CHAPTER 1

Configuring Flexible NetFlow

NetFlow is a monitoring feature used on customer applications for network monitoring, user monitoring and profiling, network planning, security analysis, billing and accounting, and data warehousing and mining. You can use Flexible NetFlow on uplink ports to monitor user-defined flows, collect flow statistics, and perform per-flow policing. It collects and exports flow statistics to a collector device.

Note Flexible NetFlow is supported only on the Catalyst 3750-X and 3560-X switch running the IP base or IP services feature set and equipped with the network services module. It is not supported on switches running the NPE or the LAN base image.

For more detailed information about Flexible NetFlow, see the NetFlow Configuration Guide: http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/12_4t/fnf_12_4t_book.html

For information about the commands, see the *Cisco IOS Flexible NetFlow Command Reference*:

http://www.cisco.com/en/US/docs/ios/fnetflow/command/reference/fnf_book.html

Note Not all of the Flexible NetFlow commands in the command reference are available on the switch. Unsupported commands are either not visible or generate an error message if entered.

Understanding Flexible NetFlow

With Flexible NetFlow, traffic is processed and packets are classified into flows. New flows are inserted in the NetFlow table, and statistics are automatically updated. You must configure both ingress and egress NetFlow monitoring. The network services module supports one monitor per interface per direction.

Flexible NetFlow has these components:

- *Records* are combinations of key and nonkey fields assigned to monitor Flexible NetFlow monitors to define the cache used to store data.
- *Flow monitors* are applied to interfaces to perform network traffic monitoring. A flow monitor includes a user-defined record, an optional flow exporter, and a cache that is automatically created when the monitor is applied to the first interface. The switch supports normal caches that age out according to settings.
- Flow exporters export the data in the flow monitor cache to a remote system, such as a server running NetFlow collector.

- Flow samplers reduce the load that Flexible NetFlow puts on the networking device to monitor traffic by limiting the number of packets that are analyzed.

You can configure unidirectional flow (destination or source-address based flows), and you can also configure flow aging. These features are supported on the network services module:

- You can configure collection statistics for Layer 2-switched (nonrouting) traffic, Layer 3 IPv4 and IPv6 traffic, and Layer 4 TCP, IGMP, and ICMP traffic.
- NetFlow counting, maintenance, troubleshooting (debugging commands).
- NetFlow analysis is performed on traffic crossing the physical interfaces on the network services module. The switch processes egress (outbound) traffic after forwarding decisions are performed. You can force locally switched or routed traffic through service module ports by configuring private VLANs or protected ports.

These NetFlow characteristics are not supported:

- Netflow-5 protocol
- Predefined flow records
- ISL
- Policy-based NetFlow
- Cisco TrustSec monitoring

Although other modules that can be installed in the Catalyst 3750-X and 3560-X have 1-Gigabit and 10-Gigabit uplink interfaces, NetFlow is supported only on the network services module.

Configuring Flexible NetFlow

These are some basic Flexible NetFlow configurations.

- Configuring a Customized Flow Record, page 1-2
- Configuring the Flow Exporter, page 1-5
- Configuring a Customized Flow Monitor, page 1-6
- Applying a Flow Monitor to an Interface, page 1-7
- Configuring and Enabling Flow Sampling, page 1-9

For more information about Flexible NetFlow, see the *Cisco IOS Flexible NetFlow Configuration Guide*: http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/12_4t/fnf_12_4t_book.html

For information about the commands, see the *Cisco IOS Flexible NetFlow Command Reference*:

http://www.cisco.com/en/US/docs/ios/fnetflow/command/reference/fnf_book.html

Configuring a Customized Flow Record

You can **match** these key fields for the flow record:

- IPv4 or IPv6 destination address
- Datalink fields to identify Layer 2 source and destination address and VLAN for traffic entering or leaving the interfaces, providing the MAC address of the directly connected host. Class of Service (CoS) and Ethertype datalink header fields are also available.

- Transport field source and destination ports to identify the type of application: ICMP, IGMP, or TCP traffic.

You can **collect** these key fields for the flow record:

- The total number of bytes, flows or packets sent by the exporter (**exporter**) or the number of bytes or packets in a 64-bit counter (**long**).
- The timestamp based on system uptime from the time the first packet was sent or from the time the most recent (**last**) packet was seen.
- The SNMP index of the input or output interface. The interface for traffic entering or leaving the service module is based on the switch forwarding cache. This field is typically used in conjunction with datalink, IPv4, and IPv6 addresses, and provides the actual first-hop interface for directly connected hosts.
  - A value of 0 means that interface information is not available in the cache.
  - Some NetFlow collectors require this information in the flow record.

See the *Cisco IOS Flexible NetFlow Configuration Guide* and the *Cisco IOS Flexible NetFlow Command Reference* for more detailed information.

Beginning in privileged EXEC mode, follow these steps to configure the customized flow record.

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**flow record** *record-name*	Creates a flow record and enters Flexible NetFlow flow record configuration mode. You can also use this command to modify an existing flow record.
Step 3	**description** *description*	(Optional) Creates a description for the flow record.
Step 4	**match** {**ipv4** | **ipv6**} {**destination** | **source**} **address** or **match datalink** {**destination-vlan-id** | **dot1q** | **ethertype** | **mac** | **source-vlan-id**} or **match transport** {**icmp** | **igmp**| **source-port** | **tcp** | **udp**}	Configures a key field for the flow record. See the *Cisco IOS Flexible NetFlow Configuration Guide* and the *Cisco IOS Flexible NetFlow Command Reference* for more detailed information.
Step 5	Repeat step 4 to configure additional files for the record.	
Step 6	**collect counter** {**bytes** [**exported** | **long**] **flows** [**exported**] | **packets**} [**exported** | **long**] or **collect timestamp sys-uptime** {**first** | **last**} or **collect interface** {**input** | **output**} **snmp**	Configures one or more source fields in the flow as counter fields, timestamp fields, or interface fields. See the *Cisco IOS Flexible NetFlow Configuration Guide* and the *Cisco IOS Flexible NetFlow Command Reference* for more detailed information.
Step 7	Repeat Step 6 as required to configure additional fields for the record.	
Step 8	**end**	Returns to privileged EXEC mode.

	Command	Purpose
Step 9	**show running-config flow record**	(Optional) Displays the configured flow records.
Step 10	**show flow record**	(Optional) Displays the status of the flow records.
Step 11	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

This example shows how to configure a flow record:

```
Switch(config)# flow record
Switch(config-flow-record)# description record to monitor network traffic
Switch(config-flow-record)# match ipv4 destination address
Switch(config-flow-record)# collect counter packets
Switch(config-flow-record)# collect counter bytes
Switch(config-flow-record)# end
```

This is an example of output from the **show flow record** command:

```
Switch# show flow record
flow record L2L4ipv4:
  Description:        User defined
  No. of users:       1
  Total field space:  56 bytes
  Fields:
    match datalink dot1q priority
    match datalink mac source-address
    match datalink mac destination-address
    match ipv4 tos
    match ipv4 ttl
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
    match transport source-port
    match transport destination-port
    collect interface input snmp
    collect interface output snmp
    collect counter flows
    collect counter bytes
    collect counter packets
    collect timestamp sys-uptime first
    collect timestamp sys-uptime last

flow record L2L4ipv6:
  Description:        User defined
  No. of users:       1
  Total field space:  81 bytes
  Fields:
    match datalink mac source-address
    match datalink mac destination-address
    match ipv6 traffic-class
    match ipv6 protocol
    match ipv6 source address
    match ipv6 destination address
    match ipv6 fragmentation flags
    match transport source-port
    match transport destination-port
    match transport icmp ipv6 type
    match transport icmp ipv6 code
    collect interface input snmp
    collect interface output snmp
    collect counter flows
    collect counter bytes
    collect counter packets
```

```
collect timestamp sys-uptime first
collect timestamp sys-uptime last
```

Configuring the Flow Exporter

Beginning in privileged EXEC mode, follow these steps to configure the NetFlow exporter. For more information about configuring Flexible NetFlow flow exporters, see the *Configuring Data Export for Cisco IOS Flexible NetFlow with Flow Exporters* document:

http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/cfg_de_fnflow_exprts.html

Note The optional **export-protocol** flow exporter configuration command specifies the NetFlow export protocol used by the exporter. The switch supports only **netflow-v9.** Although visible in the CLI help, **netflow-5** is not supported.

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**flow exporter** *exporter-name*	Creates the flow exporter and enters Flexible NetFlow flow exporter configuration mode. You can also use this command to modify an existing flow exporter.
Step 3	**description** *description*	(Optional) Configures a description for the exporter that appears in the configuration and in the display of the **show flow exporter** command.
Step 4	**destination** {*hostname* | *ip-address*} [**vrf** *vrf-name*]	Specifies the IP address or hostname of the destination system for the exporter.
Step 5	**dscp** *dscp*	(Optional) Configures differentiated services code point (DSCP) parameters for datagrams sent by the exporter. The DSCP range is from 0 to 63. The default is 0.
Step 6	**source** *interface-id*	(Optional) Specifies the local interface from which the exporter uses the IP address as the source IP address for exported datagrams.
Step 7	**option** {**exporter-stats** | **interface-table** | **sampler-table**} [**timeout** *seconds*]	(Optional) Configures options data parameters for the exporter. You can configure all three options concurrently. The range for the timeout is 1 to 86400 seconds. The default is 600.
Step 8	**template data timeout** *seconds*	(Optional) Configures resending of templates based on a timeout. The range is 1 to 86400 seconds (86400 seconds equals 24 hours). The default is 600.
Step 9	**transport udp** *udp-port*	Specifies the UDP port on which the destination system is listening for exported datagrams. The range for *udp-port* is from 1 to 65536.
Step 10	**ttl** *seconds*	(Optional) Configures the time-to-live (TTL) value for datagrams sent by the exporter. The range is from 1 to 255 seconds. The default is 255.
Step 11	**end**	Returns to privileged EXEC mode.
Step 12	**show running-config flow exporter** *exporter-name*	(Optional) Verifies the configured flow exporter.
Step 13	**show flow exporter** *exporter-name*	(Optional) Displays the status of a flow exporter.
Step 14	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

This example shows how to configure the flow exporter:

```
Switch(config)# flow exporter QoS-Collector
Switch(config-flow-exporter)# description QoS Collector Bldg 19
Switch(config-flow-exporter)# destination 172.20.244.28
Switch(config-flow-exporter)# source vlan 1
Switch(config-flow-exporter)# dscp 3
Switch(config-flow-exporter)# transport udp 2055
Switch(config-flow-exporter)# end
```

This is an example of output from the **show flow exporter** command:

```
Switch# show flow exporter EXPORTER-1
Flow Exporter QoS-Collector:
  Description:              QoS Collector Bldg 19
  Export protocol:          NetFlow Version 9
  Transport Configuration:
    Destination IP address: 172.20.244.28
    Source IP address:      10.30.0.234
    Source Interface:       Vlan1
    Transport Protocol:     UDP
    Destination Port:       2055
    Source Port:            62401
    DSCP:                   0x3
    TTL:                    255
    Output Features:        Not Used
```

Configuring a Customized Flow Monitor

Beginning in privileged EXEC mode, follow these steps to configure a NetFlow monitor.

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**flow monitor** *monitor -name*	Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode. You can also use this command to modify an existing flow monitor
Step 3	**description** *description*	(Optional) Configures a description for the flow monitor.
Step 4	**record** *record-name*	Specifies the record for the flow monitor.
Step 5	**cache** {**timeout active** *seconds* | **type normal**}	(Optional) Modifies the flow monitor cache parameters such as timeout values, number of cache entries, and the cache type. • **timeout active** *seconds*—Configure the active flow timeout. This defines the granularity of the traffic analysis. The range is from 1 to 604800 seconds. The default is 1800. Typical values are 60 or 300 seconds. See the *Configuring Data Export for Cisco IOS Flexible NetFlow with Flow Exporters* document for recommended values. • **type normal—**Configure normal flow removal from the flow cache. **Note** Although visible in the command line help, the **entries** keyword and **inactive** and **update** timeouts are not supported.
Step 6	Repeat step 5 to configure additional cache parameters for the flow monitor.	
Step 7	**exporter** *exporter-name*	(Optional) Specifies the name of an exporter that was created previously.

	Command	Purpose
Step 8	Repeat step 5 to configure additional exporters.	
Step 9	**end**	Returns to privileged EXEC mode.
Step 10	**show running-config flow monitor** *monitor -name*	(Optional) Verifies the flow monitor configuration.
Step 11	**show flow monitor** *monitor -name*	(Optional) Displays the current status of a flow monitor.
Step 12	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

This example shows how to configure a flow monitor:

```
Switch(config)# flow monitor FLOW-MONITOR-1
Switch(config-flow-monitor)# Used for ipv4 traffic analysis
Switch(config-flow-monitor)# record FLOW-RECORD-1
Switch(config-flow-monitor)# cache timeout active 300
Switch(config-flow-monitor)# cache type normal
Switch(config-flow-monitor)# exporter EXPORTER-1
Switch(config-flow-monitor)# exit
```

This is an example of output from the **show flow monitor** command:

```
Switch# show flow monitor FLOW-MONITOR-1

Flow Monitor FLOW-MONITOR-1:
  Description:       Used for basic ipv4 traffic analysis
  Flow Record:       FLOW-RECORD-1
  Flow Exporter:     EXPORTER-1
  Cache:
    Type:              normal (Platform cache)
    Status:            allocated
    Size:              Unknown
    Inactive Timeout:  15 secs
    Active Timeout:    1800 secs    1800 secs
    Update Timeout:    1800 secs
```

Applying a Flow Monitor to an Interface

Beginning in privileged EXEC mode, follow these steps to apply a NetFlow monitor to an interface.

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface** *interface-id*	Identifies an interface and enters interface configuration mode. Flexible Net Flow is supported only on the service module 1-Gigabit or 10-Gigabit Ethernet interfaces. **Note** You cannot attach a NetFlow monitor to a port channel interface. If both service module interfaces are part of an EtherChannel, you should attach the monitor to both physical interfaces.

	Command	Purpose
Step 3	{**ip** | **ipv6**} **flow monitor** *monitor -name* [**layer2-switched** | **multicast** | **sampler** | **unicast**] {**input** | **output**}	Activates a previously created flow monitor by assigning it to the interface to analyze incoming or outgoing traffic. • **ip**—Enter in records matching IPv4 IP addresses. • **ipv6**—Enter in records matching IPv6 IP addresses. **Note** This keyword is visible only when the dual IPv4 and IPv6 Switch Database Management (SDM) template is configured on the switch. • **layer2-switched**—(Optional) Apply the flow monitor on Layer 2 switched traffic. • **multicast**—(Optional) Apply the flow monitor on multicast traffic. • **sampler**—(Optional) Apply the flow monitor sampler. • **unicast**—(Optional) Apply the flow monitor on unicast traffic. • **input**—Apply the flow monitor on input traffic. • **output**—Apply the flow monitor on output traffic.
Step 4	**exit**	Returns to global configuration mode.
Step 5	Repeat steps 2 and 3 to configure additional cache parameters for the flow monitor.	
Step 6	**end**	Returns to privileged EXEC mode.
Step 7	**show flow interface** *interface-id*	(Optional) Verifies that the Flexible NetFlow is configured on the interface.
Step 8	**show flow monitor name** *monitor -name* **cache**	(Optional) Displays data in the flow monitor cache.
Step 9	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

This example shows how to apply a flow monitor to an interface:

```
Switch(config)# interface gigabitethernet 1/1/2
Switch(config-if)# ip flow monitor FLOW-MONITOR-1 input
Switch(config-if)# ip flow monitor FLOW-MONITOR-2 output
Switch(config-if)# end
```

This is an example of output from the **show flow interface** command:

```
Switch# show flow interface gigabitethernet 1/1/2

Interface Gigabit Ethernet1/1/2
  FNF:  monitor:         FLOW-MONITOR-1
        direction:       Input
        traffic(ip):     on
  FNF:  monitor:         FLOW-MONITOR-2
        direction:       Input
        traffic(ipv6):   on
```

Configuring and Enabling Flow Sampling

Beginning in privileged EXEC mode, follow these steps to configure and enable flow sampling.

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**sampler** *sampler -name*	Creates a flow monitor and enters Flexible NetFlow sampler configuration mode. You can also use this command to modify an existing sampler.
Step 3	**description** *description*	(Optional) Configures a description for the sampler.
Step 4	**mode random 1 out-of** *window-size*	Specifies the mode and window size from which to select packets. The window size range is from 2 to 32768. **Note** Although visible in the CLI help, the **mode deterministic** keyword is not supported.
Step 5	**exit**	Returns to global configuration mode.
Step 6	**interface** *interface-id*	Identifies an interface and enters interface configuration mode. Flexible Net Flow is supported only on the service module 1-Gigabit or 10-Gigabit Ethernet interfaces.
Step 7	{**ip**| **ipv6**} **flow monitor** *monitor-name* **sampler** *sampler-name* {**input** | **output**}	Activates a previously created IPv4 or IPv6 flow monitor by assigning it to the interface to analyze traffic.
Step 8	**end**	Returns to privileged EXEC mode.
Step 9	**show sampler** *sampler -name*	(Optional) Displays the current status of a flow sampler.
Step 10	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

This example shows how to configure and enable a flow sampler:

```
Switch(config)# sampler SAMPLER-1
Switch(config-sampler)# description Sample at 50
Switch(config-sampler)# mode random 1 out-of 2
Switch(config-sampler)# exit
Switch(config)# interface gigabitethernet 1/1/2
Switch(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLE-1 input
```

This is an example of output from the **show sampler** command:

```
Switch# 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
```