



Configuring NetFlow

Release 12.1
January 8, 2001

This chapter describes how to configure NetFlow in Cisco IOS Release 12.1 and Release 12.0S. For a complete description of NetFlow commands used in this chapter, refer to the *Cisco IOS Switching Services Command Reference*. For documentation on other commands that appear in this chapter, you can use the command reference master index or search online.

NetFlow Implementation

With NetFlow, you can export data (traffic statistics) to a remote workstation for processing.

NetFlow does not involve any connection-setup protocol either between routers or to any other networking device or end station and does not require any change externally—either to the traffic or packets themselves or to any other networking device. Thus, NetFlow is completely transparent to the existing network, including end stations and application software and network devices like LAN switches. Also, because NetFlow is performed independently on each internetworking device, it does not need to be operational on each router in the network. Network planners can selectively invoke NetFlow (and NetFlow data export) on a router or interface basis to gain traffic performance, control, or accounting benefits in specific network locations.



Note

NetFlow does consume additional memory and CPU resources; therefore, it is important to understand the resources required on your router before enabling NetFlow.

NetFlow Configuration Task List

To configure NetFlow, complete the tasks in the following sections. At a minimum, you must enable NetFlow. The remaining tasks are optional.

- Enabling NetFlow (Required)
- Exporting NetFlow Statistics (Optional)
- Customizing the Number of Entries in the NetFlow Cache (Optional)
- Managing NetFlow Statistics (Optional)
- Configuring IP Distributed Switching and NetFlow on VIP Interfaces (Optional)
- Configuring an Aggregation Cache (Optional)

- Configuring NetFlow Policy Routing (Optional)

Enabling NetFlow

To enable NetFlow, first configure the router for IP routing as described in the IP configuration chapters in the *Cisco IOS IP and IP Routing Configuration Guide*. After you configure IP routing, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	<code>interface type slot/port-adapter/port (Cisco 7500 series routers)</code> <code>interface type slot/port (Cisco 7200 series routers)</code>	Specifies the interface, and enter interface configuration mode.
Step 2	<code>ip route-cache flow</code>	Enables Netflow.

Exporting NetFlow Statistics

NetFlow information can also be exported to network management applications. To configure the router to export NetFlow statistics maintained in the NetFlow cache to a workstation when a flow expires, use one of the following commands in global configuration mode:

Command	Purpose
<code>ip flow-export ip-address udp-port [version 1]</code>	Configures the router to export NetFlow cache entries to a workstation if you are using receiving software that requires version 1. Version 1 is the default.
<code>ip flow-export ip-address udp-port version 5 [origin-as peer-as]</code>	Configures the router to export NetFlow cache entries to a workstation if you are using receiving software that accepts version 5. Optionally specify origin or peer autonomous system (AS). The default is to export neither AS which provides improved performance.

Customizing the Number of Entries in the NetFlow Cache

Normally the size of the NetFlow cache will meet your needs. However, you can increase or decrease the number of entries maintained in the cache to meet the needs of your NetFlow traffic rates. The default is 64K flow cache entries. Each cache entry is approximately 64 bytes of storage. Assuming a cache with the default number of entries, approximately 4 MB of DRAM would be required. Each time a new flow is taken from the free-flow queue, the number of free flows is checked. If there are only a few free flows remaining, NetFlow attempts to age 30 flows using an accelerated timeout. If there is only one free flow remaining, NetFlow automatically ages 30 flows regardless of their age. The intent is to ensure free flow entries are always available.

To customize the number of entries in the NetFlow cache, use the following command in global configuration mode:

Command	Purpose
<code>ip flow-cache entries number</code>	Changes the number of entries maintained in the NetFlow cache. The number of entries can be 1024 to 524288. The default is 65536.



Caution

We recommend that you not change the NetFlow cache entries. Improper use of this feature could cause network problems. To return to the default NetFlow cache entries, use the **no ip flow-cache entries** global configuration command.

Managing NetFlow Statistics

You can display and clear NetFlow statistics. NetFlow statistics consist of IP packet size distribution, IP NetFlow cache information, and flow information such as the protocol, total flow, flows per second, and so forth. The resulting information can be used to find out information about your router traffic. To manage NetFlow statistics, use either of the following commands in privileged EXEC mode:

Command	Purpose
<code>show ip cache flow</code>	Displays the NetFlow statistics.
<code>clear ip flow stats</code>	Clears the NetFlow statistics.

Configuring IP Distributed Switching and NetFlow on VIP Interfaces

On Cisco 7500 series routers with a Route Switch Processor (RSP) and with Versatile Interface Processor (VIP) controllers, the VIP hardware can be configured to switch packets received by the VIP with no per-packet intervention on the part of the RSP. This process is called *distributed switching*. Distributed switching decreases the demand on the RSP.

The VIP hardware can also be configured for NetFlow, a new high-performance feature that caches information about the flow. NetFlow data can also be exported to network management applications.

Refer to the Cisco Product Catalog for information about VIP port adapters used for distributed switching.

To configure distributed switching on the VIP, first configure the router for IP routing as described in this chapter and the various routing protocol chapters, depending on the protocols you use.

After you configure IP routing, use the following commands beginning in global configuration mode:

Command	Purpose
Step 1 <code>interface type slot/port-adapter/port</code>	Specifies the interface, and enter interface configuration mode.

	Command	Purpose
Step 2	<code>ip route-cache distributed</code>	Enables VIP distributed switching of IP packets on the interface.
Step 3	<code>ip route-cache flow</code>	Enables Netflow.

When the RSP or VIP is using NetFlow, it uses a flow cache instead of a destination network cache to switch IP packets. The flow cache uses source and destination network address, protocol, and source and destination port numbers to distinguish entries.

To export NetFlow cache entries to a workstation when a flow expires, use the following command in global configuration mode:

Command	Purpose
<code>ip flow-export ip-address udp-port</code>	Configures the router to export NetFlow cache entries to a workstation.

Configuring an Aggregation Cache

To configure an aggregation cache, you must enter aggregation cache configuration mode, and you must decide which type of aggregation scheme you would like to configure: autonomous system, Destination Prefix, Prefix, Protocol Prefix, or Source Prefix aggregation cache. Once you define the aggregation scheme, define the operational parameters for that scheme.

	Command	Purpose
Step 1	<code>Router(config)# ip flow-aggregation cache as</code>	Enters aggregation cache configuration mode and enables an aggregation cache scheme (as, destination-prefix, prefix, protocol-port, or source-prefix)
Step 2	<code>Router(config-flow-cache)# cache entries 2046</code>	Specifies the number (in this example, 2046) of cache entries to allocate for the autonomous system aggregation cache.
Step 3	<code>Router(config-flow-cache)# cache timeout inactive 199</code>	Specifies the number of seconds (in this example, 199) that an inactive entry is allowed to remain in the aggregation cache before it is deleted.
Step 4	<code>Router(config-flow-cache)# cache timeout active 45</code>	Specifies the number of minutes (in this example, 45) that an active entry is active.
Step 5	<code>Router(config-flow-cache)# export destination 10.42.41.1 9991</code>	Enables the data export.
Step 6	<code>Router(config-flow-cache)# enabled</code>	Enables aggregation cache creation.

Verifying Aggregation Cache Configuration and Data Export

To verify the aggregation cache information, use the following command in EXEC mode:

Command	Purpose
<code>show ip cache flow aggregation</code>	Displays the aggregation cache information.

To confirm data export, use the following command in EXEC mode:

Command	Purpose
<code>show ip flow export</code>	Displays the statistics for the data export including the main cache and all other enabled caches.

Configuring NetFlow Policy Routing

As long as policy routing is configured, NetFlow policy routing is enabled by default and cannot be disabled. That is, NPR is the default policy routing mode. No configuration tasks are required to enable policy routing in conjunction with CEF, dCEF, or NetFlow. As soon as one of these features is turned on, packets are automatically subject to policy routing in the appropriate switching path.

There is one new, optional configuration command (**set ip next-hop verify-availability**). This command has the following restrictions:

- It can cause some performance degradation.
- CDP must be configured on the interface.
- The direct next hop must be a Cisco device with CDP enabled.
- It is not available in dCEF, due to the dependency of the CDP neighbor database.

It is assumed that policy routing itself is already configured.

If the router is policy routing packets to the next hop and the next hop happens to be down, the router will try unsuccessfully to use Address Resolution Protocol (ARP) for the next hop (which is down). This behavior will continue forever.

To prevent this situation, you can configure the router to first verify that the next hop(s) of the route map is the router's CDP neighbor(s) before routing to that next hop.

This task is optional because some media or encapsulations do not support CDP, or it may not be a Cisco device that is sending the router traffic.

To configure the router to verify that the next hop is a CDP neighbor before the router tries to policy route to it, use the following command in route-map configuration mode:

Command	Purpose
<code>set ip next-hop verify-availability</code>	Causes the router to confirm that the next hop(s) of the route map is a CDP neighbor(s) of the router.

If the command shown is set and the next hop is not a CDP neighbor, the router looks to the subsequent next hop, if there is one. If there is none, the packets simply are not policy routed.

If the command shown is not set, the packets are either successfully policy routed or remain forever unrouted.

If you want to selectively verify availability of only some next hops, you can configure different route-map entries (under the same route-map name) with different criteria (using access list matching or packet size matching), and use the **set ip next-hop verify-availability** command selectively.

Monitoring NetFlow Policy Routing

Typically, you would use existing policy routing and NetFlow **show** commands to monitor these features. For more information on these **show** commands, refer to the policy routing and NetFlow documentation.

To display the route map Inter Processor Communication (IPC) message statistics in the RP or VIP, use the following command in EXEC mode:

Command	Purpose
<code>show route-map ipc</code>	Displays the route map IPC message statistics in the RP or VIP.

NetFlow Configuration Examples

This section provides the following basic configuration examples:

- NetFlow Configuration Example
- NetFlow Aggregation Configuration Examples
- NetFlow Policy Routing Example

NetFlow Configuration Example

The following example shows how to modify the configuration of serial interface 3/0/0 to enable NetFlow and to export the flow statistics for further processing to UDP port 0 on a workstation with the IP address of 1.1.15.1. In this example, existing NetFlow statistics are cleared to ensure accurate information when the **show ip cache flow** command is executed to view a summary of the NetFlow statistics.

```
configure terminal
interface serial 3/0/0
 ip route-cache flow
 exit
 ip flow-export 1.1.15.1 0 version 5 peer-as
 exit
clear ip flow stats
```

NetFlow Aggregation Configuration Examples

This section provides the following aggregation cache configuration examples:

- Autonomous System Configuration Example
- Destination Prefix Configuration Example
- Prefix Configuration Example
- Protocol Port Configuration Example
- Source Prefix Configuration Example

Autonomous System Configuration Example

The following example shows how to configure an autonomous system aggregation cache with a cache size of 2046, an inactive timeout of 200 seconds, a cache active timeout of 45 minutes, an export destination IP address of 10.42.42.1, and a destination port of 9992.

```
Router(config)# ip flow-aggregation cache as
Router(config-flow-cache)# cache entries 2046
Router(config-flow-cache)# cache timeout inactive 200
Router(config-flow-cache)# cache timeout active 45
Router(config-flow-cache)# export destination 10.42.42.1 9992
Router(config-flow-cache)# enabled
```

Destination Prefix Configuration Example

The following example shows how to configure a Destination Prefix aggregation cache with a cache size of 2046, an inactive timeout of 200 seconds, a cache active timeout of 45 minutes, an export destination IP address of 10.42.42.1, and a destination port of 9992.

```
Router(config)# ip flow-aggregation cache destination-prefix
Router(config-flow-cache)# cache entries 2046
Router(config-flow-cache)# cache timeout inactive 200
Router(config-flow-cache)# cache timeout active 45
Router(config-flow-cache)# export destination 10.42.42.1 9992
Router(config-flow-cache)# enabled
```

Prefix Configuration Example

The following example shows how to configure a Prefix aggregation cache with a cache size of 2046, an inactive timeout of 200 seconds, a cache active timeout of 45 minutes, an export destination IP address of 10.42.42.1, and a destination port of 9992.

```
Router(config)# ip flow-aggregation cache prefix
Router(config-flow-cache)# cache entries 2046
Router(config-flow-cache)# cache timeout inactive 200
Router(config-flow-cache)# cache timeout active 45
Router(config-flow-cache)# export destination 10.42.42.1 9992
Router(config-flow-cache)# enabled
```

Protocol Port Configuration Example

The following example shows how to configure a Protocol Port aggregation cache with a cache size of 2046, an inactive timeout of 200 seconds, a cache active timeout of 45 minutes, an export destination IP address of 10.42.42.1, and a destination port of 9992.

```
Router(config)# ip flow-aggregation cache protocol-port
Router(config-flow-cache)# cache entries 2046
Router(config-flow-cache)# cache timeout inactive 200
Router(config-flow-cache)# cache timeout active 45
Router(config-flow-cache)# export destination 10.42.42.1 9992
Router(config-flow-cache)# enabled
```

Source Prefix Configuration Example

The following example shows how to configure a Source Prefix aggregation cache with a cache size of 2046, an inactive timeout of 200 seconds, a cache active timeout of 45 minutes, an export destination IP address of 10.42.42.1, and a destination port of 9992.

```
Router(config)# ip flow-aggregation cache source-prefix
Router(config-flow-cache)# cache entries 2046
Router(config-flow-cache)# cache timeout inactive 200
Router(config-flow-cache)# cache timeout active 45
Router(config-flow-cache)# export destination 10.42.42.1 9992
Router(config-flow-cache)# enabled
```

NetFlow Policy Routing Example

The following example configures CEF and NetFlow. It also configures policy routing to verify that next hop 50.0.0.8 of route map *test* is a CDP neighbor before the router tries to policy route to it.

If the first packet is being policy routed via route map *test* sequence 10, the subsequent packets of the same flow always take the same route map *test* sequence 10, not route map *test* sequence 20, because they all match or pass access list 1 check.

```
ip cef
interface ethernet0/0/1
 ip route-cache flow
 ip policy route-map test
route-map test permit 10
 match ip address 1
  set ip precedence priority
  set ip next-hop 50.0.0.8
  set ip next-hop verify-availability
route-map test permit 20
 match ip address 101
  set interface Ethernet0/0/3
  set ip tos max-throughput
```

This document published January 8, 2001. Last content update: January 7, 2004