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:

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

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.
Chapter 1  Configuring Flexible NetFlow

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:

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

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.
Chapter 1      Configuring Flexible NetFlow

- 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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>flow record record-name</td>
</tr>
<tr>
<td></td>
<td>Creates a flow record and enters Flexible NetFlow flow record configuration mode. You can also use this command to modify an existing flow record.</td>
</tr>
<tr>
<td>Step 3</td>
<td>description description</td>
</tr>
<tr>
<td></td>
<td>(Optional) Creates a description for the flow record.</td>
</tr>
<tr>
<td>Step 4</td>
<td>match [ipv4</td>
</tr>
<tr>
<td></td>
<td>or match datalink [destination-vlan-id</td>
</tr>
<tr>
<td></td>
<td>or match transport [icmp</td>
</tr>
<tr>
<td></td>
<td>Configures a key field for the flow record.</td>
</tr>
<tr>
<td></td>
<td>See the Cisco IOS Flexible NetFlow Configuration Guide and the Cisco IOS Flexible NetFlow Command Reference for more detailed information.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Repeat step 4 to configure additional fields for the record.</td>
</tr>
<tr>
<td>Step 6</td>
<td>collect counter [bytes [exported</td>
</tr>
<tr>
<td></td>
<td>or collect timestamp sys-uptime [first</td>
</tr>
<tr>
<td></td>
<td>or collect interface [input</td>
</tr>
<tr>
<td></td>
<td>Configures one or more source fields in the flow as counter fields, timestamp fields, or interface fields.</td>
</tr>
<tr>
<td></td>
<td>See the Cisco IOS Flexible NetFlow Configuration Guide and the Cisco IOS Flexible NetFlow Command Reference for more detailed information.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Repeat Step 6 as required to configure additional fields for the record.</td>
</tr>
<tr>
<td>Step 8</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
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
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config flow record</td>
<td>(Optional) Displays the configured flow records.</td>
</tr>
<tr>
<td>show flow record</td>
<td>(Optional) Displays the status of the flow records.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Configuring Flexible NetFlow

```plaintext
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:


**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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>flow exporter exporter-name</td>
<td>Creates the flow exporter and enters Flexible NetFlow flow exporter configuration mode. You can also use this command to modify an existing flow exporter.</td>
</tr>
<tr>
<td>3</td>
<td>description description</td>
<td>(Optional) Configures a description for the exporter that appears in the configuration and in the display of the <code>show flow exporter</code> command.</td>
</tr>
<tr>
<td>4</td>
<td>destination {hostname</td>
<td>ip-address} [vrf vrf-name]</td>
</tr>
<tr>
<td>5</td>
<td>dscp dscp</td>
<td>(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.</td>
</tr>
<tr>
<td>6</td>
<td>source interface-id</td>
<td>(Optional) Specifies the local interface from which the exporter uses the IP address as the source IP address for exported datagrams.</td>
</tr>
<tr>
<td>7</td>
<td>option {exporter-stats</td>
<td>interface-table</td>
</tr>
<tr>
<td>8</td>
<td>template data timeout seconds</td>
<td>(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.</td>
</tr>
<tr>
<td>9</td>
<td>transport udp udp-port</td>
<td>Specifies the UDP port on which the destination system is listening for exported datagrams. The range for <code>udp-port</code> is from 1 to 65536.</td>
</tr>
<tr>
<td>10</td>
<td>ttl seconds</td>
<td>(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.</td>
</tr>
<tr>
<td>11</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>12</td>
<td>show running-config flow exporter exporter-name</td>
<td>(Optional) Verifies the configured flow exporter.</td>
</tr>
<tr>
<td>13</td>
<td>show flow exporter exporter-name</td>
<td>(Optional) Displays the status of a flow exporter.</td>
</tr>
<tr>
<td>14</td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>
This example shows how to configure the flow exporter:

```plaintext
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:

```plaintext
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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>flow monitor monitor -name</code></td>
<td>Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode. You can also use this command to modify an existing flow monitor</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>description description</code></td>
<td>(Optional) Configures a description for the flow monitor.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>record record-name</code></td>
<td>Specifies the record for the flow monitor.</td>
</tr>
<tr>
<td>Step 5</td>
<td>`cache {timeout active seconds</td>
<td>type normal}`</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>timeout active seconds</strong>—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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>type normal</strong>—Configure normal flow removal from the flow cache.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> Although visible in the command line help, the entries keyword and inactive and update timeouts are not supported.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Repeat step 5 to configure additional cache parameters for the flow monitor.</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td><code>exporter exporter-name</code></td>
<td>(Optional) Specifies the name of an exporter that was created previously.</td>
</tr>
</tbody>
</table>
Chapter 1      Configuring Flexible NetFlow

This example shows how to configure a flow monitor:

```
Switch(config)# flow monitor FLOW-MONITOR-1
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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>interface interface-id</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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.
Chapter 1  Configuring Flexible NetFlow

Configuring Flexible NetFlow

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
```

### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>`[ip</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>exit</code></td>
</tr>
<tr>
<td>Step 5</td>
<td>Repeat steps 2 and 3 to configure additional cache parameters for the flow monitor.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>end</code></td>
</tr>
<tr>
<td>Step 7</td>
<td><code>show flow interface interface-id</code></td>
</tr>
<tr>
<td>Step 8</td>
<td><code>show flow monitor name monitor-name cache</code></td>
</tr>
<tr>
<td>Step 9</td>
<td><code>copy running-config startup-config</code></td>
</tr>
</tbody>
</table>
### Configuring and Enabling Flow Sampling

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>sampler sampler-name</td>
<td>Creates a flow monitor and enters Flexible NetFlow sampler configuration mode. You can also use this command to modify an existing sampler.</td>
</tr>
<tr>
<td>3</td>
<td>description description</td>
<td>(Optional) Configures a description for the sampler.</td>
</tr>
<tr>
<td>4</td>
<td>mode random 1 out-of window-size</td>
<td>Specifies the mode and window size from which to select packets. The window size range is from 2 to 32768. <em>Note</em> Although visible in the CLI help, the <code>mode deterministic</code> keyword is not supported.</td>
</tr>
<tr>
<td>5</td>
<td>exit</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td>6</td>
<td>interface interface-id</td>
<td>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.</td>
</tr>
<tr>
<td>7</td>
<td>{ip</td>
<td>ipv6} flow monitor monitor-name sampler sampler-name {input</td>
</tr>
<tr>
<td>8</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>9</td>
<td>show sampler sampler-name</td>
<td>(Optional) Displays the current status of a flow sampler.</td>
</tr>
<tr>
<td>10</td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>

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

```plaintext
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:

```plaintext
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,Bt0/0,I  2482 out of 4964
```