



Using Cisco IOS Flexible NetFlow Flow Sampling to Reduce the CPU Overhead of Analyzing Traffic

First Published: June 19, 2006

Last Updated: November 20, 2009

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 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 12](#).

Use Cisco Feature Navigator to find information about platform support and Cisco IOS, Catalyst OS, and Cisco IOS XE software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Using Flow Sampling, page 2](#)
- [Information About Flexible NetFlow Samplers, page 3](#)
- [How to Configure Flow Sampling to Reduce the CPU Overhead of Analyzing Traffic with Flexible NetFlow, page 3](#)



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

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

- [Configuration Examples for Using Flow Sampling to Reduce the CPU Overhead of Analyzing Traffic with Flexible NetFlow, page 7](#)
- [Where to Go Next, page 10](#)
- [Additional References, page 10](#)
- [Feature Information for Flexible NetFlow, page 12](#)

Prerequisites for Using Flow Sampling

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

- You are familiar with the information in the “[Cisco IOS Flexible NetFlow Overview](#)” module.
- The networking device must be running a Cisco IOS release that supports Flexible NetFlow. See the “[Cisco IOS Flexible NetFlow Features Roadmap](#)” module for a list of Cisco IOS software releases that support Flexible NetFlow.

IPv4 Traffic

- The networking device must be configured for IPv4 routing.
- One of the following must be enabled on your router and on any interfaces on which you want to enable Flexible NetFlow: Cisco Express Forwarding (CEF) or distributed CEF (dCEF).

IPv6 Traffic

- The networking device must be configured for IPv6 routing.
- One of the following must be enabled on your router and on any interfaces on which you want to enable Flexible NetFlow: Cisco Express Forwarding IPv6 (CEF IPv6) or distributed CEF IPv6 (dCEF IPv6).

Information About Flexible NetFlow Samplers

Before you configure a Flexible NetFlow sampler, you need to understand the following:

- [Samplers, page 3](#)

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 either random or deterministic sampling techniques (modes).

- **Deterministic**—The same sampling position is used each time a sample is taken.
- **Random**—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 Flow Sampling to Reduce the CPU Overhead of Analyzing Traffic with Flexible NetFlow

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](#).

To configure flow sampling to reduce the CPU overhead of analyzing traffic with Flexible NetFlow, perform the following tasks:

- [Configuring a Flow Monitor, page 3](#)
- [Configuring and Enabling Flow Sampling, page 5](#)
- [Verifying the Flow Sampler Configuration, page 6](#) (optional)

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 create a 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. The record format can be one of the predefined record formats, or an advanced user may create his or her own record format using the **collect** and **match** commands in flow record configuration mode.

Restrictions

You must 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** *string*
5. **record** {*record-name* | **netflow-original** | **netflow** {**ipv4** | **ipv6**} *record* [**peer**]}
6. **end**

DETAILED STEPS

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

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

Configuring and Enabling Flow Sampling

To configure and enable a random flow sampler, 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 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. **sampler** *sampler-name*
4. **description** *string*
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**

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	sampler <i>sampler-name</i> Example: Router(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>string</i> Example: Router(config-sampler)# description Sample at 50%	(Optional) Creates a description for the flow sampler.
Step 5	mode { deterministic random } 1 out-of <i>window-size</i> Example: Router(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 32768.
Step 6	exit Example: Router(config-sampler)# exit	Exits sampler configuration mode and returns to global configuration mode.
Step 7	interface <i>type number</i> Example: Router(config)# interface ethernet 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]}	Assigns the flow monitor and the flow sampler that you created to the interface to enable sampling.
Step 9	end Example: Router(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.

Verifying 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**

DETAILED STEPS

Step 1 **enable**

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

```
Router> enable
```

```
Router#
```

Step 2 **show sampler**

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

```
Router# 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 Using Flow Sampling to Reduce the CPU Overhead of Analyzing Traffic with Flexible NetFlow

This section provides the following configuration examples:

- [Configuring and Enabling a Deterministic Sampler for IPv4 Traffic, page 8](#)
- [Configuring and Enabling a Deterministic Sampler for IPv6 Traffic, page 8](#)
- [Adding a Sampler to a Flow Monitor When a Flow Monitor Is Already Enabled on an Interface, page 9](#)
- [Removing a Sampler from a Flow Monitor, page 9](#)

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

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 Ethernet0/0
  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 Ethernet0/0
  ipv6 address 2001:DB8:2:ABCD::2/48
  ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
!

```

Adding a Sampler to a Flow Monitor When a Flow Monitor Is Already Enabled on an Interface

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 Ethernet0/0
Router(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 in
% 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 Ethernet0/0
Router(config-if)# no ip flow monitor FLOW-MONITOR-1 in
Router(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 in

```

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 Ethernet0/0
Router(config-if)# ip flow monitor FLOW-MONITOR-1 in
% 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 Ethernet0/0

```

```
Router(config-if)# no ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 in
Router(config-if)# ip flow monitor FLOW-MONITOR-1 in
```

Where to Go Next

For information on advanced Flexible NetFlow configurations for specific purposes such as quality of service (QoS) and bandwidth monitoring, application and user flow monitoring and profiling, and security analysis, refer to the [“Customizing Cisco IOS Flexible NetFlow Flow Records and Flow Monitors”](#) module.

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

If you want to configure data export for Flexible NetFlow, refer to the [“Configuring Data Export for Cisco IOS Flexible NetFlow with Flow Exporters”](#) module.

Additional References

The following sections provide references related to Flexible NetFlow.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Overview of Flexible NetFlow	“Cisco IOS Flexible NetFlow Overview”
Flexible NetFlow Feature Roadmap	“Cisco IOS Flexible NetFlow Features Roadmap”
Emulating original NetFlow with Flexible NetFlow	“Getting Started with Configuring Cisco IOS Flexible NetFlow”
Configuring flow exporters to export Flexible NetFlow data.	“Configuring Data Export for Cisco IOS Flexible NetFlow with Flow Exporters”
Customizing Flexible NetFlow	“Customizing Cisco IOS Flexible NetFlow Flow Records and Flow Monitors”
Configuring 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	Cisco IOS Flexible NetFlow Command Reference

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/cisco/web/support/index.html

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 12.2(33)SRC	<p>Flexible NetFlow is introduced.</p> <p>Support for this feature was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.</p> <p>Information about the Flexible NetFlow feature is included in the following sections:</p> <ul style="list-style-type: none"> • Prerequisites for Using Flow Sampling, page 2 • Information About Flexible NetFlow Samplers, page 3 • How to Configure Flow Sampling to Reduce the CPU Overhead of Analyzing Traffic with Flexible NetFlow, page 3 • Configuration Examples for Using Flow Sampling to Reduce the CPU Overhead of Analyzing Traffic with Flexible NetFlow, page 7 <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—IPv6 Unicast Flows	12.4(20)T 12.2(33)SRE	<p>Enables Flexible NetFlow to monitor IPv6 traffic.</p> <p>Support for this feature was added for Cisco 7200 and 7300 NPE series routers in Cisco IOS Release 12.2(33)SRE.</p> <p>Information about the Flexible NetFlow - IPv6 Unicast Flows feature is included in the following sections:</p> <ul style="list-style-type: none"> • How to Configure Flow Sampling to Reduce the CPU Overhead of Analyzing Traffic with Flexible NetFlow, page 3 • Configuring and Enabling a Deterministic Sampler for IPv6 Traffic, page 8 <p>The following commands were introduced or modified: collect routing, debug flow record, match routing, record, show flow monitor, show flow record, collect ipv6, collect ipv6 destination, collect ipv6 extension map, collect ipv6 fragmentation, collect ipv6 hop-limit, collect ipv6 length, collect ipv6 section, collect ipv6 source, collect transport icmp ipv6, ipv6 flow monitor, match ipv6, match ipv6 destination, match ipv6 extension map, match ipv6 fragmentation, match ipv6 hop-limit, match ipv6 length, match ipv6 section, match ipv6 source, match transport icmp ipv6.</p>

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

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

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