



Configuring Cisco IOS Flexible NetFlow with Predefined Records

First Published: June 19, 2006

Last Updated: November 20, 2009

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 non-key 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 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 makes it easier to create 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 for Flexible NetFlow” section on page 31](#).

Use Cisco Feature Navigator to find information about platform support and Cisco IOS, Catalyst OS, and Cisco IOS XE 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 Flexible NetFlow with Predefined Records, page 2](#)
- [Information About Configuring Flexible NetFlow with Predefined Records, page 2](#)



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

© 2008–2009 Cisco Systems, Inc. All rights reserved.

- [How to Configure Flexible NetFlow Using a Predefined Record for the Flow Monitor](#), page 18
- [Configuration Examples for Configuring Flexible NetFlow with Predefined Records](#), page 27
- [Where to Go Next](#), page 28
- [Additional References](#), page 28
- [Feature Information for Flexible NetFlow](#), page 31

Prerequisites for Configuring Flexible NetFlow with Predefined Records

The following prerequisites must be met before you can configure Flexible NetFlow:

- 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. See the “[Cisco IOS Flexible NetFlow Features Roadmap](#)” module for a list of Cisco IOS software releases that support 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 (CEF) or distributed CEF (dCEF).

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 (CEF IPv6) or distributed CEF IPv6 (dCEF IPv6).

Information About Configuring Flexible NetFlow with Predefined Records

Before configuring Flexible NetFlow with predefined records, you should understand the following information:

- [Flexible NetFlow Predefined Records](#), page 3
- [Benefits of Flexible NetFlow Predefined Records](#), page 3
- [Flexible NetFlow “NetFlow Original” and “NetFlow IPv4 Original Input” Predefined Records](#), page 3
- [Flexible NetFlow “NetFlow IPv4 Original Output” Predefined Record](#), page 4
- [Flexible NetFlow “NetFlow IPv6 Original Input” Predefined Record](#), page 5
- [Flexible NetFlow “NetFlow IPv6 Original Output” Predefined Record](#), page 6
- [Flexible NetFlow “Autonomous System” Predefined Record](#), page 7
- [Flexible NetFlow “Autonomous System ToS” Predefined Record](#), page 8

- Flexible NetFlow “BGP Next-Hop ToS” Predefined Record, page 10
- Flexible NetFlow “Destination Prefix” Predefined Record, page 10
- Flexible NetFlow “Destination Prefix ToS” Predefined Record, page 11
- Flexible NetFlow “Prefix” Predefined Record, page 12
- Flexible NetFlow “Prefix Port” Predefined Record, page 13
- Flexible NetFlow “Prefix ToS” Predefined Record, page 14
- Flexible NetFlow “Protocol Port” Predefined Record, page 15
- Flexible NetFlow “Protocol Port ToS” Predefined Record, page 15
- Flexible NetFlow “Source Prefix” Predefined Record, page 16
- Flexible NetFlow “Source Prefix ToS” Predefined Record, page 17

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 pre-existing Flexible NetFlow records are suitable for the majority of their traffic analysis requirements.

Flexible NetFlow “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 non-key fields. The key and non-key fields and the counters for the “NetFlow original” and “NetFlow IPv4 original input” predefined records are shown in [Table 1](#).

Table 1 Key and Non Key-Fields Used by the “NetFlow Original” and “NetFlow IPv4 Original Input” Predefined Records

Field	Key or Non-Key Field	Definition
IP ToS	Key	Value in the type of service (ToS) field.
IP Protocol	Key	Value in the IP protocol field.
IPv4 Source Address	Key	IPv4 source address.
IPv4 Destination Address	Key	IPv4 source address.

Table 1 Key and Non Key-Fields Used by the “NetFlow Original” and “NetFlow IPv4 Original Input” Predefined Records (continued)

Field	Key or Non-Key Field	Definition
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.
Flow Sampler ID	Key	ID number of the flow sampler (if flow sampling is enabled).
IP Source AS	Non-key	Source autonomous system number.
IP Destination AS	Non-key	Destination autonomous system number.
IPv4 Next Hop Address	Non-key	IPv4 address of the next hop.
IPv4 Source Mask	Non-key	Mask for the IPv4 source address.
IPv4 Destination Mask	Non-key	Mask for the IPv4 destination address.
TCP Flags	Non-key	Value in the TCP flag field.
Interface Output	Non-key	Interface on which the traffic is transmitted.
Counter Bytes	Non-key	Number of bytes seen in the flow.
Counter Packets	Non-key	Number of packets seen in the flow.
Time Stamp System Uptime First	Non-key	System uptime (time in milliseconds since this device was first booted) when the first packet was switched.
Time Stamp System Uptime Last	Non-key	System uptime (time in milliseconds since this device was first booted) when the last packet was switched.

Flexible NetFlow “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 non-key fields and the counters for the “NetFlow IPv4 original output” predefined record are shown in [Table 2](#).

Table 2 Key and Non Key Fields Used by the “NetFlow IPv4 Original Output” Predefined Record

Field	Key or Non-Key Field	Definition
IP ToS	Key	Value in the ToS field.
IP Protocol	Key	Value in the IP protocol field.
IPv4 Source Address	Key	IPv4 source address.
IPv4 Destination Address	Key	IPv4 source address.
Transport Source Port	Key	Value in the transport layer source port field.

Table 2 *Key and Non Key Fields Used by the “NetFlow IPv4 Original Output” Predefined Record (continued)*

Field	Key or Non-Key Field	Definition
Transport Destination Port	Key	Value in 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	Non-key	Source autonomous system number.
IP Destination AS	Non-key	Destination autonomous system number.
IPv4 Next Hop Address	Non-key	IPv4 address of the next hop.
IPv4 Source Mask	Non-key	Mask for the IPv4 source address.
IPv4 Destination Mask	Non-key	Mask for the IPv4 destination address.
TCP Flags	Non-key	Value in the TCP flag field.
Interface Input	Non-key	Interface on which the traffic is received.
Counter Bytes	Non-key	Number of bytes seen in the flow.
Counter Packets	Non-key	Number of packets seen in the flow.
Time Stamp System Uptime First	Non-key	System uptime (time in milliseconds since this device was first booted) when the first packet was switched.
Time Stamp System Uptime Last	Non-key	System uptime (time in milliseconds since this device was first booted) when the last packet was switched.

Flexible NetFlow “NetFlow IPv6 Original Input” Predefined Record

The key and non-key fields and the counters for the Flexible NetFlow “NetFlow IPv6 original input” predefined records are shown in [Table 3](#).

Table 3 *Key and Non Key-Fields Used by the Flexible NetFlow “NetFlow IPv6 Original Input” Predefined Record*

Field	Key or Non-Key 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 in the transport layer source port field.
Transport Destination Port	Key	Value in the transport layer destination port field.

Table 3 *Key and Non Key-Fields Used by the Flexible NetFlow “NetFlow IPv6 Original Input” Predefined Record (continued)*

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

Flexible NetFlow “NetFlow IPv6 Original Output” Predefined Record

The key and non-key fields and the counters for the Flexible NetFlow “NetFlow IPv6 original output” predefined records are shown in [Table 4](#).

Table 4 *Key and Non Key-Fields Used by the Flexible NetFlow “NetFlow IPv6 Original Output” Predefined Record*

Field	Key or Non-Key Field	Definition
Traffic Class	Key	Value in the traffic class field.
Flow Label	Key	The 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 in the transport layer source port field.
Transport Destination Port	Key	Value in the transport layer destination port field.

Table 4 *Key and Non-Key-Fields Used by the Flexible NetFlow “NetFlow IPv6 Original Output” Predefined Record (continued)*

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

Flexible NetFlow “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 non-key fields as the original NetFlow “autonomous system” aggregation cache.



Note

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

[Table 5](#) lists the key and non-key fields used in the Flexible NetFlow “autonomous system” predefined record.

Table 5 *Key and Non-Key Fields Used by the Flexible NetFlow “Autonomous System” Predefined Record*

Field	Key or Non-Key Field	Definition
IP Source AS	Key	Autonomous system of the source IP address (peer or origin).
IP Destination AS	Key	Autonomous system of the destination IP address (peer or origin).

Table 5 *Key and Non-Key Fields Used by the Flexible NetFlow “Autonomous System” Predefined Record (continued)*

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

Flexible NetFlow “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 non-key fields as the original NetFlow “autonomous system TOS” aggregation cache.



Note

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



Tip

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

Table 6 lists the key and non-key fields used in the Flexible NetFlow “autonomous system TOS” predefined record.

Table 6 *Key and Non-Key Fields Used by the “Flexible NetFlow Autonomous System ToS” Predefined Record*

Field	Key or Non-Key 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	Non-key	Number of bytes seen in the flow.

Table 6 Key and Non-Key Fields Used by the “Flexible NetFlow Autonomous System ToS” Predefined Record (continued)

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

Flexible NetFlow “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 only be used to analyze IPv6 traffic.

Table 7 lists the key and non-key fields used in the Flexible NetFlow “BGP next-hop” predefined record.

Table 7 Key and Non-Key Fields Used by the Flexible NetFlow “BGP Next-hop” Predefined Record

Field	Key or Non-Key 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	Non-key	Number of bytes seen in the flow.
Counter Packets	Non-key	Number of packets seen in the flow.
Timestamp Sys-uptime First	Non-key	System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched.
Timestamp Sys-uptime Last	Non-key	System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched.

Flexible NetFlow “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 non-key fields as the original NetFlow “BGP next-hop ToS” aggregation cache.


Note

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

[Table 8](#) lists the key and non-key fields used in the “BGP next-hop ToS” predefined record.

Table 8 *Key and Non-Key Fields Used by the Flexible NetFlow “BGP Next-hop ToS” Predefined Record*

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

Flexible NetFlow “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 non-key fields as the original NetFlow “destination prefix” aggregation cache.


Note

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

[Table 9](#) lists the key and non-key fields used in the Flexible NetFlow “destination prefix” predefined record.

Table 9 *Key and Non-Key Fields Used by the Flexible NetFlow “Destination Prefix” Predefined Record*

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

Flexible NetFlow “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 non-key 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 only be used to analyze IPv4 traffic.

[Table 10](#) lists the key and non-key fields used in the used in the Flexible NetFlow “destination prefix ToS” predefined record.

Table 10 *Key and Non Key Fields Used by the Flexible NetFlow “Destination Prefix ToS” Predefined Record*

Field	Key or Non-Key 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.

Table 10 Key and Non Key Fields Used by the Flexible NetFlow “Destination Prefix ToS” Predefined Record (continued)

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

Flexible NetFlow “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 non-key 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.

Table 11 lists the key and non-key fields used in the Flexible NetFlow “prefix” predefined record.

Table 11 Key and Non-Key Fields Used by the Flexible NetFlow “Prefix” Predefined Record

Field	Key or Non-Key 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	Non-key	Number of bytes seen in the flow.

Table 11 Key and Non-Key Fields Used by the Flexible NetFlow “Prefix” Predefined Record

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

Flexible NetFlow “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 non-key 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 only be used to analyze IPv4 traffic.

Table 12 lists the key and non-key fields used in the destination Flexible NetFlow “prefix port” predefined record.

Table 12 Key and Non-Key Fields Used by the Flexible NetFlow “Prefix Port” Predefined Record

Field	Key or Non-Key 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	Non-key	Number of bytes seen in the flow.

Table 12 Key and Non-Key Fields Used by the Flexible NetFlow “Prefix Port” Predefined Record (continued)

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

Flexible NetFlow “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 non-key fields as the original NetFlow “destination prefix ToS” aggregation cache.

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



Note

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

Table 13 lists the key and non-key fields used in the Flexible NetFlow “prefix ToS” predefined record.

Table 13 Key and Non-Key Fields Used by the Flexible NetFlow “Prefix ToS” Predefined Record

Field	Key or Non-Key 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.
Interface Output	Key	Interface on which the traffic is transmitted.
Flow Direction	Key	Direction in which the flow is being monitored.
Counter Bytes	Non-key	Number of bytes seen in the flow.
Counter Packets	Non-key	Number of packets seen in the flow.

Table 13 Key and Non-Key Fields Used by the Flexible NetFlow “Prefix ToS” Predefined Record

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

Flexible NetFlow “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 non-key fields as the original NetFlow “protocol port” aggregation cache.



Note

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

Table 14 lists the key and non-key fields used in the Flexible NetFlow “protocol port” predefined record.

Table 14 Key and Non-Key Fields Used by the Flexible NetFlow “Protocol Port” Predefined Record

Field	Key or Non-Key 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 that the flow is being monitored in.
Counter Bytes	Non-key	Number of bytes seen in the flow.
Counter Packets	Non-key	Number of packets seen in the flow.
Time Stamp System Uptime First	Non-key	System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched.
Time Stamp System Uptime Last	Non-key	System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched.

Flexible NetFlow “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 non-key fields as the original NetFlow “protocol port ToS” aggregation cache.

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

**Note**

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

Table 15 lists the key and non-key fields used in the used in the Flexible NetFlow “protocol port ToS” predefined record.

Table 15 *Key and Non-Key Fields Used by the Flexible NetFlow “Protocol Port ToS” Predefined Record*

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

Flexible NetFlow “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 non-key fields as the original NetFlow “source prefix” aggregation cache.

**Note**

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

Table 16 lists the key and non-key fields used in the Flexible NetFlow “source prefix” predefined record.

Table 16 *Key and Non-Key Fields Used by the Flexible NetFlow “Source Prefix” Predefined Record*

Field	Key or Non-Key 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.

Table 16 *Key and Non-Key Fields Used by the Flexible NetFlow “Source Prefix” Predefined Record (continued)*

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

Flexible NetFlow “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 non-key fields as the original NetFlow “source prefix” ToS aggregation cache.

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



Note

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

[Table 17](#) lists the key and non-key fields used in the Flexible NetFlow “source prefix ToS” predefined record.

Table 17 *Key and Non-Key Fields Used by the Flexible NetFlow “Source Prefix ToS” Predefined Record*

Field	Key or Non-Key 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	Non-key	Number of bytes seen in the flow.
Counter Packets	Non-key	Number of packets seen in the flow.

Table 17 Key and Non-Key Fields Used by the Flexible NetFlow “Source Prefix ToS” Predefined Record (continued)

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

How to Configure Flexible NetFlow Using a Predefined Record for the Flow Monitor

The tasks in this section explain how to configure Flexible NetFlow using 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](#).

To configure and enable Flexible NetFlow using a predefined record, perform the following tasks:

- [Configuring a Flow Monitor for IPv4 Traffic Using a Predefined Record, page 18](#)
- [Configuring a Flow Monitor for IPv6 Traffic Using a Predefined Record, page 20](#)
- [Applying an IPv4 Flow Monitor to an Interface, page 21](#)
- [Applying an IPv6 Flow Monitor to an Interface, page 22](#)
- [Verifying the Flow Monitor, page 23](#) (optional)
- [Verifying That Flexible NetFlow Is Enabled, page 25](#) (optional)
- [Viewing the Flow Monitor Cache, page 25](#) (optional)

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.

Flow Monitors

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 flow record configuration mode.

Restrictions

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** *text-string*
5. **record** {**netflow-original** | **netflow ipv4 record** [**peer**]}
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	flow monitor <i>monitor-name</i> Example: Router(config)# flow monitor FLOW-MONITOR-1	Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode. <ul style="list-style-type: none"> • This command also allows you to modify an existing flow monitor.
Step 4	description <i>text-string</i> Example: Router(config-flow-monitor)# description Used for monitoring IPv4 traffic	(Optional) Creates a description for the flow monitor.

	Command or Action	Purpose
Step 5	<pre>record {netflow-original netflow ipv4 record [peer]}</pre> <p>Example: Router(config-flow-monitor)# record netflow ipv4 original-input or</p> <p>Example: Router(config-flow-monitor)# record netflow-original</p>	Specifies the record for the flow monitor.
Step 6	<pre>end</pre> <p>Example: Router(config-flow-monitor)# end</p>	Exits flow monitor configuration mode and returns to privileged EXEC mode.

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.

Flow Monitors

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 flow record configuration mode.

Restrictions

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** *string*
5. **record netflow ipv6 record** [*peer*]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	flow monitor <i>monitor-name</i> Example: Router(config)# flow monitor FLOW-MONITOR-2	Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode. <ul style="list-style-type: none">This command also allows you to modify an existing flow monitor.
Step 4	description <i>string</i> Example: Router(config-flow-monitor)# description Used for monitoring IPv6 traffic	(Optional) Creates a description for the flow monitor.
Step 5	record netflow ipv6 <i>record</i> [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 flow monitor configuration mode and returns to privileged EXEC mode.

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, perform the following required task.

Restrictions

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 only for analyzing 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 only for analyzing output (egress) traffic.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **interface** *type number*
4. **ip flow monitor** *monitor-name* {**input** | **output**}
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Router(config)# interface ethernet 0/0	Specifies an interface and enters interface configuration mode.
Step 4	ip flow monitor <i>monitor-name</i> { input output } Example: Router(config-if)# ip flow monitor FLOW-MONITOR-1 input and/or Router(config-if)# ip flow monitor FLOW-MONITOR-1 output	Activates the flow monitor that you created previously by assigning it to the interface to analyze traffic. <ul style="list-style-type: none"> • You can configure input and output traffic analysis concurrently by configuring the ip flow monitor <i>monitor-name</i> input and ip flow monitor <i>monitor-name</i> 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.

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 IPv6 flow monitor, perform the following required task.

Restrictions

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**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Router(config)# interface ethernet 0/0	Specifies an interface and enters interface configuration mode.
Step 4	ipv6 flow monitor <i>monitor-name</i> { input output } Example: Router(config-if)# ipv6 flow monitor FLOW-MONITOR-2 input and/or Router(config-if)# ipv6 flow monitor FLOW-MONITOR-2 output	Activates the flow monitor that you created previously by assigning it to the interface to analyze traffic. <ul style="list-style-type: none"> • You can configure input and output traffic analysis concurrently by configuring the ipv6 flow monitor <i>monitor-name</i> input and ipv6 flow monitor <i>monitor-name</i> 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.

Verifying the Flow Monitor

To view the current status of a flow monitor and verify the configuration commands that you entered, perform the following optional task.

Prerequisites

The interface to which you applied the input flow monitor must be receiving traffic that meets the criteria defined by the NetFlow original record before you can view the flows in the flow monitor cache.

SUMMARY STEPS

1. **enable**
2. **show flow monitor**
3. **show running-config flow monitor**

DETAILED STEPS

Step 1 **enable**

The **enable** command enters privileged EXEC mode (enter the password if prompted).

```
Router> enable
```

```
Router#
```

Step 2 **show flow monitor**

The **show flow monitor** command shows the current status of the flow monitor that you specify.

```
Router# show flow monitor
```

```
Flow Monitor FLOW-MONITOR-1:
  Description:      Used for monitoring IPv4 traffic
  Flow Record:     netflow ipv4 original-input
  Cache:
    Type:           normal
    Status:         allocated
    Size:           4096 entries / 196620 bytes
    Inactive Timeout: 15 secs
    Active Timeout: 1800 secs
    Update Timeout: 1800 secs
```

```
Flow Monitor FLOW-MONITOR-2:
  Description:      Used for monitoring IPv6 traffic
  Flow Record:     netflow ipv6 original-input
  Cache:
    Type:           normal
    Status:         allocated
    Size:           4096 entries / 278544 bytes
    Inactive Timeout: 15 secs
    Active Timeout: 1800 secs
    Update Timeout: 1800 secs
```

Step 3 **show running-config flow monitor**

The **show running-config flow monitor** command shows the configuration commands of the flow monitor that you specify.

```
Router# show running-config flow monitor
```

```
Building configuration...
```

```
Current configuration:
!
flow monitor FLOW-MONITOR-1
  description Used for monitoring IPv4 traffic
  record netflow ipv4 original-input
!
flow monitor FLOW-MONITOR-2
  description Used for monitoring IPv6 traffic
  record netflow ipv6 original-input
```

```
!  
end
```

Verifying That Flexible NetFlow Is Enabled

To verify that Flexible NetFlow is enabled on an interface, perform the following optional task.

SUMMARY STEPS

1. **enable**
2. **show flow interface** *type number*

DETAILED STEPS

Step 1 **enable**

The **enable** command enters privileged EXEC mode (enter the password if prompted).

```
Router> enable
```

```
Router#
```

Step 2 **show flow interface** *type number*

The **show flow interface** command verifies that Flexible NetFlow is enabled on an interface.

```
Router# show flow interface ethernet 0/0
```

```
Interface Ethernet0/0  
  FNF:  monitor:      FLOW-MONITOR-1  
        direction:   Input  
        traffic(ip):  on  
  FNF:  monitor:      FLOW-MONITOR-2  
        direction:   Input  
        traffic(ipv6): on
```

Viewing the Flow Monitor Cache

To view the data in the flow monitor cache, perform the following optional task.

Prerequisites

The interface to which you applied the input flow monitor must be receiving traffic that meets the criteria defined by the NetFlow original record before you can view the flows in the flow monitor cache.

SUMMARY STEPS

1. **enable**
2. **show flow monitor name** *monitor-name* **cache format record**

DETAILED STEPS

Step 1 enable

The **enable** command enters privileged EXEC mode (enter the password if prompted).

```
Router> enable
```

```
Router#
```

Step 2 show flow monitor name *monitor-name* cache format record

The **show flow monitor name *monitor-name* cache format record** command string displays the status, statistics, and flow data in the cache for a flow monitor.

```
Router# show flow monitor name FLOW-MONITOR-1 cache format record
```

```
Cache type:                Normal
Cache size:                4096
Current entries:          1
High Watermark:           2
```

```
Flows added:              8
Flows aged:               7
  - Active timeout ( 1800 secs) 0
  - Inactive timeout ( 15 secs) 7
  - Event aged                0
  - Watermark aged            0
  - Emergency aged            0
```

```
IP DESTINATION AS:       0
IPV4 DESTINATION PREFIX: 172.16.10.0
IPV4 DESTINATION MASK:   /24
INTERFACE OUTPUT:        Et1/0
FLOW DIRECTION:          Input
counter bytes:           4292430
counter packets:         4305
timestamp first:         15853684
timestamp last:          15860868
```

```
Router# show flow monitor name FLOW-MONITOR-2 cache format record
```

```
Cache type:                Normal
Cache size:                4096
Current entries:          6
High Watermark:           8
```

```
Flows added:              1048
Flows aged:               1042
  - Active timeout ( 1800 secs) 11
  - Inactive timeout ( 15 secs) 1031
  - Event aged                0
  - Watermark aged            0
  - Emergency aged            0
```

```
IPV6 FLOW LABEL:         0
IPV6 EXTENSION MAP:      0x00000040
IPV6 SOURCE ADDRESS:     2001:DB8:1:ABCD::1
IPV6 DESTINATION ADDRESS: 2001:DB8:4:ABCD::2
TRNS SOURCE PORT:        3000
TRNS DESTINATION PORT:   55
INTERFACE INPUT:         Et0/0
FLOW DIRECTION:          Input
FLOW SAMPLER ID:         0
```

```

IP PROTOCOL:                17
IP TOS:                      0x00
ip source as:                0
ip destination as:           0
ipv6 next hop address:       ::
ipv6 source mask:            /48
ipv6 destination mask:      /0
tcp flags:                   0x00
interface output:            Null
counter bytes:                521192
counter packets:              9307
timestamp first:              9899684
timestamp last:               11660744
.
.
.
IPV6 FLOW LABEL:             0
IPV6 EXTENSION MAP:          0x00000000
IPV6 SOURCE ADDRESS:          FE80::A8AA:BBFF:FEBB:CC03
IPV6 DESTINATION ADDRESS:     FF02::9
TRNS SOURCE PORT:             521
TRNS DESTINATION PORT:        521
INTERFACE INPUT:              Et0/0
FLOW DIRECTION:               Input
FLOW SAMPLER ID:              0
IP PROTOCOL:                  17
IP TOS:                        0xE0
ip source as:                  0
ip destination as:             0
ipv6 next hop address:         ::
ipv6 source mask:              /10
ipv6 destination mask:        /0
tcp flags:                     0x00
interface output:              Null
counter bytes:                  92
counter packets:                1
timestamp first:                11653832
timestamp last:                 11653832

```

Configuration Examples for Configuring Flexible NetFlow with Predefined Records

This section provides the following configuration examples:

- [Configuring a Flexible NetFlow Predefined Record for IPv4 Traffic: Example, page 27](#)
- [Configuring a Flexible NetFlow Predefined Record for IPv6 Traffic: Example, page 28](#)

Configuring a Flexible NetFlow Predefined Record for IPv4 Traffic: Example

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 Ethernet0/0
 ip address 172.16.6.2 255.255.255.0
 ip flow monitor FLOW-MONITOR-1 input
!

```

Configuring a Flexible NetFlow Predefined Record for IPv6 Traffic: Example

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 Ethernet0/0
 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

The following sections provide references related to Flexible NetFlow.

Related Documents

Related Topic	Document Title
Cisco IOS commands	<i>Cisco IOS Master Commands List, All Releases</i>
Overview of Flexible NetFlow	“Cisco IOS Flexible NetFlow Overview”
Flexible NetFlow Feature Roadmap	“Cisco IOS Flexible NetFlow Features Roadmap”
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”
Configuring IPv4 Multicast Statistics Support for Flexible NetFlow	“Configuring IPv4 Multicast Statistics Support for Cisco IOS Flexible NetFlow”
Configuration commands for Flexible NetFlow	<i>Cisco IOS Flexible NetFlow Command Reference</i>

Standards

Standard	Title
There are no standards associated with this feature.	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 3954	<i>Cisco Systems NetFlow Services Export Version 9</i>

Technical Assistance

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

Feature Information for Flexible NetFlow

Table 18 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or Cisco IOS Releases 12.2(1) or 12.0(3)S or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Cisco IOS Flexible NetFlow Features Roadmap](#)”.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS, Catalyst OS, and Cisco IOS XE 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 18 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 18 Feature Information for Flexible NetFlow

Feature Name	Releases	Feature Configuration Information
Flexible NetFlow	12.4(9)T 12.2(33)SRC	<p>Flexible NetFlow is introduced.</p> <p>Support for this feature was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.</p> <p>Information about the Flexible NetFlow feature is included in the following sections:</p> <ul style="list-style-type: none"> • Prerequisites for Configuring Flexible NetFlow with Predefined Records, page 2 • Information About Configuring Flexible NetFlow with Predefined Records, page 2 • How to Configure Flexible NetFlow Using a Predefined Record for the Flow Monitor, page 18 • Configuration Examples for Configuring Flexible NetFlow with Predefined Records, page 27 <p>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 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 NetFlow), statistics packet, template data timeout, transport (Flexible NetFlow).</p>

Table 18 Feature Information for Flexible NetFlow

Feature Name	Releases	Feature Configuration Information
Flexible NetFlow—IPv6 Unicast Flows	12.4(20)T 12.2(33)SRE	<p>Enables Flexible NetFlow to monitor IPv6 traffic.</p> <p>Support for this feature was added for Cisco 7200 and 7300 NPE series routers in Cisco IOS Release 12.2(33)SRE.</p> <p>Information about the Flexible NetFlow—IPv6 Unicast Flows feature is included in the following sections:</p> <ul style="list-style-type: none"> • Configuring a Flow Monitor for IPv6 Traffic Using a Predefined Record, page 20 • Applying an IPv6 Flow Monitor to an Interface, page 22 • Configuring a Flexible NetFlow Predefined Record for IPv6 Traffic: Example, page 28 <p>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.</p>

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008–2009 Cisco Systems, Inc. All rights reserved.

