Flexible NetFlow—IPv4 Unicast Flows

Last Updated: NaN, yyyy

The Flexible Netflow—IPv4 Unicast Flows feature enables Flexible NetFlow to monitor IPv4 traffic.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Information About Flexible NetFlow IPv4 Unicast Flows

Flexible NetFlow—IPv4 Unicast Flows Overview

This feature enables Flexible NetFlow to monitor IPv4 traffic.

How to Configure Flexible NetFlow IPv4 Unicast Flows

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

Configuring a Customized Flow Record

Perform this task to configure 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 nonkey field.

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow record** *record-name*
4. **description** *description*
5. **match** {**ipv4** | **ipv6**}{**destination** | **source**} **address**
6. Repeat Step 5 as required to configure additional key fields for the record.
7. **collect interface** {**input** | **output**}
8. Repeat Step 7 as required to configure additional nonkey fields for the record.
9. **end**
10. **show flow record** *record-name*
11. **show running-config flow record** *record-name*

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**flow record** *record-name* **Example:** `Device(config)# flow record FLOW-RECORD-1`	Creates a flow record and enters Flexible NetFlow flow record configuration mode. • This command also allows you to modify an existing flow record.
Step 4	**description** *description* **Example:** `Device(config-flow-record)# description Used for basic traffic analysis`	(Optional) Creates a description for the flow record.
Step 5	**match** {**ipv4** | **ipv6**}{**destination** | **source**} **address** **Example:** `Device(config-flow-record)# match ipv4 destination address`	Configures a key field for the flow record. **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* .
Step 6	Repeat Step 5 as required to configure additional key fields for the record.	—
Step 7	**collect interface** {**input** | **output**} **Example:** `Device(config-flow-record)# collect interface input`	Configures the input interface as a nonkey field for the record. **Note** This example configures the input interface as a nonkey field for the record. For information on the other **collect** commands that are available to configure nonkey fields, refer to the *Cisco IOS Flexible NetFlow Command Reference*.
Step 8	Repeat Step 7 as required to configure additional nonkey fields for the record.	—
Step 9	**end** **Example:** `Device(config-flow-record)# end`	Exits Flexible NetFlow flow record configuration mode and returns to privileged EXEC mode.
Step 10	**show flow record** *record-name* **Example:** `Device# show flow record FLOW_RECORD-1`	(Optional) Displays the current status of the specified flow record.

	Command or Action	Purpose
Step 11	**show running-config flow record** *record-name* **Example:** `Device# show running-config flow record FLOW_RECORD-1`	(Optional) Displays the configuration of the specified flow record.

Configuring the Flow Exporter

To configure the flow exporter, perform the following required task.

Note Each flow exporter supports only one destination. If you want to export the data to multiple destinations, you must configure multiple flow exporters and assign them to the flow monitor.

You can export to a destination using either an IPv4 or IPv6 address.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow exporter** *exporter-name*
4. **description** *description*
5. **destination** {*ip-address* | *hostname*} [**vrf** *vrf-name*]
6. **export-protocol** {**netflow-v5** | **netflow-v9** | **ipfix**}
7. **dscp** *dscp*
8. **source** *interface-type interface-number*
9. **option** {**exporter-stats** | **interface-table** | **sampler-table**| **vrf-table**} [**timeout** *seconds*]
10. **output-features**
11. **template data timeout** *seconds*
12. **transport udp** *udp-port*
13. **ttl** *seconds*
14. **end**
15. **show flow exporter** *exporter-name*
16. **show running-config flow exporter** *exporter-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**flow exporter** *exporter-name* **Example:** `Device(config)# flow exporter EXPORTER-1`	Creates the flow exporter and enters Flexible NetFlow flow exporter configuration mode. • This command also allows you to modify an existing flow exporter.
Step 4	**description** *description* **Example:** `Device(config-flow-exporter)# description Exports to the datacenter`	(Optional) Configures a description to the exporter that will appear in the configuration and the display of the **show flow exporter** command.
Step 5	**destination** {*ip-address* | *hostname*} [**vrf** *vrf-name*] **Example:** `Device(config-flow-exporter)# destination 172.16.10.2`	Specifies the IP address or hostname of the destination system for the exporter. **Note** You can export to a destination using either an IPv4 or IPv6 address.
Step 6	**export-protocol** {**netflow-v5** | **netflow-v9** | **ipfix**} **Example:** `Device(config-flow-exporter)# export-protocol netflow-v9`	Specifies the version of the NetFlow export protocol used by the exporter. The export of extracted fields from NBAR is supported only over IPFIX. • Default: **netflow-v9**.
Step 7	**dscp** *dscp* **Example:** `Device(config-flow-exporter)# dscp 63`	(Optional) Configures differentiated services code point (DSCP) parameters for datagrams sent by the exporter. • The range for the *dscp* argument is from 0 to 63. Default: 0.

	Command or Action	Purpose
Step 8	**source** *interface-type interface-number* **Example:** `Device(config-flow-exporter)# source ethernet 0/0`	(Optional) Specifies the local interface from which the exporter will use the IP address as the source IP address for exported datagrams.
Step 9	**option** {**exporter-stats** | **interface-table** | **sampler-table**| **vrf-table**} [**timeout** *seconds*] **Example:** `Device(config-flow-exporter)# option exporter-stats timeout 120`	(Optional) Configures options data parameters for the exporter. • You can configure all three options concurrently. • The range for the *seconds* argument is 1 to 86,400. Default: 600.
Step 10	**output-features** **Example:** `Device(config-flow-exporter)# output-features`	(Optional) Enables sending export packets using quality of service (QoS) and encryption.
Step 11	**template data timeout** *seconds* **Example:** `Device(config-flow-exporter)# template data timeout 120`	(Optional) Configure resending of templates based on a timeout. • The range for the *seconds* argument is 1 to 86400 (86400 seconds = 24 hours).
Step 12	**transport udp** *udp-port* **Example:** `Device(config-flow-exporter)# transport udp 650`	Specifies the UDP port on which the destination system is listening for exported datagrams. • The range for the *udp-port* argument is from 1 to 65536.
Step 13	**ttl** *seconds* **Example:** `Device(config-flow-exporter)# ttl 15`	(Optional) Configures the time-to-live (TTL) value for datagrams sent by the exporter. • The range for the *seconds* argument is from 1 to 255.
Step 14	**end** **Example:** `Device(config-flow-exporter)# end`	Exits flow exporter configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
Step 15	**show flow exporter** *exporter-name* **Example:** `Device# show flow exporter FLOW_EXPORTER-1`	(Optional) Displays the current status of the specified flow exporter.
Step 16	**show running-config flow exporter** *exporter-name* **Example:** `Device# show running-config flow exporter FLOW_EXPORTER-1`	(Optional) Displays the configuration of the specified flow exporter.

Creating a Customized Flow Monitor

Perform this required task to create a customized 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.

An advanced user can create a customized format using the **flow record** command.

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.

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.

Note 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** *description*
5. **record** {*record-name* | **netflow-original** | **netflow** {**ipv4** | **ipv6**} *record* [**peer**]}
6. **cache** {**entries** *number* | **timeout** {**active** | **inactive** | **update**} *seconds* | **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**
12. **show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]] [**statistics**]]
13. **show running-config flow monitor** *monitor-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**flow monitor** *monitor-name* **Example:** `Device(config)# flow monitor FLOW-MONITOR-1`	Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode. • This command also allows you to modify an existing flow monitor.
Step 4	**description** *description* **Example:** `Device(config-flow-monitor)# description Used for basic ipv4 traffic analysis`	(Optional) Creates a description for the flow monitor.

	Command or Action	Purpose
Step 5	**record** {*record-name* | **netflow-original** | **netflow** {**ipv4** | **ipv6**} *record* [**peer**]} **Example:** `Device(config-flow-monitor)# record FLOW-RECORD-1`	Specifies the record for the flow monitor.
Step 6	**cache** {**entries** *number* | **timeout** {**active** | **inactive** | **update**} *seconds* | **type** {**immediate** | **normal** | **permanent**}} **Example:** `Device(config-flow-monitor)# cache type normal`	(Optional) Modifies the flow monitor cache parameters such as timeout values, number of cache entries, and the cache type. • The values for the keywords associated with the **timeout** keyword have no 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	**statistics packet protocol** **Example:** `Device(config-flow-monitor)# statistics packet protocol`	(Optional) Enables the collection of protocol distribution statistics for Flexible NetFlow monitors.
Step 9	**statistics packet size** **Example:** `Device(config-flow-monitor)# statistics packet size`	(Optional) Enables the collection of size distribution statistics for Flexible NetFlow monitors.
Step 10	**exporter** *exporter-name* **Example:** `Device(config-flow-monitor)# exporter EXPORTER-1`	(Optional) Specifies the name of an exporter that was created previously.
Step 11	**end** **Example:** `Device(config-flow-monitor)# end`	Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
Step 12	**show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]] [**statistics**]] **Example:** `Device# show flow monitor FLOW-MONITOR-2 cache`	(Optional) Displays the status and statistics for a Flexible NetFlow flow monitor.
Step 13	**show running-config flow monitor** *monitor-name* **Example:** `Device# show running-config flow monitor FLOW_MONITOR-1`	(Optional) Displays the configuration of the specified flow monitor.

Configuring a Flow Monitor for IPv4 or IPv6 Traffic Using the Predefined Record

To configure a flow monitor for IPv4/IPv6 traffic using the Flexible NetFlow "NetFlow IPv4/IPv6 original input" predefined record for the flow monitor, perform the following required task.

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

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow monitor** *monitor-name*
4. **description** *description*
5. **record netflow {ipv4 | ipv6} original-input**
6. **end**
7. **show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]][**statistics**]]
8. **show running-config flow monitor** *monitor-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**flow monitor** *monitor-name* **Example:** `Device(config)# flow monitor FLOW-MONITOR-1`	Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode. • This command also allows you to modify an existing flow monitor.
Step 4	**description** *description* **Example:** `Device(config-flow-monitor)# description Used for monitoring IPv4 traffic`	(Optional) Creates a description for the flow monitor.
Step 5	**record netflow {ipv4 | ipv6} original-input** **Example:** `Device(config-flow-monitor)# record netflow ipv4 original-input`	Specifies the record for the flow monitor.
Step 6	**end** **Example:** `Device(config-flow-monitor)# end`	Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode.
Step 7	**show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]][**statistics**]] **Example:** `Device# show flow monitor FLOW-MONITOR-2 cache`	(Optional) Displays the status and statistics for a Flexible NetFlow flow monitor.

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

Applying a Flow Monitor to an Interface

Before it can be activated, a flow monitor must be applied to at least one interface. Perform this required task to activate a flow monitor.

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 device over which you want to monitor traffic.
6. **end**
7. **show flow interface** *type number*
8. **show flow monitor name** *monitor-name* **cache format record**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/0`	Specifies an interface and enters interface configuration mode.

	Command or Action	Purpose
Step 4	{**ip** | **ipv6**} **flow monitor** *monitor-name* {**input** | **output**} **Example:** `Device(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 device over which you want to monitor traffic.	—
Step 6	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 7	**show flow interface** *type number* **Example:** `Device# show flow interface GigabitEthernet 0/0/0`	Displays the status of Flexible NetFlow (enabled or disabled) on the specified interface.
Step 8	**show flow monitor name** *monitor-name* **cache format record** **Example:** `Device# show flow monitor name FLOW_MONITOR-1 cache format record`	Displays the status, statistics, and flow data in the cache for the specified flow monitor.

Configuring and Enabling Flexible NetFlow with Data Export

You must create a flow monitor to configure the types of traffic for which you want to export the cache data. You must enable the flow monitor by applying it to at least one interface to start exporting data. To configure and enable Flexible NetFlow with data export, perform this required task.

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

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

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 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 flow monitor can be used only for analyzing output (egress) traffic.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow monitor** *monitor-name*
4. **record** {*record-name* | **netflow-original** | **netflow** {**ipv4** | **ipv6** *record* [**peer**] }]
5. **exporter** *exporter-name*
6. **exit**
7. **interface** *type number*
8. {**ip** | **ipv6**} **flow monitor** *monitor-name* {**input** | **output**}
9. **end**
10. **show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]][**statistics**]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**flow monitor** *monitor-name* **Example:** `Device(config)# flow monitor FLOW-MONITOR-1`	Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode. • This command also allows you to modify an existing flow monitor.

	Command or Action	Purpose
Step 4	**record** {*record-name* | **netflow-original** | **netflow** {**ipv4** | **ipv6** *record* [**peer**] }] **Example:** `Device(config-flow-monitor)# record netflow ipv4 original-input`	Specifies the record for the flow monitor.
Step 5	**exporter** *exporter-name* **Example:** `Device(config-flow-monitor)# exporter EXPORTER-1`	Specifies the name of an exporter that you created previously.
Step 6	**exit** **Example:** `Device(config-flow-monitor)# exit`	Exits Flexible NetFlow flow monitor configuration mode and returns to global configuration mode.
Step 7	**interface** *type number* **Example:** `Device(config)# interface ethernet 0/0`	Specifies an interface and enters interface configuration mode.
Step 8	{**ip** | **ipv6**} **flow monitor** *monitor-name* {**input** | **output**} **Example:** `Device(config-if)# ip flow monitor FLOW-MONITOR-1 input`	Activates the flow monitor that you created previously by assigning it to the interface to analyze traffic.
Step 9	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 10	**show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]][**statistics**]] **Example:** `Device# show flow monitor FLOW-MONITOR-2 cache`	(Optional) Displays the status and statistics for a Flexible NetFlow flow monitor. This will verify data export is enabled for the flow monitor cache.

Configuration Examples for Flexible NetFlow IPv4 Unicast Flows

Example: Configuring Multiple Export Destinations

The following example shows how to configure multiple export destinations for Flexible NetFlow for IPv4 or IPv6 traffic.

This sample starts in global configuration mode:

```
!
flow exporter EXPORTER-1
 destination 172.16.10.2
 transport udp 90
 exit
!
flow exporter EXPORTER-2
 destination 172.16.10.3
 transport udp 90
 exit
!
flow monitor FLOW-MONITOR-1
 record netflow ipv4 original-input
 exporter EXPORTER-2
 exporter EXPORTER-1
!
!
flow monitor FLOW-MONITOR-2
 record netflow ipv6 original-input
 exporter EXPORTER-2
 exporter EXPORTER-1
!
ip cef
!
interface GigabitEthernet1/0/0
 ip address 172.16.6.2 255.255.255.0
 ipv6 address 2001:DB8:2:ABCD::2/48
 ip flow monitor FLOW-MONITOR-1 input
 ipv6 flow monitor FLOW-MONITOR-2 input
!
```

The following display output shows that the flow monitor is exporting data to the two exporters:

```
Router# show flow monitor FLOW-MONITOR-1
Flow Monitor FLOW-MONITOR-1:
  Description:       User defined
  Flow Record:       netflow original-input
  Flow Exporter:     EXPORTER-1
                     EXPORTER-2
  Cache:
    Type:              normal (Platform cache)
    Status:            allocated
    Size:              4096 entries / 311316 bytes
    Inactive Timeout:  15 secs
    Active Timeout:    1800 secs
    Update Timeout:    1800 secs
```

Example: Configuring Flexible NetFlow Egress Accounting for IPv4 and IPv6 Traffic

The following example shows how to configure Flexible NetFlow egress accounting for IPv4 and IPv6 traffic.

This example starts in global configuration mode.

```
!
flow monitor FLOW-MONITOR-1
 record netflow ipv4 original-output
 exit
!
!
flow monitor FLOW-MONITOR-2
 record netflow ipv6 original-output
 exit
!
ip cef
ipv6 cef
!
interface Ethernet0/0
 ip address 172.16.6.2 255.255.255.0
 ipv6 address 2001:DB8:2:ABCD::2/48
 ip flow monitor FLOW-MONITOR-1 output
 ipv6 flow monitor FLOW-MONITOR-2 output
!
```

Feature Information for Flexible NetFlow—IPv4 Unicast Flows

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

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

Table 1 Feature Information for Flexible NetFlow—IPv4 Unicast Flows

Feature Name	Releases	Feature Information
Flexible NetFlow—IPv4 Unicast Flows	12.2(33)SRC 12.2(50)SY 12.4(9)T 15.0(1)SY 15.0(1)SY1	Enables Flexible NetFlow to monitor IPv4 traffic. Support for this feature was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC. The following commands were introduced or modified: **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**.