Using NetFlow Sampling to Select the Network Traffic to Track

This module contains information about and instructions for selecting the network traffic to track through the use of NetFlow sampling. The Random Sampled NetFlow feature, described in this module, allows you to collect data from specific subsets of traffic. The Random Sampled NetFlow feature provides NetFlow data for a subset of traffic in a Cisco router by processing only one randomly selected packet out of *n* sequential packets (*n* is a user-configurable parameter).

NetFlow is a Cisco IOS XE application that provides statistics on packets flowing through the router. It is emerging as a primary network accounting and security technology.

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 Table at the end of this document.

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 NetFlow Sampling to Select Network Traffic to Track

Before you can configure the Random Sampled NetFlow feature, you must:

- Configure the router for IP routing.
- Configure Cisco Express Forwarding on your router and on the interfaces on which you want to configure Random Sampled NetFlow. Fast switching is not supported.
- Configure NetFlow Version 9 data export if you want to export NetFlow data (otherwise, NetFlow data is visible in the cache, but is not exported).
- Configure NetFlow Version 9 if you want to use sampler option templates or view NetFlow sampler IDs.

Restrictions for Using NetFlow Sampling to Select Network Traffic to Track

If full NetFlow is enabled on an interface, it takes precedence over Random Sampled NetFlow (which will thus have no effect). This means that you should disable full NetFlow on an interface before enabling Random Sampled NetFlow on that interface.

Enabling Random Sampled NetFlow on a physical interface does not automatically enable Random Sampled NetFlow on subinterfaces; you must explicitly configure it on subinterfaces. Also, disabling Random Sampled NetFlow on a physical interface (or a subinterface) does not enable full NetFlow. This restriction prevents the transition to full NetFlow from overwhelming the physical interface (or subinterface). If you want full NetFlow, you must explicitly enable it.

Use NetFlow Version 9 if you want to use sampler option templates.

Information About Using NetFlow Sampling to Select Network Traffic to Track

Sampling of NetFlow Traffic

NetFlow provides highly granular per-flow traffic statistics in a Cisco router. A flow is a unidirectional stream of packets that arrive at the router on the same subinterface, have the same source and destination IP addresses, Layer 4 protocol, TCP/UDP source and destination ports, and the same ToS (type of service) byte in the IP headers. The router accumulates NetFlow statistics in a NetFlow cache and can export them to an external device (such as the Cisco Networking Services (CNS) NetFlow Collection Engine) for further processing.

Full NetFlow accounts for all traffic entering the subinterface on which it is enabled. But in some cases, you might gather NetFlow data on only a subset of this traffic. The Random Sampled NetFlow feature provides a way to limit incoming traffic to only traffic of interest for NetFlow processing. Random Sampled NetFlow

provides NetFlow data for a subset of traffic in a Cisco router by processing only one randomly selected packet out of *n* sequential packets.

Note Random Sampled NetFlow is more statistically accurate than Sampled NetFlow. NetFlow's ability to sample packets was first provided by a feature named Sampled NetFlow. The methodology that the Sampled NetFlow feature uses is *deterministic* sampling, which selects every nth packet for NetFlow processing on a per-interface basis. For example, if you set the sampling rate to 1 out of 100 packets, then Sampled NetFlow samples the 1st, 101st, 201st, 301st, and so on packets. Sampled NetFlow does not allow random sampling and thus can make statistics inaccurate when traffic arrives in fixed patterns.

Random Sampled NetFlow Sampling Mode

Sampling mode makes use of an algorithm that selects a subset of traffic for NetFlow processing. In the random sampling mode that the Random Sampled NetFlow feature uses, incoming packets are randomly selected so that one out of each n sequential packets is selected *on average* for NetFlow processing. For example, if you set the sampling rate to 1 out of 100 packets, then NetFlow might sample the 5th packet and then the 120th, 199th, 302nd, and so on. This sample configuration provides NetFlow data on 1 percent of total traffic. The n value is a parameter from 1 to 65535 packets that you can configure.

Random Sampled NetFlow The NetFlow Sampler

A NetFlow sampler map defines a set of properties (such as the sampling rate and NetFlow sampler name) for NetFlow sampling. Each NetFlow sampler map can be applied to one or many subinterfaces as well as physical interfaces. You can define up to eight NetFlow sampler maps.

For example, you can create a NetFlow sampler map named mysampler1 with the following properties: random sampling mode and a sampling rate of 1 out of 100 packets. This NetFlow sampler map can be applied to any number of subinterfaces, each of which would refer to mysampler1 to perform NetFlow sampling. Traffic from these subinterfaces is merged (from a sampling point of view). This introduces even more "randomness" than random per-subinterface NetFlow sampling does, but statistically it provides the same sampling rate of 1 out of 100 packets for each participating subinterface.

The sampling in random sampled NetFlow is done by NetFlow samplers. A NetFlow sampler is defined as an instance of a NetFlow sampler map that has been applied to a physical interface or subinterface. If full NetFlow is configured on a physical interface, it overrides random sampled NetFlow on all subinterfaces of this physical interface.

How to Configure NetFlow Sampling

Configuring Random Sampled NetFlow to Reduce the Impact of NetFlow Data Export

To configure and verify the configuration for the Random Sampled NetFlow feature, perform the following tasks:

Defining a NetFlow Sampler Map

To define a NetFlow sampler map, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow-sampler-map** *sampler-map-name*
4. **mode random one-out-of** *sampling-rate*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.
Step 3	**flow-sampler-map** *sampler-map-name* **Example:** `Router(config)# flow-sampler-map mysampler1`	(Required) Defines a NetFlow sampler map and enters flow sampler map configuration mode. • The *sampler-map-name* argument is the name of the NetFlow sampler map to be defined.
Step 4	**mode random one-out-of** *sampling-rate* **Example:** `Router(config-sampler)# mode random one-out-of 100`	(Required) Enables random mode and specifies a sampling rate for the NetFlow sampler. • The **random** keyword specifies that sampling uses the random mode. • The **one-out-of** *sampling-rate* keyword-argument pair specifies the sampling rate (one out of every *n* packets) from which to sample. For *n*, you can specify from 1 to 65535 (packets).
Step 5	**end** **Example:** `Router(config-sampler)# end`	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Applying a NetFlow Sampler Map to an Interface

To apply a NetFlow sampler map to an interface, perform the following steps.

You can apply a NetFlow sampler map to a physical interface (or a subinterface) to create a NetFlow sampler.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-type interface-number*
4. **flow-sampler** *sampler-map-name*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.
Step 3	**interface** *interface-type interface-number* **Example:** `Router(config)# fastethernet 1/0/0.2`	(Required) Specifies the interface and enters interface configuration mode.
Step 4	**flow-sampler** *sampler-map-name* **Example:** `Router(config-if)# flow-sampler mysampler1`	(Required) Applies a NetFlow sampler map to the interface to create the NetFlow sampler. • The *sampler-map-name* argument is the name of the NetFlow sampler map to apply to the interface.
Step 5	**end** **Example:** `Router(config-if)# end`	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Verifying the Configuration of Random Sampled NetFlow

To verify the configuration of random sampled NetFlow, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **show flow-sampler**
3. **show ip cache verbose flow**
4. **show ip flow export template**
5. **end**

DETAILED STEPS

Step 1 **enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
```

Router#

Step 2 **show flow-sampler**

Use this command to display attributes (including mode, sampling rate, and number of sampled packets) of one or all Random Sampled NetFlow samplers to verify the sampler configuration. For example:

Example:

```
Router# show flow-sampler
Sampler : mysampler1, id : 1, packets matched : 10, mode : random sampling mode
  sampling interval is : 100
 Sampler : myflowsampler2, id : 2, packets matched : 5, mode : random sampling mode
  sampling interval is : 200
```

To verify attributes for a particular NetFlow sampler, use the **show flow-sampler** *sampler-map-name*command. For example, enter the following for a NetFlow sampler named mysampler1:

Example:

```
Router# show flow-sampler mysampler1
Sampler : mysampler1, id : 1, packets matched : 0, mode : random sampling mode
  sampling interval is : 100
```

Step 3 **show ip cache verbose flow**

Use this command to display additional NetFlow fields in the header when Random Sampled NetFlow is configured. For example:

Example:

```
Router# show ip cache verbose flow
...
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
BGP: BGP NextHop
Fet1/0/0        8.8.8.8        FEt0/0/0*      9.9.9.9         01 00  10       3
0000 /8  302                   0800 /8  300   3.3.3.3               100     0.1
BGP: 2.2.2.2         Sampler: 1  Class: 1  FFlags: 01
```

This example shows the NetFlow output of the **show ip cache verbose flow** command in which the sampler, class-id, and general flags are set. What is displayed for a flow depends on what flags are set in the flow. If the flow was captured by a sampler, the output shows the sampler ID. If the flow was marked by MQC, the display includes the class ID. If any general flags are set, the output includes the flags.

NetFlow flags (FFlags) that might appear in the **show ip cache verbose flow** command output are:

- FFlags: 01 (#define FLOW_FLAGS_OUTPUT 0x0001)--Egress flow
- FFlags: 02 (#define FLOW_FLAGS_DROP 0x0002)--Dropped flow (for example, dropped by an ACL)
- FFlags: 08 (#define FLOW_FLAGS_IPV6 0x0008)--IPv6 flow
- FFlags: 10 (#define FLOW_FLAGS_RSVD 0x0010)--Reserved

IPv6 and RSVD FFlags are seldom used. If FFlags is zero, the line is omitted from the output. If multiple flags are defined (logical ORed together), then both sets of flags are displayed in hexadecimal format.

Step 4 **show ip flow export template**

Use this command to display the statistics for the NetFlow data export (such as template timeout and refresh rate) for the template-specific configurations. For example:

Example:

```
Router# show ip flow export template
Template Options Flag = 0
   Total number of Templates added = 0
   Total active Templates = 0
   Flow Templates active = 0
   Flow Templates added = 0
   Option Templates active = 0
   Option Templates added = 0
   Template ager polls = 0
   Option Template ager polls = 0
Main cache version 9 export is enabled
 Template export information
   Template timeout = 30
   Template refresh rate = 20
 Option export information
   Option timeout = 30
   Option refresh rate = 20
```

Step 5 **end**

Use this command to exit privileged EXEC mode.

Example:

```
Router# end
```

Troubleshooting Tips

If there are no multicast flow records in the NetFlow cache, check the multicast switching counters for the existence of process-switched packets (NetFlow exports only fast-switched or MDFS-switched packets). If process-switched packets are present, check the MDFS routing table to help determine potential problems.

Configuration Examples for Configuring NetFlow Sampling

Configuring Random Sampled NetFlow to Reduce the Impact of NetFlow Data Export Examples

Defining a NetFlow Sampler Map Example

The following example shows how to define a NetFlow sampler map named mysampler1:

```
configure terminal
!
flow-sampler-map mysampler1
 mode random one-out-of 100
 end
```

Applying a NetFlow Sampler Map to an Interface Example

The following example shows how to enable Cisco Express Forwarding switching and apply a NetFlow sampler map named mysampler1 to Fastethernet interface 1/0/0 to create a NetFlow sampler on that interface:

```
configure terminal
!
ip cef
!
interface fastethernet 1/0/0
 flow-sampler mysampler1
 end
```

Additional References

Related Documents

Related Topic	Document Title
NetFlow commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS NetFlow Command Reference*
Tasks for configuring NetFlow to capture and export network traffic data	"Configuring NetFlow and NetFlow Data Export"
Tasks for configuring Random Sampled NetFlow	"Using NetFlow Sampling to Select the Network Traffic to Track"
Tasks for configuring NetFlow aggregation caches	Configuring NetFlow Aggregation Caches"
Information for installing, starting, and configuring the CNS NetFlow Collection Engine	"Cisco CNS NetFlow Collection Engine Documentation"

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Using NetFlow Sampling to Select Network Traffic to Track

Table 1: Feature Information for Using NetFlow Sampling to Select Network Traffic to Track

Feature Name	Releases	Feature Configuration Information
Random Sampled NetFlow	Cisco IOS XE Release 2.1	Random Sampled NetFlow provides NetFlow data for a subset of traffic in a Cisco router by processing only one randomly selected packet out of n sequential packets (n is a user-configurable parameter). Packets are sampled as they arrive (before any NetFlow cache entries are made for those packets). Statistical traffic sampling substantially reduces consumption of router resources (especially CPU resources) while providing valuable NetFlow data. The main uses of Random Sampled NetFlow are traffic engineering, capacity planning, and applications where full NetFlow is not needed for an accurate view of network traffic. In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified by this feature: **debug flow-sampler**, **flow-sampler**, **flow-sampler-map**, **ip flow-export, mode** (**flow sampler map configuration**), **show flow-sampler**.

Glossary

ACL --Access control list. A roster of users and groups of users kept by a router. The list is used to control access to or from the router for a number of services.

BGP --Border Gateway Protocol. Interdomain routing protocol that replaces Exterior Gateway Protocol (EGP). A BGP system exchanges reachability information with other BGP systems. BGP is defined by RFC 1163.

CEF --Cisco Express Forwarding. Layer 3 IP switching technology that optimizes network performance and scalability for networks with large and dynamic traffic patterns.

fast switching --Cisco feature in which a route cache is used to expedite packet switching through a router.

flow --Unidirectional stream of packets between a given source and destination. Source and destination are each defined by a network-layer IP address and transport-layer source and destination port numbers.

MQC --Modular Quality of Service (QoS) Command-line Interface (CLI). A CLI structure that lets you create traffic polices and attach them to interfaces. A traffic policy contains a traffic class and one or more QoS features. The QoS features in the traffic policy determine how the classified traffic is treated.

NBAR --Network-Based Application Recognition. A classification engine in Cisco IOS software that recognizes a wide variety of applications, including web-based applications and client/server applications that dynamically assign Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port numbers. After the application is recognized, the network can invoke specific services for that application. NBAR is a key part of the Cisco Content Networking architecture and works with QoS features to let you use network bandwidth efficiently.

NetFlow --Cisco IOS XE security and accounting feature that maintains per-flow information.

NetFlow sampler --A set of properties that are defined in a NetFlow sampler map that has been applied to at least one physical interface or subinterface.

NetFlow sampler map --The definition of a set of properties (such as the sampling rate) for NetFlow sampling.

NetFlow v9 --NetFlow export format Version 9. A flexible and extensible means for carrying NetFlow records from a network node to a collector. NetFlow Version 9 has definable record types and is self-describing for easier NetFlow Collection Engine configuration.

ToS --type of service. Second byte in the IP header that indicates the desired quality of service for a specific datagram.