



Using Flexible NetFlow Flow Sampling

Last Updated: November 23, 2012

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.

- [Finding Feature Information, page 1](#)
- [Prerequisites for Using Flow Sampling, page 1](#)
- [Information About Flexible NetFlow Samplers, page 2](#)
- [How to Configure Flexible NetFlow Flow Sampling, page 2](#)
- [Configuration Examples for Using Flexible NetFlow Flow Sampling, page 6](#)
- [Additional References, page 8](#)
- [Feature Information for Flexible Netflow—Random Sampling, page 9](#)

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.

Prerequisites for Using Flow Sampling

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



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

Information About Flexible NetFlow Samplers

- [Flow Samplers, page 2](#)

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 Flexible NetFlow by limiting the number of packets that are selected for analysis.

Samplers use random sampling techniques (modes); that is, a randomly selected sampling position is used each time a sample is taken.

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, page 2](#)
- [Configuring and Enabling Flow Sampling, page 4](#)

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. To configure a 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 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

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

Command or Action	Purpose
<p>Step 5 <code>record {record-name netflow-original netflow {ipv4 ipv6} record [peer]}</code></p> <p>Example:</p> <pre>Device(config-flow-monitor)# record netflow ipv4 original-input</pre>	Specifies the record for the flow monitor.
<p>Step 6 <code>end</code></p> <p>Example:</p> <pre>Device(config-flow-monitor)# end</pre>	Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode.

Configuring and Enabling Flow Sampling

To configure and enable a flow sampler, perform the following required task.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `sampler sampler-name`
4. `description description`
5. `mode {deterministic | 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

Command or Action	Purpose
<p>Step 1 <code>enable</code></p> <p>Example:</p> <pre>Device> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	sampler <i>sampler-name</i> Example: Device(config)# sampler SAMPLER-1	Creates a sampler and enters sampler configuration mode. <ul style="list-style-type: none"> This command also allows you to modify an existing sampler.
Step 4	description <i>description</i> Example: Device(config-sampler)# description Sample at 50%	(Optional) Creates a description for the flow sampler.
Step 5	mode { <i>deterministic</i> <i>random</i> } 1 out-of <i>window-size</i> Example: Device(config-sampler)# mode random 1 out-of 2	Specifies the sampler mode and the flow sampler window size. <ul style="list-style-type: none"> The range for the <i>window-size</i> argument is from 2 to 32,768.
Step 6	exit Example: Device(config-sampler)# exit	Exits sampler configuration mode and returns to global configuration mode.
Step 7	interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/0	Specifies an interface and enters interface configuration mode.
Step 8	{ip ipv6} flow monitor <i>monitor-name</i> [[sampler <i>sampler-name</i>] {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.

	Command or Action	Purpose
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.

Configuration Examples for Using Flexible NetFlow Flow Sampling

- [Example: Configuring and Enabling a Deterministic Sampler for IPv4 Traffic, page 6](#)
- [Example: Configuring and Enabling a Deterministic Sampler for IPv6 Traffic, page 7](#)
- [Example: Adding a Sampler to a Flow Monitor When a Flow Monitor Is Already Enabled, page 7](#)
- [Example: Removing a Sampler from a Flow Monitor, page 8](#)

Example: Configuring and Enabling a Deterministic Sampler for IPv4 Traffic

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

This sample starts in global configuration mode:

```
!
flow monitor FLOW-MONITOR-1
 record netflow ipv4 original-output
 exit
!
sampler SAMPLER-1
 mode deterministic 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 deterministic sampling for IPv4 input traffic.

This sample starts in global configuration mode:

```
!
flow monitor FLOW-MONITOR-1
 record netflow ipv4 original-input
 exit
!
```

```
sampler SAMPLER-1
 mode deterministic 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: Configuring and Enabling a Deterministic Sampler for IPv6 Traffic

The following example shows how to configure and enable deterministic sampling for IPv6 output traffic.

This sample starts in global configuration mode:

```
!
flow monitor FLOW-MONITOR-2
 record netflow ipv6 original-output
 exit
!
sampler SAMPLER-1
 mode deterministic 1 out-of 2
 exit
!
ip cef
ipv6 cef
!
interface GigabitEthernet 0/0/0
 ipv6 address 2001:DB8:2:ABCD::2/48
 ipv6 flow monitor FLOW-MONITOR-2 sampler SAMPLER-1 output
!
```

The following example shows how to configure and enable deterministic sampling for IPv6 input traffic.

This sample starts in global configuration mode:

```
!
flow monitor FLOW-MONITOR-2
 record netflow ipv6 original-input
 exit
!
sampler SAMPLER-1
 mode deterministic 1 out-of 2
 exit
!
ip cef
ipv6 cef
!
interface GigabitEthernet 0/0/0
 ipv6 address 2001:DB8:2:ABCD::2/48
 ipv6 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:

```
Router(config)# interface GigabitEthernet 0/0/0
Router(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:

```
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# no ip flow monitor FLOW-MONITOR-1 input
Router(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 flow monitor command again without the sampler keyword and argument:

```
Router(config)# interface GigabitEthernet 0/0/0
Router(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:

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned 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. (1110R)

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

© 2012 Cisco Systems, Inc. All rights reserved.