

Using Flexible NetFlow Flow Sampling

This document contains information about and instructions for configuring sampling to reduce the CPU overhead of analyzing traffic with Flexible NetFlow.

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

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

- Prerequisites for Using Flexible NetFlow Flow Sampling, on page 1
- Restrictions for Using Flexible NetFlow Flow Sampling, on page 1
- Information About Flexible NetFlow Flow Sampling , on page 1
- How to Configure Flexible NetFlow Flow Sampling, on page 2
- Configuration Examples for Flexible NetFlow Flow Sampling, on page 6
- Additional References, on page 8
- Feature Information for Flexible NetFlow Flow Sampling, on page 8

Prerequisites for Using Flexible NetFlow Flow Sampling

- The networking device must be running a Cisco release that supports Flexible NetFlow.

Restrictions for Using Flexible NetFlow Flow Sampling

Information About Flexible NetFlow Flow Sampling

Flow Samplers

Flow samplers are created as separate components in a router's configuration. Flow samplers are used to reduce the load on the device that is running by limiting the number of packets that are selected for analysis.

Flow sampling exchanges monitoring accuracy for router performance. When you apply a sampler to a flow monitor, the overhead load on the router of running the flow monitor is reduced because the number of packets that the flow monitor must analyze is reduced. The reduction in the number of packets that are analyzed by the flow monitor causes a corresponding reduction in the accuracy of the information stored in the flow monitor's cache.

Samplers are combined with flow monitors when they are applied to an interface with the **ip flow monitor** command.

How to Configure Flexible NetFlow Flow Sampling

Flow sampling reduces the CPU overhead of analyzing traffic with Flexible NetFlow by reducing the number of packets that are analyzed.



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* .

Configuring a Flow Monitor

Samplers are applied to an interface in conjunction with a flow monitor. You must create a flow monitor to configure the types of traffic that you want to analyze before you can enable sampling. Perform this required task to configure a 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. 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 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.

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. **end**

DETAILED STEPS

Procedure

	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 traffic analysis`	(Optional) Creates a description for the flow monitor.
Step 5	**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 6	**end** **Example:** `Device(config-flow-monitor)# end`	Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode.

Perform this required task to configure and enable a flow sampler.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sampler** *sampler-name*
4. **description** *description*
5. **mode** {**random**} **1 out-of** *window-size*

6. **exit**
7. **interface** *type number*
8. {**ip** | **ipv6**} **flow monitor** *monitor-name* [[**sampler**] *sampler-name*] {**input** | **output**}
9. **end**
10. **show sampler sampler-name**

DETAILED STEPS

Procedure

	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	**sampler** *sampler-name* **Example:** `Device(config)# sampler SAMPLER-1`	Creates a sampler and enters sampler configuration mode. • This command also allows you to modify an existing sampler.
Step 4	**description** *description* **Example:** `Device(config-sampler)# description Sample at 50%`	(Optional) Creates a description for the flow sampler.
Step 5	**mode** {**random**} **1 out-of** *window-size* **Example:** `Device(config-sampler)# mode random 1 out-of 2`	Specifies the sampler mode and the flow sampler window size. • The range for the *window-size* argument is from .
Step 6	**exit** **Example:** `Device(config-sampler)# exit`	Exits sampler configuration mode and returns to global configuration mode.
Step 7	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/0`	Specifies an interface and enters interface configuration mode.

	Command or Action	Purpose
Step 8	{**ip** | **ipv6**} **flow monitor** *monitor-name* [[**sampler**] *sampler-name*] {**input** | **output**} **Example:** `Device(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input`	Assigns the flow monitor and the flow sampler that you created to the interface to enable sampling.
Step 9	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 10	**show sampler sampler-name** **Example:** `Device# show sampler SAMPLER-1`	Displays the status and statistics of the flow sampler that you configured and enabled.

Displaying the Status and Statistics of the Flow Sampler Configuration

To display the status and statistics of the flow sampler that you configured and enabled, perform the following optional task.

SUMMARY STEPS

1. **enable**
2. **show sampler sampler-name**

DETAILED STEPS

Procedure

Step 1 **enable**

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

Example:

```
Device> enable
Device#
```

Step 2 **show sampler sampler-name**

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

Example:

```
Device# show sampler SAMPLER-1
Sampler SAMPLER-1:
  ID:             2
```

```
Description:    Sample at 50%
Type:           random
Rate:           1 out of 2
Samples:        2482
Requests:       4964
Users (1):
  flow monitor FLOW-MONITOR-1 (ip,Et0/0,I  2482 out of 4964
```

Configuration Examples for Flexible NetFlow Flow Sampling

Example: Configuring and Enabling a Random Sampler for IPv4 Traffic

The following example shows how to configure and enable random sampling for IPv4 output traffic.

This example starts in global configuration mode.

```
!
flow record v4_r1
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long
!
flow monitor FLOW-MONITOR-1
 record v4_r1
 exit
!
sampler SAMPLER-1
 mode random 1 out-of 2
 exit
!
ip cef
!
interface GigabitEthernet 0/0/0
 ip address 172.16.6.2 255.255.255.0
 ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 output
!
```

The following example shows how to configure and enable random sampling for IPv4 input traffic.

This example starts in global configuration mode.

```
!
flow record v4_r1
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long
```

```
!
flow monitor FLOW-MONITOR-1
 record v4_r1
 exit
!
sampler SAMPLER-1
 mode random 1 out-of 2
 exit
!
ip cef
!
interface GigabitEthernet 0/0/0
 ip address 172.16.6.2 255.255.255.0
 ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
!
```

Example: Adding a Sampler to a Flow Monitor When a Flow Monitor Is Already Enabled

The following example shows what happens when you try to add a sampler to a flow monitor that has already been enabled on an interface without a sampler:

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
% Flow Monitor: Flow Monitor 'FLOW-MONITOR-1' is already on in full mode and cannot be
enabled with a sampler.
```

The following example shows how to remove the flow monitor from the interface so that it can be enabled with the sampler:

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# no ip flow monitor FLOW-MONITOR-1 input
Device(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
```

Example: Removing a Sampler from a Flow Monitor

The following example shows what happens when you try to remove a sampler from a flow monitor on an interface by entering the **ip flow monitor** command again without the sampler keyword and argument:

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip flow monitor FLOW-MONITOR-1 input
% Flow Monitor: Flow Monitor 'FLOW-MONITOR-1' is already on in sampled mode and cannot be
enabled in full mode.
```

The following example shows how to remove the flow monitor that was enabled with a sampler from the interface so that it can be enabled without the sampler:

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# no ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
Device(config-if)# ip flow monitor FLOW-MONITOR-1 input
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Flexible NetFlow conceptual information and configuration tasks	*Flexible NetFlow Configuration Guide*
Flexible NetFlow commands	*Cisco IOS Flexible NetFlow Command Reference*

Standards/RFCs

Standard	Title
No new or modified standards/RFCs are supported by this feature.	—

MIBs

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

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Flexible NetFlow Flow Sampling

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 Flow Sampling

Feature Name	Releases	Feature Information
Flexible Netflow - Random Sampling	12.2(50)SY 12.4(20)T Cisco IOS XE Release 3.1S Cisco IOS XE Release 3.2SE	Flow samplers are created as separate components in a router's configuration. Flow samplers are used to reduce the load on the device that is running Flexible NetFlow by limiting the number of packets that are selected for analysis. Samplers use either random or deterministic sampling techniques (modes). The following commands were introduced or modified: **clear sampler**, **debug sampler** , **mode** , **record** , **sampler** , **show sampler** .