



Customizing Cisco IOS Flexible NetFlow Flow Records and Flow Monitors

First Published: June 19, 2006
Last Updated: October 2, 2009

This document contains information about and instructions for customizing Flexible NetFlow flow records and flow monitor requirements. If the tasks and configuration examples in the “[Getting Started with Configuring Cisco IOS Flexible NetFlow](#)” module and the “[Configuring Cisco IOS Flexible NetFlow with Predefined Records](#)” module were not suitable for your traffic analysis requirements, you can use the information and instructions in this document to customize Flexible NetFlow to meet your traffic analysis requirements.

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 21.

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.



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

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

Contents

- [Prerequisites for Customizing Flexible NetFlow Flow Records and Flow Monitors, page 2](#)
- [Restrictions for Customizing Flexible NetFlow Flow Records and Flow Monitors, page 3](#)
- [Information About Customizing Flexible NetFlow Flow Records and Flow Monitors, page 3](#)
- [How to Customize Flexible NetFlow Flow Records and Flow Monitors, page 4](#)
- [Configuration Examples for Customizing Flexible NetFlow Flow Records and Flow Monitors, page 16](#)
- [Where to Go Next, page 20](#)
- [Additional References, page 20](#)
- [Feature Information for Flexible NetFlow, page 21](#)

Prerequisites for Customizing Flexible NetFlow Flow Records and Flow Monitors

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.
- You are familiar with the Flexible NetFlow key fields as they are defined in the following commands in the *Cisco IOS Flexible NetFlow Command Reference*:
 - **match flow**
 - **match interface**
 - **match {ipv4 | ipv6}**
 - **match routing**
 - **match transport**
- You are familiar with the Flexible NetFlow non-key fields as they are defined in the following commands in the *Cisco IOS Flexible NetFlow Command Reference*:
 - **collect counter**
 - **collect flow**
 - **collect interface**
 - **collect {ipv4 | ipv6}**
 - **collect routing**
 - **collect timestamp sys-uptime**
 - **collect transport**
- 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).

Restrictions for Customizing Flexible NetFlow Flow Records and Flow Monitors

The following restrictions apply to customizing Flexible NetFlow flow records and flow monitors:

- The Configuring Flexible NetFlow—Ingress VRF Support feature supports VRFs configured on the incoming interface. In the case where VRFs are associated with an interface via methods such as VRF Selection Using Policy Based Routing/ Source IP Address, a VRF ID of 0 will be recorded. If a packet arrives on an interface that does not belong to a VRF, a VRF ID of 0 is recorded.

Information About Customizing Flexible NetFlow Flow Records and Flow Monitors

Before you customize Flexible NetFlow flow records and flow monitors, you must understand the following concept:

- [Identifying the Types of Traffic That You Want to Analyze, page 3](#)

Identifying the Types of Traffic That You Want to Analyze

If the predefined Flexible NetFlow records are not suitable for your traffic requirements, you can create a user-defined (custom) record using the Flexible NetFlow **collect** and **match** commands. Before you can create a customized record, you must decide the criteria that you are going to use for the key and non-key fields.

If you want to create a customized record for detecting network attacks, you must include the appropriate key and non-key fields in the record to ensure that the router creates the flows and captures the data that you need to analyze the attack and respond to it. For example, SYN flood attacks are a common denial of service (DoS) attack in which TCP flags are used to flood open TCP requests to a destination host. When a normal TCP connection starts, a destination host receives a SYN (synchronize/start) packet from a source host and sends back a SYN ACK (synchronize acknowledge). The destination host must then hear an ACK (acknowledge) of the SYN ACK before the connection is established. This is referred to as the "TCP three-way handshake." While waiting for the ACK to the SYN ACK, a connection queue of finite size on the destination host keeps track of connections waiting to be completed. This queue typically empties quickly since the ACK is expected to arrive a few milliseconds after the SYN ACK. The TCP SYN attack exploits this design by having an attacking source host generate TCP SYN packets with random source addresses toward a victim host. The victim destination host sends a SYN ACK back to the random source address and adds an entry to the connection queue. Since the SYN ACK is destined for an incorrect or non-existent host, the last part of the "three-way handshake" is never completed and

the entry remains in the connection queue until a timer expires, typically for about one minute. By generating phony TCP SYN packets from random IP addresses at a rapid rate, it is possible to fill up the connection queue and deny TCP services (such as e-mail, file transfer, or WWW) to legitimate users.

The information needed for a security monitoring record for this type of DoS attack might include the following key and non-key fields:

- Key fields:
 - Destination IP address or destination IP subnet
 - TCP flags
 - Packet count
- Non-key fields
 - Destination IP address
 - Source IP address
 - Interface input and output

**Tip**

Many users configure a general Flexible NetFlow monitor that triggers a more detailed Flexible NetFlow view of a DoS attack using these key and non-key fields.

How to Customize Flexible NetFlow Flow Records and Flow Monitors

The tasks in this section explain how to do the following:

- Customize a Flexible NetFlow flow record.
- Customize a Flexible NetFlow flow monitor.
- Enable Flexible NetFlow.

**Note**

Only the keywords and arguments required for the Flexible NetFlow commands used in these tasks are explained in these tasks. For information about the other keywords and arguments available for these Flexible NetFlow commands, refer to the [Cisco IOS Flexible NetFlow Command Reference](#).

To customize Flexible NetFlow flow records and flow monitors, and to enable Flexible NetFlow, perform the following tasks:

- [Configuring a Customized Flow Record, page 5](#)
- [Verifying the Flow Record, page 8](#) (optional)
- [Customizing a Flow Monitor, page 9](#)
- [Verifying the Flow Monitor, page 11](#) (optional)
- [Applying a Flow Monitor to an Interface, page 12](#)
- [Verifying That Flexible NetFlow Is Enabled, page 14](#) (optional)
- [Viewing the Flow Monitor Cache, page 14](#) (optional)

Configuring a Customized Flow Record

Customized flow records are used to analyze traffic data for a specific purpose. A customized flow record must have at least one **match** criterion for use as the key field and typically has at least one **collect** criterion for use as a non-key field.

There are hundreds of possible permutations of customized flow records. This task explains the steps that are used to create one of the possible permutations. Modify the steps in these tasks as appropriate to create a customized flow record for your requirements.

To configure a customized flow record, perform either of the following tasks:

- [Configuring a Customized Flow Record for IPv4 Traffic](#)
- [Configuring a Customized Flow Record for IPv6 Traffic](#)

Configuring a Customized Flow Record for IPv4 Traffic

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow record** *flow-record-name*
4. **description** *string*
5. **match ipv4** {**destination** | **source**} **address**
6. Repeat Step 5 as required to configure additional key fields for the record.
7. **collect ipv4 source** {**address** | **mask** [**minimum-mask** *mask*] | **prefix** [**minimum-mask** *mask*]}
8. Repeat Step 7 as required to configure additional non-key fields for the record
9. **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 record <i>flow-record-name</i> Example: Router(config)# flow record FLOW-RECORD-1	Creates a flow record and enters flow record configuration mode. <ul style="list-style-type: none"> • This command also allows you to modify an existing flow record. For example, to modify the configuration of a flow record named “record-name” use the flow record <i>record-name</i> command and argument in global configuration mode.

	Command or Action	Purpose
Step 4	<p>description <i>string</i></p> <p>Example: Router(config-flow-record)# description Used for basic traffic analysis</p>	(Optional) Creates a description for the flow record.
Step 5	<p>match ipv4 {destination source} address</p> <p>Example: Router(config-flow-record)# match ipv4 destination address</p>	<p>Configures a key field for the flow record.</p> <p>Note This example configures the IPv4 destination address as a key field for the record. For information about the other key fields available for the match ipv4 command, and the other match commands that are available to configure key fields, refer to the Cisco IOS Flexible NetFlow Command Reference.</p>
Step 6	Repeat Step 5 as required to configure additional key fields for the record.	—
Step 7	<p>collect ipv4 source {address mask [minimum-mask <i>mask</i>] prefix [minimum-mask <i>mask</i>] }</p> <p>Example: Router(config-flow-record)# collect ipv4 source address</p>	<p>Configures one or more of the IPv4 source fields in the flow as a non-key field for the record.</p> <p>Note This example configures the IPv4 source address as a non-key field for the record. For information on the other collect commands that are available to configure non-key fields, refer to the Cisco IOS Flexible NetFlow Command Reference.</p>
Step 8	Repeat Step 7 as required to configure additional non-key fields for the record.	—
Step 9	<p>end</p> <p>Example: Router(config-flow-record)# end</p>	Exits flow record configuration mode and returns to privileged EXEC mode.

Configuring a Customized Flow Record for IPv6 Traffic

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow record** *flow-record-name*
4. **description** *string*
5. **match ipv6** {**destination** | **source**} **address**
6. Repeat Step 5 as required to configure additional key fields for the record.
7. **collect ipv6 source** {**address** | **mask** [**minimum-mask** *mask*] | **prefix** [**minimum-mask** *mask*] }
8. Repeat Step 7 as required to configure additional non-key fields for the record
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>flow record <i>flow-record-name</i></p> <p>Example: Router(config)# flow record FLOW-RECORD-2</p>	<p>Creates a flow record and enters flow record configuration mode.</p> <ul style="list-style-type: none"> This command also allows you to modify an existing flow record. For example, to modify the configuration of a flow record named “record-name” use the flow record <i>record-name</i> command and argument in global configuration mode.
Step 4	<p>description <i>string</i></p> <p>Example: Router(config-flow-record)# description Used for basic IPv6 traffic analysis</p>	<p>(Optional) Creates a description for the flow record.</p>
Step 5	<p>match ipv6 (<i>destination</i> <i>source</i>) <i>address</i></p> <p>Example: Router(config-flow-record)# match ipv6 destination address</p>	<p>Configures a key field for the flow record.</p> <p>Note This example configures the IPv6 destination address as a key field for the record. For information about the other key fields available for the match ipv6 command, and the other match commands that are available to configure key fields, refer to the Cisco IOS Flexible NetFlow Command Reference.</p>
Step 6	<p>Repeat Step 5 as required to configure additional key fields for the record.</p>	—
Step 7	<p>collect ipv6 source [<i>address</i> <i>mask</i> [<i>minimum-mask</i> <i>mask</i>] <i>prefix</i> [<i>minimum-mask</i> <i>mask</i>]]</p> <p>Example: Router(config-flow-record)# collect ipv6 source address</p>	<p>Configures the number of packets in the flow as a non-key field for the record.</p> <p>Note This example configures the IPv6 source address as a non-key field for the record. For information about the other collect commands that are available to configure non-key fields, refer to the Cisco IOS Flexible NetFlow Command Reference.</p>
Step 8	<p>Repeat Step 7 as required to configure additional non-key fields for the record.</p>	—
Step 9	<p>end</p> <p>Example: Router(config-flow-record)# end</p>	<p>Exits flow record configuration mode and returns to privileged EXEC mode.</p>

Verifying the Flow Record

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

SUMMARY STEPS

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

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

```
Router# show flow record
```

```
flow record FLOW-RECORD-2:
  Description:      Used for basic IPv6 traffic analysis
  No. of users:    1
  Total field space: 53 bytes
  Fields:
    match ipv6 destination address
    collect ipv6 protocol
    collect ipv6 source address
    collect transport source-port
    collect transport destination-port
    collect counter bytes
    collect counter packets
    collect timestamp sys-uptime first
    collect timestamp sys-uptime last
```

```
flow record FLOW-RECORD-1:
  Description:      Used for basic IPv4 traffic analysis
  No. of users:    1
  Total field space: 29 bytes
  Fields:
    match ipv4 destination address
    collect ipv4 protocol
    collect ipv4 source address
    collect transport source-port
    collect transport destination-port
    collect counter bytes
    collect counter packets
    collect timestamp sys-uptime first
    collect timestamp sys-uptime last
```

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

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

```
Router# show running-config flow record

Current configuration:
!
flow record FLOW-RECORD-2
  description Used for basic IPv6 traffic analysis
  match ipv6 destination address
  collect ipv6 protocol
  collect ipv6 source address
  collect transport source-port
  collect transport destination-port
  collect counter bytes
  collect counter packets
  collect timestamp sys-uptime first
  collect timestamp sys-uptime last
!
!
flow record FLOW-RECORD-1
  description Used for basic IPv4 traffic analysis
  match ipv4 destination address
  collect ipv4 protocol
  collect ipv4 source address
  collect transport source-port
  collect transport destination-port
  collect counter bytes
  collect counter packets
  collect timestamp sys-uptime first
  collect timestamp sys-uptime last
!
```

Customizing a Flow Monitor

To create a customized flow monitor, perform the following required task.

Flow Monitor

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. These record formats can be one of the predefined formats, or an advanced user can create a customized format using the **flow record** command. This task uses the record that you created in the [“Configuring a Customized Flow Record”](#) section on page 5.

Prerequisites

If you want to use a customized record instead of using one of the Flexible NetFlow predefined records, you must create the customized record before you can perform this task. Refer to the [“Configuring a Customized Flow Record”](#) section on page 5 for information about and instructions for creating a customized flow record.

If you want to add a flow exporter to the flow monitor for data export, you must create the exporter before you can complete this task. Refer to the [“Configuring Data Export for Cisco IOS Flexible NetFlow with Flow Exporters”](#) module for information about and instructions for creating a flow exporter.

Restrictions

You must use the **no ip flow monitor** command to remove a flow monitor from all of the interfaces to which you have applied it before you can modify the parameters for the **record** command on the flow monitor. For information about the **ip flow monitor** command, refer to the [Cisco IOS Flexible NetFlow Command Reference](#).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow monitor** *monitor-name*
4. **description** *string*
5. **record** {*record-name* | **netflow-original** | **netflow** {**ipv4** | **ipv6**} *record* [**peer**]}
6. **cache** {**entries** *entries* | **timeout** {**active** *active* | **inactive** *inactive* | **update** *update*} | **type** {**immediate** | **normal** | **permanent**}}
7. Repeat Step 6 as required to finish modifying the cache parameters for this flow monitor.
8. **statistics packet protocol**
9. **statistics packet size**
10. **exporter** *exporter-name*
11. **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. For example, to modify the configuration of a flow monitor named “monitor-name”, use the flow monitor <i>monitor-name</i> command and argument in global configuration mode.
Step 4	description <i>string</i> Example: Router(config-flow-monitor)# description Used for basic ipv4 traffic analysis	(Optional) Creates a description for the flow monitor.

	Command or Action	Purpose
Step 5	<p>record {<i>record-name</i> netflow-original netflow {ipv4 ipv6} <i>record</i> [peer]}</p> <p>Example: Router(config-flow-monitor)# record FLOW-RECORD-1</p>	Specifies the record for the flow monitor.
Step 6	<p>cache {entries <i>entries</i> timeout {active <i>active</i> inactive <i>inactive</i> update <i>update</i>} type {immediate normal permanent}}</p> <p>Example: Router(config-flow-monitor)# cache entries 1000</p>	<p>(Optional) Modifies the flow monitor cache parameters such as timeout values, number of cache entries, and the cache type.</p> <ul style="list-style-type: none"> The timeout keywords do not have any effect when the cache type is set to immediate.
Step 7	Repeat Step 6 as required to finish modifying the cache parameters for this flow monitor.	—
Step 8	<p>statistics packet protocol</p> <p>Example: Router(config-flow-monitor)# statistics packet protocol</p>	(Optional) Enables the collection of protocol distribution statistics for Flexible NetFlow monitors.
Step 9	<p>statistics packet size</p> <p>Example: Router(config-flow-monitor)# statistics packet size</p>	(Optional) Enables the collection of size distribution statistics for Flexible NetFlow monitors.
Step 10	<p>exporter <i>exporter-name</i></p> <p>Example: Router(config-flow-monitor)# exporter EXPORTER-1</p>	<p>(Optional) Specifies the name of an exporter that was created previously.</p> <ul style="list-style-type: none"> Refer to the “Configuring Data Export for Cisco IOS Flexible NetFlow with Flow Exporters” module for information about and instructions for configuring flow exporters.
Step 11	<p>end</p> <p>Example: Router(config-flow-monitor)# end</p>	Exits flow monitor 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.

SUMMARY STEPS

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

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** *monitor-name*

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

```
Router# show flow monitor FLOW-MONITOR-1
```

```
Flow Monitor FLOW-MONITOR-1:
  Description:      Used for basic ipv4 traffic analysis
  Flow Record:      FLOW-RECORD-1
  Flow Exporter:    EXPORTER-1
  Cache:
    Type:            normal
    Status:          allocated
    Size:            1000 entries / 50052 bytes
    Inactive Timeout: 15 secs
    Active Timeout:  1800 secs
    Update Timeout:  1800 secs
  Stats:
    protocol distribution
    size distribution
```

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 FLOW-MONITOR-1
```

```
Current configuration:
!
flow monitor FLOW-MONITOR-1
description Used for basic ipv4 traffic analysis
record FLOW-RECORD-1
exporter EXPORTER-1
cache entries 1000
statistics packet protocol
statistics packet size
!
```

Applying a Flow Monitor to an Interface

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

Restrictions

When you specify the “NetFlow original” or the “NetFlow IPv4 original input” or the “NetFlow IPv6 original input” predefined record for the flow monitor to emulate original NetFlow, the Flexible NetFlow flow monitor can be used only for analyzing input (ingress) traffic.

When you specify the “NetFlow IPv4 original output” or the “NetFlow IPv6 original output” predefined record for the flow monitor to emulate the Egress NetFlow Accounting feature, the Flexible NetFlow flow monitor can be used only for analyzing output (egress) traffic.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **{ip | ipv6} flow monitor** *monitor-name* **{input | output}**
5. Repeat Steps 3 and 4 to activate a flow monitor on any other interfaces in the router over which you want to monitor traffic.
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	interface <i>type number</i> Example: Router(config)# interface ethernet 0/0	Specifies an interface and enters interface configuration mode.
Step 4	{ip ipv6} flow monitor <i>monitor-name</i> {input output} Example: Router(config-if)# ip flow monitor FLOW-MONITOR-1 input	Activates a flow monitor that was created previously by assigning it to the interface to analyze traffic.
Step 5	Repeat Steps 3 and 4 to activate a flow monitor on any other interfaces in the router over which you want to monitor traffic.	—
Step 6	end Example: Router(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.

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**

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**

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
```

```
Router# show flow interface ethernet 1/0
```

```
Interface Ethernet1/0
  FNF: monitor:      FLOW-MONITOR-1
        direction:   Output
        traffic(ip):  on
  FNF: monitor:      FLOW-MONITOR-2
        direction:   Output
        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 on 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:                               1000
Current entries:                           4
High Watermark:                            4
```

```
Flows added:                               101
Flows aged:                                97
- Active timeout ( 1800 secs)              3
- Inactive timeout ( 15 secs)              94
- Event aged                               0
- Watermark aged                           0
- Emergency aged                           0
```

```
IPV4 DESTINATION ADDRESS: 172.16.10.5
ipv4 source address:      10.10.11.1
trns source port:        25
trns destination port:   25
counter bytes:           72840
counter packets:         1821
timestamp first:         21237828
timestamp last:          22086520
ip protocol:             6
```

```
IPV4 DESTINATION ADDRESS: 172.16.10.2
ipv4 source address:      10.10.10.2
trns source port:        20
trns destination port:   20
counter bytes:           3913860
counter packets:         7326
timestamp first:         21238788
timestamp last:          22088080
ip protocol:             6
```

```
IPV4 DESTINATION ADDRESS: 172.16.10.200
ipv4 source address:      192.168.67.6
trns source port:        0
trns destination port:   3073
counter bytes:           51072
counter packets:         1824
timestamp first:         21239228
```

```

timestamp last:          22087980
ip protocol:            1

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

Cache type:              Normal
Cache size:              1000
Current entries:         2
High Watermark:         3

Flows added:            95
Flows aged:             93
- Active timeout ( 1800 secs) 0
- Inactive timeout ( 15 secs) 93
- Event aged              0
- Watermark aged          0
- Emergency aged          0

IPV6 DESTINATION ADDRESS: 2001:DB8:4:ABCD::2
ipv6 source address:     2001:DB8:1:ABCD::1
trns source port:       33572
trns destination port:  23
counter bytes:          19140
counter packets:        349
timestamp first:        2172704
timestamp last:         2198272
ip protocol:            6

IPV6 DESTINATION ADDRESS: FF02::9
ipv6 source address:     FE80::A8AA:BBFF:FEBB:CC03
trns source port:       521
trns destination port:  521
counter bytes:          92
counter packets:        1
timestamp first:        2195672
timestamp last:         2195672
ip protocol:            17

```

Configuration Examples for Customizing Flexible NetFlow Flow Records and Flow Monitors

This section contains the following configuration examples:

- [Configuring a Permanent Flow Record Cache with a Limited Number of Possible Flows: Example, page 17](#)
- [Configuring a Customized Flow Record Cache for Monitoring IPv6 Traffic: Example, page 18](#)
- [Configuring Flexible NetFlow for Monitoring MAC and VLAN Statistics: Example, page 18](#)
- [Configuring Flexible NetFlow for Ingress VRF Support: Example, page 19](#)
- [Configuring Flexible NetFlow for Network Based Application Recognition \(NBAR\) : Example, page 19](#)

Configuring a Permanent Flow Record Cache with a Limited Number of Possible Flows: Example

The following example is designed to monitor the type of service (ToS) field usage on all interfaces in the router. An exporter is not configured because this example is intended to be used to capture additional data for analysis on the router using the **show flow monitor** command.

This sample starts in global configuration mode:

```
!  
ip cef  
!  
flow record QOS_RECORD  
  description UD: Flow Record to monitor the use of TOS within this router/network  
  match interface input  
  match interface output  
  match ipv4 tos  
  collect counter packets  
  collect counter bytes  
  exit  
!  
flow monitor QOS_MONITOR  
  description UD: Flow Monitor which watches the limited combinations of interface and TOS  
  record QOS_RECORD  
  cache type permanent  
  cache entries 8192    ! 2^5 (combos of interfaces) * 256 (values of TOS)  
  exit  
!  
interface ethernet0/0  
  ip flow monitor QOS_MONITOR input  
  exit  
!  
interface ethernet0/1  
  ip flow monitor QOS_MONITOR input  
  exit  
!  
interface ethernet0/2  
  ip flow monitor QOS_MONITOR input  
  exit  
!  
interface serial2/0  
  ip flow monitor QOS_MONITOR input  
  exit  
!  
interface serial2/1  
  ip flow monitor QOS_MONITOR input  
  exit  
!
```

The display from the **show flow monitor** command shows the current status of the cache.

```
Router# show flow monitor QOS_MONITOR cache  
Cache type:                Permanent  
Cache size:                 8192  
Current entries:           2  
High Watermark:           2  
  
Flows added:                2  
Updates sent                ( 1800 secs) 0
```

Configuring a Customized Flow Record Cache for Monitoring IPv6 Traffic: Example

The following example creates a customized flow record for monitoring common IPv6 traffic characteristics.

This sample starts in global configuration mode:

```
!
ip cef
ipv6 cef
!
flow record FLOW-RECORD-2
description Used for basic IPv6 traffic analysis
match ipv6 destination address
collect ipv6 protocol
collect ipv6 source address
collect transport source-port
collect transport destination-port
collect counter bytes
collect counter packets
collect timestamp sys-uptime first
collect timestamp sys-uptime last
!
flow monitor FLOW-MONITOR-2
description Used for basic IPv6 traffic analysis
record FLOW-RECORD-2
cache entries 1000
statistics packet protocol
statistics packet size
!
interface Ethernet0/0
ipv6 address 2001:DB8:2:ABCD::2/48
ipv6 flow monitor FLOW-MONITOR-2 input
!
interface Ethernet1/0
ipv6 address 2001:DB8:3:ABCD::1/48
ipv6 flow monitor FLOW-MONITOR-2 output
!
```

Configuring Flexible NetFlow for Monitoring MAC and VLAN Statistics: Example

The following example shows how to configure Flexible NetFlow for monitoring MAC and VLAN statistics.

This sample starts in global configuration mode:

```
!
flow record LAYER-2-FIELDS-1
match ipv4 source address
match ipv4 destination address
collect datalink dot1q vlan output
collect datalink mac source address input
collect datalink mac source address output
collect datalink mac destination address input
collect flow direction
collect counter bytes
collect counter packets
```

```
!
  exit
!
!
flow monitor FLOW-MONITOR-4
  record LAYER-2-FIELDS-1
  exit
!
ip cef
!
interface Ethernet0/0
  ip address 172.16.6.2 255.255.255.0
  ip flow monitor FLOW-MONITOR-1 input
!
```

Configuring Flexible NetFlow for Ingress VRF Support: Example

The following example configures the collection of the virtual route forwarding (VRF) ID from incoming packets on a router by applying an input flow monitor having a flow record that collects the VRF ID as a key field.

This sample starts in global configuration mode:

```
!
flow record rm_1
match routing vrf input
match ipv4 source address
match ipv4 destination address
collect interface input
collect interface output
collect counter packets
!
flow monitor mm_1
record rm_1
!
interface Serial2/0
ip vrf forwarding green
ip address 172.16.2.2 255.255.255.252
ip flow monitor mm_1 output
!
end
```

Configuring Flexible NetFlow for Network Based Application Recognition (NBAR) : Example

The following example creates different flows for each application seen between any two IP hosts by applying a flow monitor having a flow record that collects the application name as a key field.

This sample starts in global configuration mode:

```
!
flow record rm_1
match application name
match ipv4 source address
match ipv4 destination address
collect interface input
collect interface output
collect counter packets
!
```

```

flow monitor mm_1
record rm_1
!
interface FastEthernet0/0
ip address 172.16.2.2 255.255.255.0
ip flow monitor mm_1 input
!
end

```

Where to Go Next

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.

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 any of the predefined records for Flexible NetFlow, refer to the [“Configuring Cisco IOS Flexible NetFlow with Predefined Records”](#) module.

Additional References

The following sections provide references related to Flexible NetFlow.

Related Documents

Related Topic	Document Title
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”
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”
Configuring Flexible NetFlow using predefined records	“Configuring Cisco IOS Flexible NetFlow with Predefined Records”
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>	http://www.cisco.com/techsupport

Feature Information for Flexible NetFlow

Table 1 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 1](#) 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 1 Feature Information for Flexible NetFlow

Feature Name	Releases	Feature Configuration Information
Flexible NetFlow	12.4(9)T	<p>Flexible NetFlow is introduced.</p> <p>Information about the Flexible NetFlow feature is included in the following sections:</p> <ul style="list-style-type: none"> • Prerequisites for Customizing Flexible NetFlow Flow Records and Flow Monitors, page 2 • Information About Customizing Flexible NetFlow Flow Records and Flow Monitors, page 3 • How to Customize Flexible NetFlow Flow Records and Flow Monitors, page 4 • Configuration Examples for Customizing Flexible NetFlow Flow Records and Flow Monitors, page 16 <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 1 Feature Information for Flexible NetFlow

Feature Name	Releases	Feature Configuration Information
Flexible NetFlow - IPv4 Unicast Flows	12.4(9)T	<p>Enables Flexible NetFlow to monitor IPv4 traffic.</p> <p>Information about the Flexible NetFlow - IPv4 Unicast Flows feature is included in the following sections:</p> <ul style="list-style-type: none"> • Configuring a Customized Flow Record for IPv4 Traffic, page 5 • Applying a Flow Monitor to an Interface, page 12 <p>The following commands were introduced or modified: collect routing, debug flow record, collect ipv4, collect ipv4 destination, collect ipv4 fragmentation, collect ipv4 section, collect ipv4 source, ip flow monitor, match ipv4, match ipv4 destination, match ipv4 fragmentation, match ipv4 section, match ipv4 source, match routing, record, show flow monitor, show flow record.</p>
Flexible Netflow - Layer 2 Fields	12.4(22)T	<p>Enables collecting statistics for Layer 2 fields such as MAC addresses and virtual LAN (VLAN) IDs from traffic.</p> <p>Information about the Flexible NetFlow - Layer 2 Fields feature is included in the following sections:</p> <ul style="list-style-type: none"> • Configuring Flexible NetFlow for Monitoring MAC and VLAN Statistics: Example, page 18 <p>The following commands were introduced or modified: collect datalink dot1q vlan, collect datalink mac, match datalink dot1q vlan, match datalink mac.</p>
Flexible NetFlow - IPv6 Unicast Flows	12.4(20)T	<p>Enables Flexible NetFlow to monitor IPv6 traffic.</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 Customized Flow Record for IPv6 Traffic, page 6 • Applying a Flow Monitor to an Interface, page 12 • Configuring a Customized Flow Record Cache for Monitoring IPv6 Traffic: Example, page 18 <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>

Table 1 Feature Information for Flexible NetFlow

Feature Name	Releases	Feature Configuration Information
Flexible Netflow—Ingress VRF Support	15.0(1)M	<p>Enables collecting the virtual route forwarding (VRF) ID from incoming packets on a router by applying an input flow monitor having a flow record that collects the VRF ID as a key or a non-key field.</p> <p>Information about the Flexible Netflow—Ingress VRF Support feature is included in the following sections:</p> <ul style="list-style-type: none"> • Restrictions for Customizing Flexible NetFlow Flow Records and Flow Monitors, page 3 • Configuring Flexible NetFlow for Ingress VRF Support: Example, page 19 <p>The following commands were introduced or modified: collect routing, match routing, option (Flexible Netflow), show flow monitor.</p>
Flexible Netflow—NBAR Application Recognition	15.0(1)M	<p>Enables creation of different flows for each application seen between any two IP hosts by applying a flow monitor having a flow record that collects the application name as a key or a non-key field.</p> <p>Information about the NBAR Application Recognition feature is included in the following sections:</p> <ul style="list-style-type: none"> • Configuring Flexible NetFlow for Network Based Application Recognition (NBAR) : Example, page 19 <p>The following commands were introduced or modified: collect application name, match application name, option (Flexible Netflow), show flow monitor.</p>

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, 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, and Flip Gift Card 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 Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, 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. (0908R)

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.