System Uptime First	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched.
Time Stamp System Uptime Last	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched.

NetFlow IPv6 Original Input Predefined Record

The key and nonkey fields and the counters for the Flexible NetFlow "NetFlow IPv6 original input" predefined record are shown in the table below.

Table 4   Key and Nonkey Fields Used by the Flexible NetFlow NetFlow IPv6 Original Input Predefined Record

Field	Key or NonKey Field	Definition
Traffic Class	Key	Value in the traffic class field.
Flow Label	Key	Flow label.
Protocol	Key	Value in the protocol field.
Extension Map	Key	Value in the extension map bitmap.
IP Source Address	Key	IP source address.
IP Destination Address	Key	IP destination address.
Transport Source Port	Key	Value of the transport layer source port field.
Transport Destination Port	Key	Value of the transport layer destination port field.
Interface Input	Key	Interface on which the traffic is received.
Flow Direction	Key	The direction of the flow.
Flow Sampler	Key	ID number of the flow sampler (if flow sampling is enabled).
Routing Source AS	Nonkey	Source autonomous system number.

Field	Key or NonKey Field	Definition
Routing Destination AS	Nonkey	Destination autonomous system number.
Routing Next-hop Address	Nonkey	IP address of the next hop.
IP Source Mask	Nonkey	Mask for the IP source address.
IP Destination Mask	Nonkey	Mask for the IP destination address.
Transport TCP Flags	Nonkey	Value in the TCP flag field.
Interface Output	Nonkey	Interface over which the traffic is transmitted.
Counter Bytes	Nonkey	Number of bytes seen in the flow.
Counter Packets	Nonkey	Number of packets seen in the flow.
Time Stamp System Uptime First	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched.
Time Stamp System Uptime Last	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched.

Autonomous System Predefined Record

The Flexible NetFlow "autonomous system" predefined record creates flows based on autonomous system-to-autonomous system traffic flow data. The Flexible NetFlow "autonomous system" predefined record uses the same key and nonkey fields as the original NetFlow "autonomous system" aggregation cache.

Note   This predefined record can be used to analyze IPv4 and IPv6 traffic.

The table below lists the key and nonkey fields used in the Flexible NetFlow "autonomous system" predefined record.

Table 5   *Key and Nonkey Fields Used by the Flexible NetFlow Autonomous System Predefined Record*

Field	Key or Nonkey Field	Definition
IP Source AS	Key	Autonomous system of the source IP address (peer or origin).

Field	Key or Nonkey Field	Definition
IP Destination AS	Key	Autonomous system of the destination IP address (peer or origin).
Interface Input	Key	Interface on which the traffic is received.
Interface Output	Key	Interface on which the traffic is transmitted.
Flow Direction	Key	Direction in which the flow is being monitored.
Counter Bytes	Nonkey	Number of bytes seen in the flow.
Counter Packets	Nonkey	Number of packets seen in the flow.
Time Stamp System Uptime First	Nonkey	System uptime (time, in milliseconds since this device was first booted) when the first packet was switched.
Time Stamp System Uptime Last	Nonkey	System uptime (time, in milliseconds since this device was first booted) when the last packet was switched.

Autonomous System ToS Predefined Record

The Flexible NetFlow "autonomous system ToS" predefined record creates flows based on autonomous system-to-autonomous system and type of service (ToS) traffic flow data. The Flexible NetFlow "autonomous system ToS" predefined record uses the same key and nonkey fields as the original NetFlow "autonomous system ToS" aggregation cache.

Note This predefined record can be used to analyze only IPv4 traffic.

Tip This predefined record is particularly useful for generating autonomous system-to-autonomous system traffic flow data.

The table below lists the key and nonkey fields used in the Flexible NetFlow "autonomous system ToS" predefined record.

Table 6   *Key and Nonkey Fields Used by the Flexible NetFlow Autonomous System ToS Predefined Record*

Field	Key or Nonkey Field	Definition
IP ToS	Key	Value in the ToS field.
IP Source autonomous system	Key	Autonomous system of the source IP address (peer or origin).
IP Destination autonomous system	Key	Autonomous system of the destination IP address (peer or origin).
Interface Input	Key	Interface on which the traffic is received.
Interface Output	Key	Interface on which the traffic is transmitted.
Flow Direction	Key	Direction in which the flow is being monitored.
Counter Bytes	Nonkey	Number of bytes seen in the flow.
Counter Packets	Nonkey	Number of packets seen in the flow.
Time Stamp System Uptime First	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched.
Time Stamp System Uptime Last	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched.

BGP Next-Hop Predefined Record

The Flexible NetFlow "BGP next-hop" predefined record creates flows based on Border Gateway Protocol (BGP) traffic flow data.

Note   This predefined record can be used to analyze only IPv6 traffic.

The table below lists the key and nonkey fields used in the Flexible NetFlow "BGP next-hop" predefined record.

Table 7   *Key and Nonkey Fields Used by the Flexible NetFlow BGP Next-Hop Predefined Record*

Field	Key or Nonkey Field	Definition
Routing Source AS	Key	Autonomous system of the source IP address.
Routing Destination AS	Key	Autonomous system of the destination IP address.
Routing Next-hop Address IPv6 BGP	Key	IPv6 address of the BGP next hop.
Interface Input	Key	Interface on which the traffic is received.
Interface Output	Key	Interface on which the traffic is transmitted.
Flow Direction	Key	Direction in which the flow is being monitored.
Counter Bytes	Nonkey	Number of bytes seen in the flow.
Counter Packets	Nonkey	Number of packets seen in the flow.
Timestamp Sys-uptime First	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched.
Timestamp Sys-uptime Last	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched.

BGP Next-Hop ToS Predefined Record

The Flexible NetFlow "BGP next-hop ToS" predefined record creates flows based on BGP and ToS traffic flow data. The Flexible NetFlow "BGP next-hop ToS" predefined record uses the same key and nonkey fields as the original NetFlow "BGP next-hop ToS" aggregation cache.

Note   This predefined record can be used to analyze only IPv4 traffic.

The table below lists the key and nonkey fields used in the "BGP next-hop ToS" predefined record.

Table 8   *Key and Nonkey Fields Used by the Flexible NetFlow BGP Next-Hop ToS Predefined Record*

Field	Key or Nonkey Field	Definition
IP ToS	Key	Value in the ToS field.
IP Source autonomous system	Key	Autonomous system of the source IP address (peer or origin).
IP Destination autonomous system	Key	Autonomous system of the destination IP address (peer or origin).
IPv4 Next Hop Address BGP	Key	IPv4 address of the BGP next hop.
Interface Input	Key	Interface on which the traffic is received.
Interface Output	Key	Interface on which the traffic is transmitted.
Flow Direction	Key	Direction in which the flow is being monitored.
Counter Bytes	Nonkey	Number of bytes seen in the flow.
Counter Packets	Nonkey	Number of packets seen in the flow.
Time Stamp System Uptime First	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched.
Time Stamp System Uptime Last	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched.

Destination Prefix Predefined Record

The Flexible NetFlow "destination prefix" predefined record creates flows based on destination prefix traffic flow data. The Flexible NetFlow "destination prefix" predefined record uses the same key and nonkey fields as the original NetFlow "destination prefix" aggregation cache.

Note   This predefined record can be used to analyze IPv4 and IPv6 traffic.

The table below lists the key and nonkey fields used in the Flexible NetFlow "destination prefix" predefined record.

Table 9   *Key and Nonkey Fields Used by the Flexible NetFlow Destination Prefix Predefined Record*

Field	Key or Nonkey Field	Definition
IP Destination autonomous system	Key	Autonomous system of the destination IP address (peer or origin).
IPv4 or IPv6 Destination Prefix	Key	Destination IP address ANDed with the destination prefix mask.
IPv4 or IPv6 Destination Mask	Key	Number of bits in the destination prefix.
Interface Output	Key	Interface on which the traffic is transmitted.
Flow Direction	Key	Direction in which the flow is being monitored.
Counter Bytes	Nonkey	Number of bytes seen in the flow.
Counter Packets	Nonkey	Number of packets seen in the flow.
Time Stamp System Uptime First	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched.
Time Stamp System Uptime Last	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched.

Destination Prefix ToS Predefined Record

The Flexible NetFlow "destination prefix ToS" predefined record creates flows based on destination prefix and ToS traffic flow data. The Flexible NetFlow "destination prefix ToS" predefined record uses the same key and nonkey fields as the original NetFlow "destination prefix ToS" aggregation cache.

This predefined record is particularly useful for capturing data with which you can examine the destinations of network traffic passing through a NetFlow-enabled device.

Note   This predefined record can be used to analyze only IPv4 traffic.

The table below lists the key and nonkey fields used in the Flexible NetFlow "destination prefix ToS" predefined record.

Table 10   Key and Nonkey Fields Used by the Flexible NetFlow Destination Prefix ToS Predefined Record

Field	Key or Nonkey Field	Definition
IP ToS	Key	Value in the ToS field.
IP Destination autonomous system	Key	Autonomous system of the destination IP address (peer or origin).
IPv4 Destination Prefix	Key	Destination IP address ANDed with the destination prefix mask.
IPv4 Destination Mask	Key	Number of bits in the destination prefix.
Interface Output	Key	Interface on which the traffic is transmitted.
Flow Direction	Key	Direction in which the flow is being monitored.
Counter Bytes	Nonkey	Number of bytes seen in the flow.
Counter Packets	Nonkey	Number of packets seen in the flow.
Time Stamp System Uptime First	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched.
Time Stamp System Uptime Last	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched.

Prefix Predefined Record

The Flexible NetFlow "prefix" predefined record creates flows based on the source and destination prefixes in the traffic flow data. The Flexible NetFlow "prefix" predefined record uses the same key and nonkey fields as the original NetFlow "prefix" aggregation cache.

Note   This predefined record can be used to analyze IPv4 and IPv6 traffic. For IPv6 traffic, a minimum prefix mask length of 0 bits is assumed.

The table below lists the key and nonkey fields used in the Flexible NetFlow "prefix" predefined record.

Table 11   *Key and Nonkey Fields Used by the Flexible NetFlow Prefix Predefined Record*

Field	Key or Nonkey Field	Definition
IP Source autonomous system	Key	Autonomous system of the source IP address (peer or origin).
IP Destination autonomous system	Key	Autonomous system of the destination IP address (peer or origin).
IPv4 or IPv6 Source Prefix	Key	Source IP address ANDed with the source prefix mask, or the prefix to which the source IP address of the aggregated flows belongs.
IPv4 or IPv6 Source Mask	Key	Number of bits in the source prefix.
IPv4 or IPv6 Destination Prefix	Key	Destination IP address ANDed with the destination prefix mask.
IPv4 or IPv6 Destination Mask	Key	Number of bits in the destination prefix.
Interface Input	Key	Interface on which the traffic is received.
Interface Output	Key	Interface on which the traffic is transmitted.
Counter Bytes	Nonkey	Number of bytes seen in the flow.
Counter Packets	Nonkey	Number of packets seen in the flow.
Time Stamp System Uptime First	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched.
Time Stamp System Uptime Last	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched.

Prefix Port Predefined Record

The Flexible NetFlow "prefix port" predefined record creates flows based on source and destination prefixes and ports in the traffic flow data. The Flexible NetFlow "prefix port" predefined record uses the same key and nonkey fields as the original NetFlow "prefix port" aggregation cache.

This predefined record is particularly useful for capturing data with which you can examine the sources and destinations of network traffic passing through a NetFlow-enabled device.

Note This predefined record can be used to analyze only IPv4 traffic.

The table below lists the key and nonkey fields used in the destination Flexible NetFlow "prefix port" predefined record.

Table 12   *Key and Nonkey Fields Used by the Flexible NetFlow Prefix Port Predefined Record*

Field	Key or Nonkey Field	Definition
IP ToS	Key	Value in the ToS field.
IP Protocol	Key	Value in the IP protocol field.
IPv4 Source Prefix	Key	Source IP address ANDed with the source prefix mask, or the prefix to which the source IP address of the aggregated flows belongs.
IPv4 Source Mask	Key	Number of bits in the source prefix.
IPv4 Destination Prefix	Key	Destination IP address ANDed with the destination prefix mask.
IPv4 Destination Mask	Key	Number of bits in the destination prefix.
Transport Source Port	Key	Value in the transport layer source port field.
Transport Destination Port	Key	Value in the transport layer destination port field.
Interface Input	Key	Interface on which the traffic is received.
Interface Output	Key	Interface on which the traffic is transmitted.
Flow Direction	Key	Direction in which the flow is being monitored.
Counter Bytes	Nonkey	Number of bytes seen in the flow.
Counter Packets	Nonkey	Number of packets seen in the flow.
Time Stamp System Uptime First	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched.

Field	Key or Nonkey Field	Definition
Time Stamp System Uptime Last	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched.

Prefix ToS Predefined Record

The Flexible NetFlow "prefix ToS" predefined record creates flows based on source and destination prefixes and ToS traffic flow data. The Flexible NetFlow "prefix ToS" predefined record uses the same key and nonkey fields as the original NetFlow "destination prefix ToS" aggregation cache.

This predefined record is particularly useful for capturing data with which you can examine the sources and destinations of network traffic passing through a NetFlow-enabled device.

Note This predefined record can be used to analyze only IPv4 traffic.

The table below lists the key and nonkey fields used in the Flexible NetFlow "prefix ToS" predefined record.

Table 13   *Key and Nonkey Fields Used by the Flexible NetFlow Prefix ToS Predefined Record*

Field	Key or Nonkey Field	Definition
IP ToS	Key	Value in the ToS field.
IP Source autonomous system	Key	Autonomous system of the source IP address (peer or origin).
IP Destination autonomous system	Key	Autonomous system of the destination IP address (peer or origin).
IPv4 Source Prefix	Key	Source IP address ANDed with the source prefix mask, or the prefix to which the source IP address of the aggregated flows belongs.
IPv4 Source Mask	Key	Number of bits in the source prefix.
IPv4 Destination Prefix	Key	Destination IP address ANDed with the destination prefix mask.
IPv4 Destination Mask	Key	Number of bits in the destination prefix.
Interface Input	Key	Interface on which the traffic is received.

Field	Key or Nonkey Field	Definition
Interface Output	Key	Interface on which the traffic is transmitted.
Flow Direction	Key	Direction in which the flow is being monitored.
Counter Bytes	Nonkey	Number of bytes seen in the flow.
Counter Packets	Nonkey	Number of packets seen in the flow.
Time Stamp System Uptime First	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched.
Time Stamp System Uptime Last	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched.

Protocol Port Predefined Record

The Flexible NetFlow "protocol port" predefined record creates flows based on protocols and ports in the traffic flow data. The Flexible NetFlow "protocol port" predefined record uses the same key and nonkey fields as the original NetFlow "protocol port" aggregation cache.

Note   This predefined record can be used to analyze IPv4 and IPv6 traffic.

The table below lists the key and nonkey fields used in the Flexible NetFlow "protocol port" predefined record.

Table 14   Key and Nonkey Fields Used by the Flexible NetFlow Protocol Port Predefined Record

Field	Key or Nonkey Field	Definition
IP Protocol	Key	Value in the IP protocol field.
Transport Source Port	Key	Value in the transport layer source port field.
Transport Destination Port	Key	Value in the transport layer destination port field.
Flow Direction	Key	Direction in which the flow is being monitored.
Counter Bytes	Nonkey	Number of bytes seen in the flow.

Field	Key or Nonkey Field	Definition
Counter Packets	Nonkey	Number of packets seen in the flow.
Time Stamp System Uptime First	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched.
Time Stamp System Uptime Last	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched.

Protocol Port ToS Predefined Record

The Flexible NetFlow "protocol port ToS" predefined record creates flows based on the protocol, port, and ToS value in the traffic data. The Flexible NetFlow "protocol port ToS" predefined record uses the same key and nonkey fields as the original NetFlow "protocol port ToS" aggregation cache.

This predefined record is particularly useful for capturing data with which you can examine network usage by type of traffic.

Note This predefined record can be used to analyze only IPv4 traffic.

The table below lists the key and nonkey fields used in the Flexible NetFlow "protocol port ToS" predefined record.

Table 15   *Key and Nonkey Fields Used by the Flexible NetFlow Protocol Port ToS Predefined Record*

Field	Key or Nonkey Field	Definition
IP ToS	Key	Value in the ToS field.
IP Protocol	Key	Value in the IP protocol field.
Transport Source Port	Key	Value in the transport layer source port field.
Transport Destination Port	Key	Value in the transport layer destination port field.
Flow Direction	Key	Direction in which the flow is being monitored.
Counter Bytes	Nonkey	Number of bytes seen in the flow.
Counter Packets	Nonkey	Number of packets seen in the flow.

Field	Key or Nonkey Field	Definition
Time Stamp System Uptime First	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched.
Time Stamp System Uptime Last	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched.

Source Prefix Predefined Record

The Flexible NetFlow "source prefix" predefined record creates flows based on source prefixes in the network traffic. The Flexible NetFlow "source prefix" predefined record uses the same key and nonkey fields as the original NetFlow "source prefix" aggregation cache.

Note This predefined record can be used to analyze IPv4 and IPv6 traffic.

The table below lists the key and nonkey fields used in the Flexible NetFlow "source prefix" predefined record.

Table 16   Key and Nonkey Fields Used by the Flexible NetFlow Source Prefix Predefined Record

Field	Key or Nonkey Field	Definition
IP Source autonomous system	Key	Autonomous system of the source IP address (peer or origin).
IPv4 or IPv6 Source Prefix	Key	Source IP address ANDed with the source prefix mask, or the prefix to which the source IP address of the aggregated flows belongs.
IPv4 or IPv6 Source Mask	Key	Number of bits in the source prefix.
Interface Input	Key	Interface on which the traffic is received.
Flow Direction	Key	Direction in which the flow is being monitored.
Counter Bytes	Nonkey	Number of bytes seen in the flow.
Counter Packets	Nonkey	Number of packets seen in the flow.

Field	Key or Nonkey Field	Definition
Time Stamp System Uptime First	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched.
Time Stamp System Uptime Last	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched.

Source Prefix ToS Predefined Record

The Flexible NetFlow "source prefix ToS" predefined record creates flows based on source prefixes and ToS values in the network traffic. The Flexible NetFlow "source prefix ToS" predefined record uses the same key and nonkey fields as the original NetFlow "source prefix ToS" aggregation cache.

This predefined record is particularly useful for capturing data with which you can examine the sources of network traffic passing through a NetFlow-enabled device.

Note   This predefined record can be used to analyze only IPv4 traffic.

The table below lists the key and nonkey fields used in the Flexible NetFlow "source prefix ToS" predefined record.

Table 17   Key and Nonkey Fields Used by the Flexible NetFlow Source Prefix ToS Predefined Record

Field	Key or Nonkey Field	Definition
IP ToS	Key	Value in the ToS field.
IP Source autonomous system	Key	Autonomous system of the source IP address (peer or origin).
IPv4 Source Prefix	Key	Source IP address ANDed with the source prefix mask, or the prefix to which the source IP address of the aggregated flows belongs.
IPv4 Source Mask	Key	Number of bits in the source prefix.
Interface Input	Key	Interface on which the traffic is received.
Flow Direction	Key	Direction in which the flow is being monitored.
Counter Bytes	Nonkey	Number of bytes seen in the flow.

Field	Key or Nonkey Field	Definition
Counter Packets	Nonkey	Number of packets seen in the flow.
Time Stamp System Uptime First	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched.
Time Stamp System Uptime Last	Nonkey	System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched.

How to Configure a Predefined Record for the Flow Monitor

Note Only the keywords and arguments required for the Flexible NetFlow commands used in these tasks are explained in these tasks. For information on the other keywords and arguments available for these Flexible NetFlow commands, refer to the *Cisco IOS Flexible NetFlow Command Reference*.

Configuring a Flow Monitor for IPv4 Traffic Using a Predefined Record

To configure a flow monitor for IPv4 traffic using a predefined record for the flow monitor, perform the following required task.

Each flow monitor has a separate cache assigned to it. Each flow monitor requires a record to define the contents and layout of its cache entries. The record format can be one of the predefined record formats, or an advanced user may create his or her own record format using the **collect** and **match** commands in Flexible NetFlow flow record configuration mode.

Note You must remove a flow monitor from all of the interfaces on which you have applied it before you can modify the **record** format of the flow monitor.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow monitor** *monitor-name*
4. **description** *description*
5. **record** {**netflow-original** | **netflow ipv4** *record* [**peer**]}
6. **end**
7. **show flow record** *record-name*
8. **show running-config flow record** *record-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**flow monitor** *monitor-name* **Example:** `Router(config)# flow monitor FLOW-MONITOR-1`	Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode. • This command also allows you to modify an existing flow monitor.
Step 4	**description** *description* **Example:** `Router(config-flow-monitor)# description Used for monitoring IPv4 traffic`	(Optional) Creates a description for the flow monitor.
Step 5	**record** {**netflow-original**	**netflow ipv4** *record* [**peer**]} **Example:** `Router(config-flow-monitor)# record netflow ipv4 original-input`	Specifies the record for the flow monitor.

	Command or Action	Purpose
Step 6	**end** **Example:** Router(config-flow-monitor)# end	Exits Flexible NetFlowflow monitor configuration mode and returns to privileged EXEC mode.
Step 7	**show flow record** *record-name* **Example:** Router# show flow record FLOW_RECORD-1	(Optional) Displays the current status of the specified flow record.
Step 8	**show running-config flow record** *record-name* **Example:** Router# show running-config flow record FLOW_RECORD-1	(Optional) Displays the configuration of the specified flow record.

Configuring a Flow Monitor for IPv6 Traffic Using a Predefined Record

To configure a flow monitor for IPv6 traffic using a predefined record for the flow monitor, perform the following required task.

Each flow monitor has a separate cache assigned to it. Each flow monitor requires a record to define the contents and layout of its cache entries. The record format can be one of the predefined record formats, or an advanced user may create his or her own record format using the **collect** and **match**commands in Flexible NetFlow flow record configuration mode.

Note   You must remove a flow monitor from all of the interfaces on which you have applied it before you can modify the **record** format of the flow monitor.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow monitor** *monitor-name*
4. **description** *description*
5. **record netflow ipv6** *record* [**peer**]
6. **end**
7. **show flow record** *record-name*
8. **show running-config flow record** *record-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**flow monitor** *monitor-name* **Example:** Router(config)# flow monitor FLOW-MONITOR-2	Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode. • This command also allows you to modify an existing flow monitor.
Step 4	**description** *description* **Example:** Router(config-flow-monitor)# description Used for monitoring IPv6 traffic	(Optional) Creates a description for the flow monitor.
Step 5	**record netflow ipv6** *record* [**peer**] **Example:** Router(config-flow-monitor)# record netflow ipv6 original-input	Specifies the record for the flow monitor.
Step 6	**end** **Example:** Router(config-flow-monitor)# end	Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode.
Step 7	**show flow record** *record-name* **Example:** Router# show flow record FLOW_RECORD-1	(Optional) Displays the current status of the specified flow record.

Command or Action	Purpose
Step 8 **show running-config flow record** *record-name*	(Optional) Displays the configuration of the specified flow record.
Example:	
`Router# show running-config flow record FLOW_RECORD-1`	

Applying an IPv4 Flow Monitor to an Interface

Before it can be activated, an IPv4 flow monitor must be applied to at least one interface. To activate an IPv4 flow monitor by applying the flow monitor to an interface, perform the following required task.

✎

Note   When you specify the "NetFlow original" or the "NetFlow IPv4 original input" predefined record for the flow monitor to emulate original NetFlow, the flow monitor can be used for analyzing only input (ingress) traffic.

When you specify the "NetFlow IPv4 original output" predefined record for the flow monitor to emulate the Egress NetFlow Accounting feature, the flow monitor can be used for analyzing only output (egress) traffic.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip flow monitor** *monitor-name* {**input** | **output**}
5. **end**
6. **show flow monitor** *monitor-name*
7. **show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]][**statistics**]]

DETAILED STEPS

Command or Action	Purpose
Step 1 **enable**	Enables privileged EXEC mode.
	• Enter your password if prompted.
Example:	
`Router> enable`	

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface ethernet 0/0	Specifies an interface and enters interface configuration mode.
Step 4	**ip flow monitor** *monitor-name* {**input** | **output**} **Example:** Router(config-if)# ip flow monitor FLOW-MONITOR-1 input	Activates the flow monitor that you created previously by assigning it to the interface to analyze traffic. • You can configure input and output traffic analysis concurrently by configuring the **ip flow monitor** *monitor-name* **input** and **ip flow monitor** *monitor-name* **output** commands on the same interface. You can use different flow monitors for input and output traffic analysis.
Step 5	**end** **Example:** Router(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.
Step 6	**show flow monitor** *monitor-name* **Example:** Router# show flow monitor FLOW_MONITOR-1	(Optional) Displays the current status of the specified flow monitor.
Step 7	**show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]][**statistics**]] **Example:** Router# show flow monitor FLOW-MONITOR-1	(Optional) Displays the status and statistics for a Flexible NetFlow flow monitor.

Applying an IPv6 Flow Monitor to an Interface

Before it can be activated, an IPv6 flow monitor must be applied to at least one interface. To activate an IPv4 flow monitor by applying the flow monitor to an interface, perform the following required task.

✎

Note   When you specify the "NetFlow IPv6 original input" predefined record for the flow monitor to emulate original NetFlow, the flow monitor can be used only for analyzing input (ingress) traffic.

When you specify the "NetFlow IPv6 original output" predefined record for the flow monitor to emulate the Egress NetFlow Accounting feature, the flow monitor can be used only for analyzing output (egress) traffic.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 flow monitor** *monitor-name* {**input** | **output**}
5. **end**
6. **show flow monitor** *monitor-name*
7. **show running-config flow monitor** *monitor-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 0/0`	Specifies an interface and enters interface configuration mode.
Step 4	**ipv6 flow monitor** *monitor-name* {**input**	**output**} **Example:** `Router(config-if)# ipv6 flow monitor FLOW-MONITOR-2 input`	Activates the flow monitor that you created previously by assigning it to the interface to analyze traffic. • You can configure input and output traffic analysis concurrently by configuring the **ipv6 flow monitor** *monitor-name* **input** and **ipv6 flow monitor** *monitor-name* **output** commands on the same interface. You can use different flow monitors for input and output traffic analysis.

Command or Action	Purpose
Step 5 **end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 6 **show flow monitor** *monitor-name* **Example:** `Router# show flow monitor FLOW_MONITOR-1`	(Optional) Displays the current status of the specified flow monitor.
Step 7 **show running-config flow monitor** *monitor-name* **Example:** `Router# show flow monitor FLOW_MONITOR-1`	(Optional) Displays the configuration of the specified flow monitor.

Configuration Examples for Flexible NetFlow with Predefined Records

Example Configuring a Flexible NetFlow Predefined Record for IPv4 Traffic

The following example shows how to configure a flow monitor using the Flexible NetFlow "BGP ToS next-hop" predefined record to monitor IPv4 traffic.

This sample starts in global configuration mode:

```
!
flow monitor FLOW-MONITOR-1
 record netflow ipv4 bgp-nexthop-tos
 exit
!
ip cef
!
interface Ethernet 0/0
 ip address 172.16.6.2 255.255.255.0
 ip flow monitor FLOW-MONITOR-1 input
!
```

Example Configuring a Flexible NetFlow Predefined Record for IPv6 Traffic

The following example shows how to configure a flow monitor using the Flexible NetFlow "source prefix" predefined record to monitor IPv6 traffic.

This sample starts in global configuration mode:

```
!
flow monitor FLOW-MONITOR-2
 record netflow ipv6 source-prefix
 exit
ip cef
ipv6 cef
!
interface Ethernet 0/0
 ipv6 address 2001:DB8:2:ABCD::2/48
 ipv6 flow monitor FLOW-MONITOR-2 input
!
```

Where to Go Next

For information on advanced Flexible NetFlow configurations for specific purposes such as quality of service (QoS) and bandwidth monitoring, application and user flow monitoring and profiling, and security analysis, refer to the "Customizing Cisco IOS Flexible NetFlow Flow Records and Flow Monitors" module.

If you want to configure flow sampling to reduce the CPU overhead of analyzing traffic, refer to the "Using Cisco IOS Flexible NetFlow Flow Sampling to Reduce the CPU Overhead of Analyzing Traffic" module.

If you want to configure data export for Flexible NetFlow, refer to the "Configuring Data Export for Cisco IOS Flexible NetFlow with Flow Exporters" module.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Overview of Flexible NetFlow	"Cisco IOS Flexible NetFlow Overview"
Emulating original NetFlow with Flexible NetFlow	"Getting Started with Configuring Cisco IOS Flexible NetFlow"
Configuring flow exporters to export Flexible NetFlow data	"Configuring Data Export for Cisco IOS Flexible NetFlow with Flow Exporters"
Customizing Flexible NetFlow	"Customizing Cisco IOS Flexible NetFlow Flow Records and Flow Monitors"
Configuring flow sampling to reduce the overhead of monitoring traffic with Flexible NetFlow	"Using Cisco IOS Flexible NetFlow Flow Sampling to Reduce the CPU Overhead of Analyzing Traffic"
Using Flexible NetFlow Top N Talkers to analyze network traffic	"Using Cisco IOS Flexible NetFlow Top N Talkers to Analyze Network Traffic"

Related Topic	Document Title
Configuring IPv4 multicast statistics support for Flexible NetFlow	"Configuring IPv4 Multicast Statistics Support for Cisco IOS Flexible NetFlow"
Configuration commands for Flexible NetFlow	*Cisco IOS Flexible NetFlow Command Reference*

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	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

RFC	Title
RFC 3954	*Cisco Systems NetFlow Services Export Version 9*

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 Flexible NetFlow

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

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

Table 18   ***Feature Information for Flexible NetFlow***

Feature Name	Releases	Feature Information
Flexible NetFlow	12.2(33)SRC 12.2(50)SY 12.4(9)T 15.0(1)SY	Flexible NetFlow is introduced. Support for this feature was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC. The following commands were introduced or modified: **cache**(Flexible NetFlow), **clear flow exporter**, **clear flow monitor**, **clear sampler**, **collect counter**, **collect flow**, **collect interface**, **collect ipv4**, **collect ipv4 destination**, **collect ipv4 fragmentation**, **collect ipv4 section**, **collect ipv4 source**, **collect ipv4 total-length**, **collect ipv4 ttl**, **collect routing**, **collect timestamp sys-uptime**, **collect transport**, **collect transport icmp ipv4**, **collect transport tcp**, **collect transport udp**, **debug flow exporter**, **debug flow monitor**, **debug flow record**, **debug sampler**, **description** (Flexible NetFlow), **destination**, **dscp** (Flexible NetFlow), **exporter**, **flow exporter**, **flow monitor**, **flow platform**, **flow record**, **ip flow monitor**, **match flow**, **match interface** (Flexible NetFlow), **match ipv4**, **match ipv4 destination**, **match ipv4 fragmentation**, **match ipv4 section**, **match ipv4 source**, **match ipv4 total-length**, **match ipv4 ttl**, **match routing**, **match transport**, **match transport icmp ipv4**, **match transport tcp**, **match transport udp**, **mode** (Flexible NetFlow), **option** (Flexible NetFlow), **record**, **sampler**, **show flow exporter**, **show flow interface**, **show flow monitor**, **show flow record**, **show sampler**, **source** (Flexible

Feature Name	Releases	Feature Information
		NetFlow), **statistics packet**, **template data timeout**, **transport** (Flexible NetFlow).
Flexible NetFlow--IPv6 Unicast Flows	12.2(33)SRE 12.2(50)SY 12.4(20)T 15.0(1)SY	Enables Flexible NetFlow to monitor IPv6 traffic. Support for this feature was added for Cisco 7200 and 7300 Network Processing Engine (NPE) series routers in Cisco IOS Release 12.2(33)SRE. The following commands were introduced or modified: **collect routing**, **debug flow record**, **match routing**, **record**, **show flow monitor**, **show flow record**, **collect ipv6**, **collect ipv6 destination**, **collect ipv6 extension map**, **collect ipv6 fragmentation**, **collect ipv6 hop-limit**, **collect ipv6 length**, **collect ipv6 section**, **collect ipv6 source**, **collect transport icmp ipv6**, **ipv6 flow monitor**, **match ipv6**, **match ipv6 destination**, **match ipv6 extension map**, **match ipv6 fragmentation**, **match ipv6 hop-limit**, **match ipv6 length**, **match ipv6 section**, **match ipv6 source**, **match transport icmp ipv6**.