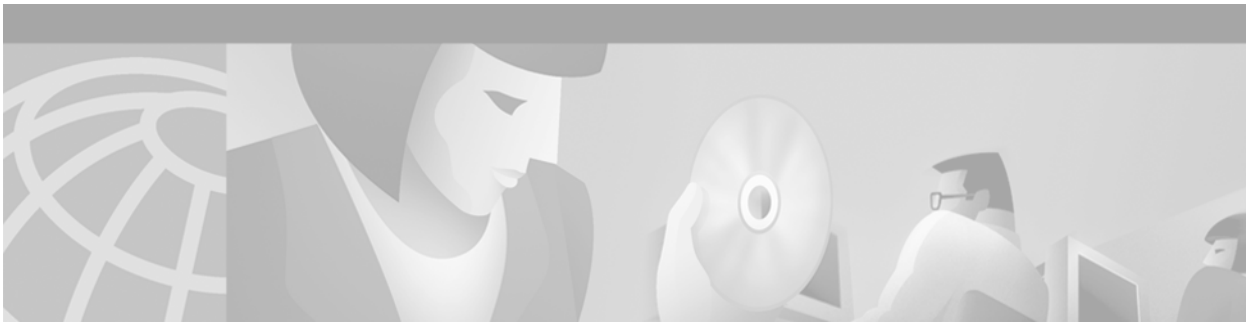

Configuring NetFlow

This chapter describes how to configure NetFlow data accounting on your routing devices.

For a complete description of the commands in this chapter, refer to the the *Cisco IOS Switching Services Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the section "Finding Support Information for Platforms and Cisco IOS Software Images" in the chapter "Using Cisco IOS Software."

What is NetFlow?

NetFlow enables you to collect traffic flow statistics on your routing devices. NetFlow is based on identifying packet flows for ingress IP packets. It 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. NetFlow is completely transparent to the existing network, including end stations and application software and network devices like LAN switches. Also, NetFlow is performed independently on each internetworking device, it need not be operational on each router in the network. Using NetFlow Data Export (NDE), you can export data to a remote workstation for data collection and further processing. Network planners can selectively invoke NDE on a router or on a per-subinterface 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, perform the tasks described in the following sections. The task in the first section is required; 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 and NetFlow on VIP Interfaces (Optional)
- Configuring an Aggregation Cache (Optional)
- Configuring a NetFlow Minimum Prefix Mask for Router-Based Aggregation (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 Configuration Guide, Volume 2 of 3: Routing Protocols*. After you configure IP routing, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface type slot/port-adapter/port` (Cisco 7500 series routers) or `Router(config)# interface type slot/port` (Cisco 7200 series routers)	Specifies the interface, and enter interface configuration mode.
Step 2	`Router(config-if)# ip route-cache flow`	Enables NetFlow for IP routing.

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 either of the following commands in global configuration mode:

Command	Purpose
`Router(config)# ip flow-export` *ip-address udp-port* [**version 1**]	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.
`Router(config)# ip flow-export` *ip-address udp-port* **version 5** [**origin-as** | **peer-as**]	Configures the router to export NetFlow cache entries to a workstation if you are using receiving software that accepts version 5. Optionally specify the origin or peer autonomous system. The default is to export neither AS that provides improved performance. **Caution** Entering the **ip flow-export** or **no ip flow-export** command on the Cisco 12000 Series Internet Routers and specifying any version format other than version 1 (in other words, entering the **ip flow-export** or **no ip flow-export** command and specifying either the **version 5** or **version 9** keyword) causes packet forwarding to stop for a few seconds while NetFlow reloads the route processor and line card CEF tables. To avoid interruption of service to a live network, apply this command during a change window, or include it in the startup-config file to be executed during a router reboot.

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 requires about 64 bytes of storage. Assuming a cache with the default number of entries, about 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 only a few free flows remain, NetFlow attempts to age 30 flows using an accelerated timeout. If only one free flow remains, NetFlow automatically ages 30 flows regardless of their age. The intent is to ensure that 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
`Router(config)# ip flow-cache entries` *number*	Changes the number of entries maintained in the NetFlow cache. The number of entries can be from 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 flow cache information, and flow information such as the protocol, total flow, flows per second, and so on. The resulting information can be used to determine information about your router traffic. To manage NetFlow statistics, use the following commands in privileged EXEC mode as needed:

Command	Purpose
`Router# show ip cache flow`	Displays the NetFlow statistics.
`Router# clear ip flow stats`	Clears the NetFlow statistics.

Configuring IP Distributed 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 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	`Router(config)# interface` *type slot/port-adapter/port*	Specifies the interface, and enters interface configuration mode.
Step 2	`Router(config-if)# ip route-cache distributed`	Enables VIP distributed switching of IP packets on the interface.
Step 3	`Router(config-if)# ip route-cache flow`	Enables NetFlow.

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

Command	Purpose
`Router(config)# ip flow-export ip-address udp-port`	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	`Router(config)# ip flow-aggregation cache as`	Enters aggregation cache configuration mode and enables an aggregation cache scheme (as, destination-prefix, prefix, protocol-port, or source-prefix).
Step 2	`Router(config-flow-cache)# cache entries 2046`	Specifies the number (in this example, 2046) of cache entries to allocate for the Autonomous System aggregation cache.
Step 3	`Router(config-flow-cache)# cache timeout inactive 199`	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	`Router(config-flow-cache)# cache timeout active 45`	Specifies the number of minutes (in this example, 45) that an active entry is active.
Step 5	`Router(config-flow-cache)# export destination 10.42.41.1 9991`	Enables the data export.
Step 6	`Router(config-flow-cache)# enabled`	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
`Router# show ip cache flow aggregation`	Displays the aggregation cache information.

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

Command	Purpose
`Router# show ip flow export`	Displays the statistics for the data export including the main cache and all other enabled caches.

Configuring a NetFlow Minimum Prefix Mask for Router-Based Aggregation

To configure NetFlow Minimum Prefix Mask for Router-Based Aggregation feature, perform the tasks described in the following sections. Each task is optional.

- Configuring the Minimum Mask of a Prefix Aggregation Scheme (Optional)
- Configuring the Minimum Mask of a Destination-Prefix Aggregation Scheme (Optional)
- Configuring the Minimum Mask of a Source-Prefix Aggregation Scheme (Optional)

Per form the following section to verify your NetFlow aggregation configuration:

- Monitoring and Maintaining Minimum Masks for Aggregation Schemes (Optional)

Configuring the Minimum Mask of a Prefix Aggregation Scheme

To configure the minimum mask of a prefix aggregation scheme, use the following commands beginning in aggregation cache configuration mode:

	Command	Purpose
Step 1	`Router(config)# ip flow-aggregation cache prefix`	Configures the prefix aggregation cache.
Step 2	`Router(config-flow-cache)# mask source minimum value`	Specifies the minimum value for the source mask.
Step 3	`Router(config-flow-cache)# mask destination minimum value`	Specifies minimum value for the destination mask.

Configuring the Minimum Mask of a Destination-Prefix Aggregation Scheme

To configure the minimum mask of a destination-prefix aggregation scheme, use the following commands beginning in aggregation cache configuration mode:

	Command	Purpose
Step 1	`Router(config)# ip flow-aggregation cache destination-prefix`	Configures the destination aggregation cache.
Step 2	`Router(config-flow-cache)# mask destination minimum value`	Specifies the minimum value for the destination mask.

Configuring the Minimum Mask of a Source-Prefix Aggregation Scheme

To configure the minimum mask of a source-prefix aggregation scheme, use the following commands beginning in aggregation cache configuration mode:

	Command	Purpose
Step 1	`Router(config)# ip flow-aggregation cache source-prefix`	Configures the source-prefix aggregation cache.
Step 2	`Router(config-flow-cache)# mask source minimum value`	Specifies the minimum value for the source mask.

Monitoring and Maintaining Minimum Masks for Aggregation Schemes

To view the configured value of the minimum mask, use the following commands for each aggregation scheme in EXEC mode, as needed:

Command	Purpose
`Router# show ip cache flow aggregation prefix`	Displays the configured value of the minimum mask in the prefix aggregation scheme.
`Router# show ip cache flow aggregation destination-prefix`	Displays the configured value of the minimum mask in the destination-prefix aggregation scheme.
`Router# show ip cache flow aggregation source-prefix`	Displays the configured value of the minimum mask in the source-prefix aggregation scheme.

Note If the minimum mask has not been explicitly configured, no minimum mask information is displayed. The default value of the minimum mask is zero. The configurable range for the minimum mask is from 1 to 32. An appropriate value should be chosen by the user depending on the traffic. A higher value of the minimum mask will provide more detailed network addresses, but it may also result in increased number of flows in the aggregation cache.

Configuring NetFlow Policy Routing

As long as policy routing is configured, NetFlow policy routing (NPR) 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 or dCEF. 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 optional configuration command (**set ip next-hop verify-availability** route-map configuration command). 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 hops of the route map are CDP neighbors of the router 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
`Router(config-route-map)# set ip next-hop verify-availability`	Causes the router to confirm that the next hops of the route map are CDP neighbors 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** route-map configuration command selectively.

Monitoring NetFlow Policy Routing

Typically, you would use existing policy routing and NetFlow **show** EXEC 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
`Router# show route-map ipc`	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
- Setting a NetFlow Minimum Prefix Mask for Router-Based Aggregation Examples

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 in privileged EXEC mode is entered 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
```

The following is a sample display of a main cache using the **show ip cache flow** command:

```
Router# show ip cache flow

IP packet size distribution (230151 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .999 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

   512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
```

The preceding output shows the percentage distribution of packets by size range. In this display, 99.9 percent of the packets fall in the size range from 1 to 32 bytes.

```
IP Flow Switching Cache, 4456448 bytes
  65509 active, 27 inactive, 820628747 added
  955454490 ager polls, 0 flow alloc failures
  Exporting flows to 1.1.15.1 (2057)
  820563238 flows exported in 34485239 udp datagrams, 0 failed
  last clearing of statistics 00:00:03

Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-BGP             71      0.0         1    49      0.0       2.5      15.8
UDP-other           17      0.0         1   328      0.0       0.0      15.7
ICMP             18966      6.7        10    28     72.9       0.1      22.9
Total:           19054      6.7        10    28     72.9       0.1      22.9

SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
Et1/1          52.52.52.1      Fd4/0          42.42.42.1      01 55  10    3748
0000 /8  50                    0000 /8  40    202.120.130.2          28    17.8
Et1/2          52.52.52.1      Fd4/0          42.42.42.1      01 CC  10    3568
0000 /8  50                    0000 /8  40    202.120.130.2          28    17.8
Et1/2          10.1.3.2        Fd4/0          42.42.42.1      01 C0  10    1124
0000 /0  0                     0000 /8  40    202.120.130.2          28    17.8
Et1/2          11.1.3.2        Fd4/0          42.42.42.1      01 C0  10    1157
0000 /0  0                     0000 /8  40    202.120.130.2          28    17.7
Et1/2          14.1.3.2        Fd4/0          42.42.42.1      01 C0  10    1149
0000 /0  0                     0000 /8  40    202.120.130.2          28    17.8
Et1/2          15.1.3.2        Fd4/0          42.42.42.1      01 C0  10    1127
0000 /0  0                     0000 /8  40    202.120.130.2          28    17.7
Et1/2          12.1.3.2        Fd4/0          42.42.42.1      01 C0  10    1204
0000 /0  0                     0000 /8  40    202.120.130.2          28    17.8
Et1/2          13.1.3.2        Fd4/0          42.42.42.1      01 C0  10    1159
0000 /0  0                     0000 /8  40    202.120.130.2          28    17.8
Et1/2          18.1.3.2        Fd4/0          42.42.42.1      01 C0  10    1223
0000 /0  0                     0000 /8  40    202.120.130.2          28    17.8
Et1/2          19.1.3.2        Fd4/0          42.42.42.1      01 C0  10    1264
0000 /0  0                     0000 /8  40    202.120.130.2          28    17.8
Et1/2          16.1.3.2        Fd4/0          42.42.42.1      01 C0  10    1170
0000 /0  0                     0000 /8  40    202.120.130.2          28    17.8
Et1/2          17.1.3.2        Fd4/0          42.42.42.1      01 C0  10    1167
0000 /0  0                     0000 /8  40    202.120.130.2          28    17.8
Et1/2          22.1.3.2        Fd4/0          42.42.42.1      01 C0  10    1193
```

```
0000 /0   0                    0000 /8   40    202.120.130.2          28    17.8
Et1/2           23.1.3.2       Fd4/0           42.42.42.1       01 C0  10    1212
0000 /0   0                    0000 /8   40    202.120.130.2          28    17.7
Et1/1           50.50.50.1     Local           31.31.31.1       06 C0  18       2
00B3 /32  0                    2AF8 /32  0     0.0.0.0                49    10.1
Et1/0           8.8.8.8        Et0/0*          9.9.9.9          01 00  10       3
0000 /8   302                  0800 /8   300   3.3.3.3                100     0.1
```

Note The very last entry in the "DstIf" field has an asterisk (*) next to the destination interface. The asterisk (*) immediately following the "DstIf" field indicates that the flow being shown is an egress flow.

Table 19 describes the significant fields shown in the flow switching cache lines of the display.

Table 19 show ip cache flow Field Descriptions in Flow Switching Cache Display

Field	Description
bytes	Number of bytes of memory used by the NetFlow cache.
active	Number of active flows in the NetFlow cache at the time this command was entered.
inactive	Number of flow buffers that are allocated in the NetFlow cache, but were not currently assigned to a specific flow at the time this command was entered.
added	Number of flows created since the start of the summary period.
ager polls	Number of times the NetFlow code looked at the cache to cause entries to expire (used by Cisco for diagnostics only).
flow alloc failures	Number of times the NetFlow code tried to allocate a flow but could not.
Exporting flows	IP address and User Datagram Protocol (UDP) port number of the workstation to which flows are exported.
flows exported in udp datagrams	Total number of flows exported and the total number of UDP datagrams used to export the flows to the workstation.
failed	Number of flows that could not be exported by the router because of output interface limitations.
last clearing of statistics	Standard time output (hh:mm:ss) since the **clear ip flow stats** privileged EXEC command was executed. This time output changes to hours and days after the time exceeds 24 hours.

Table 20 describes the significant fields shown in the activity by protocol lines of the display.

Table 20 show ip cache flow Field Descriptions in Activity by Protocol Display

Field	Description
Protocol	IP protocol and the well-known port number as described in RFC 1340.
Total Flows	Number of flows for this protocol since the last time statistics were cleared.
Flows/Sec	Average number of flows for this protocol seen per second; equal to total flows/number of seconds for this summary period.

Table 20 show ip cache flow Field Descriptions in Activity by Protocol Display (continued)

Field	Description
Packets/Flow	Average number of packets observed for the flows seen for this protocol. Equal to total packets for this protocol or number of flows for this protocol for this summary period.
Bytes/Pkt	Average number of bytes observed for the packets seen for this protocol (total bytes for this protocol or total number of packet for this protocol for this summary period).
Packets/Sec	Average number of packets for this protocol per second (total packets for this protocol) or total number of seconds for this summary period.
Active(Sec)/Flow	Sum of all the seconds from the first packet to the last packet of an expired flow (for example, TCP FIN, timeout, and so on), in seconds or total flows for this protocol for this summary period.
Idle(Sec)/Flow	Sum of all the seconds from the last packet seen in each nonexpired flow for this protocol until the time at which this command was entered, in seconds or total flows for this protocol for this summary period.

Table 21 describes the significant fields in the NetFlow record lines of the display.

Table 21 show ip cache verbose flow Field Descriptions in NetFlow Record Display

Field	Description
SrcIf	Interface on which the packet was received.
Port Msk AS	Source Border Gateway Protocol (BGP) autonomous system. This is always set to 0 in MPLS flows.
SrcIPaddress	IP address of the device that transmitted the packet.
DstIf	Interface from which the packet was transmitted. **Note** The DstIf interface can be reported as "Null" if the packets are any of the following: • Blocked by an ACL • Process-switched • Multicast traffic • Locally-generated traffic • Tunnels (IPIP, GRE, IPSEC, L2TP) • Web Cache Communication Protocol (WCCP) • Using a static route to a Null0 interface • Dropped by Quality of Service (QoS) rules (for example, Committed Access Rate or Policing) The following rules apply to QoS traffic: • The DstIf information is correct if the traffic is not dropped by QoS • The DstIf will be reported as "Null" when the traffic is dropped due to QoS rules.
Port Msk AS	Destination BGP autonomous system. This is always set to 0 in MPLS flows.

Table 21 show ip cache verbose flow Field Descriptions in NetFlow Record Display (continued)

Field	Description
DstIPaddress	IP address of the destination device.
NextHop	Specifies the BGP next-hop address. This is always set to 0 in MPLS flows.
Pr	IP protocol well-known port number as described in RFC 1340, displayed in hexadecimal format.
B/Pk	Average number of bytes observed for the packets seen for this protocol (total bytes for this protocol or the total number of flows for this protocol for this summary period).
Flgs	TCP flags (result of bitwise OR of TCP flags from all packets in the flow).
Active	Number of active flows in the NetFlow cache at the time this command was entered.
Pkts	Number of packets switched through this flow.

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
```

Setting a NetFlow Minimum Prefix Mask for Router-Based Aggregation Examples

This section provides the following NetFlow minimum prefix mask aggregation cache configuration examples:

- Prefix Aggregation Scheme Example
- Destination-Prefix Aggregation Scheme Example
- Source-Prefix Aggregation Scheme Example

Prefix Aggregation Scheme Example

```
!
ip flow-aggregation cache prefix
mask source minimum 24
```

```
mask destination minimum 28
```

Destination-Prefix Aggregation Scheme Example

```
!
ip flow-aggregation cache destination-prefix
mask destination minimum 32
!
```

Source-Prefix Aggregation Scheme Example

```
ip flow-aggregation cache source-prefix
mask source minimum 30
!
```

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 named 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
```