Configuring NetFlow Accounting for Unicast and Multicast on GRE IP Tunnel Interfaces

Last Updated: November 28, 2011

This document contains information about and instructions for configuring NetFlow Accounting for Unicast and Multicast on generic routing encapsulation (GRE) IP Tunnel Interfaces. NetFlow multicast accounting allows you to capture multicast-specific data (both packets and bytes) for multicast flows.

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

• Finding Feature Information, page 1
• Prerequisites for Configuring NetFlow Accounting for Unicast and Multicast on GRE IP Tunnel Interfaces, page 2
• Restrictions for Configuring NetFlow Accounting for Unicast and Multicast on GRE IP Tunnel Interfaces, page 2
• Information About NetFlow Accounting for Unicast and Multicast on GRE IP Tunnel Interfaces, page 2
• How to Configure NetFlow Accounting for Unicast and Multicast on GRE Tunnel Interfaces, page 7
• Configuration Examples for NetFlow Accounting for Unicast and Multicast on GRE Tunnel Interfaces, page 22
• Additional References, page 24
• Feature Information for Configuring NetFlow Accounting for Unicast and Multicast on GRE IP Tunnel Interfaces, page 25

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 Configuring NetFlow Accounting for Unicast and Multicast on GRE IP Tunnel Interfaces

- You must use the Per-interface NetFlow feature in conjunction with the NetFlow Accounting for Unicast and Multicast on GRE Tunnel Interfaces feature.
- The instructions for configuring IPv4 unicast routing are not included in this document. If you want to configure NetFlow accounting for IPv4 unicast traffic on a GRE IP interface, your switch must already be configured for IPv4 unicast routing.
- The instructions for configuring IPv4 multicast routing are not included in this document. If you want to configure NetFlow accounting for IPv4 multicast traffic on a GRE IP interface, your switch must already be configured for IPv4 multicast routing.

Restrictions for Configuring NetFlow Accounting for Unicast and Multicast on GRE IP Tunnel Interfaces

- Only Catalyst 6500 series switches with a supervisor 720 is supported.
- Multicast flow packet and byte counters will be updated only in PFC3B mode and above.
- Only hardware switched flows are supported.
- Only Version 9 NetFlow data export format is supported.

Information About NetFlow Accounting for Unicast and Multicast on GRE IP Tunnel Interfaces

- GRE Tunneling, page 2
- GRE Tunnel Keepalive, page 3
- Tunnel Interfaces, page 3
- NetFlow Accounting on GRE IP Tunnel Interfaces, page 3

GRE Tunneling

Generic routing encapsulation (GRE) tunneling is defined in RFC 2784. GRE is a carrier protocol that can be used with a variety of underlying transport protocols and that can carry a variety of passenger protocols. RFC 2784 also covers the use of GRE with IPv4 as the transport protocol and the passenger protocol. For
more information on GRE tunnels, see the *Cisco IOS Interface and Hardware Component Configuration Guide*. The figure below is an example of a typical implementation of a GRE IP tunnel.

**Figure 1**  
Sample Network with a GRE IPv4 Tunnel

![Sample Network with a GRE IPv4 Tunnel](image)

**GRE Tunnel Keepalive**

Keepalive packets can be configured to be sent over IP-encapsulated GRE tunnels. You can specify the rate at which keepalives will be sent and the number of times that a device will continue to send keepalive packets without a response before the interface becomes inactive. GRE keepalive packets may be sent from both sides of a tunnel or from just one side.

**Tunnel Interfaces**

A tunnel interface is used to pass protocol traffic across a network that does not normally support the protocol. To build a tunnel requires defining a tunnel interface on each of two routers. The tunnel interfaces must reference each other. At each router, the tunnel interface must be configured with a Layer 3 address. The tunnel endpoints, tunnel source, and tunnel destination must be defined, and the type of tunnel must be selected. Optional steps can be performed to customize the tunnel.

Remember to configure the router at each end of the tunnel. If only one side of a tunnel is configured, the tunnel interface may still come up and stay up (unless keepalive is configured), but packets going into the tunnel will be dropped.

In Cisco IOS Release 12.2(8)T and later releases, Cisco express forwarding (CEF) switching over multipoint GRE tunnels was introduced. Previously, only process switching was available for multipoint GRE tunnels.

**NetFlow Accounting on GRE IP Tunnel Interfaces**

To analyze traffic that is sent from c3825 to c3745 in the figure below, NetFlow accounting is configured as shown in the table below. The flows in the “Flows” column are shown in the Unicast IPv4 Traffic over
When you configure NetFlow accounting for IPv4 unicast traffic on a GRE tunnel interface, the traffic that is encapsulated or de-encapsulated on the router results in the creation of two flows. See the Unicast IPv4 Traffic over an IPv4 Unicast GRE Tunnel (Encapsulation) figure and the Unicast IPv4 Traffic over an IPv4 Unicast GRE Tunnel (De-encapsulation) figure. When you configure NetFlow accounting for IPv4 multicast traffic on a GRE tunnel interface, the traffic that is encapsulated or de-encapsulated on the router results in the creation of three flows. See the Multicast IPv4 Traffic over an IPv4 Unicast GRE Tunnel (Encapsulation) figure and the Multicast IPv4 Traffic over an IPv4 Unicast GRE Tunnel (De-encapsulation) figure. The increase in the number of flows created results in an increase in the usage of the hardware NetFlow table. You must monitor the hardware NetFlow table on your router to ensure that it is not oversubscribed.

If you are using NetFlow data export, the number of exported flows is also increased. Flows from the hardware table are converted to the Version 9 export format and then exported. Because the number of flows is doubled when you configure NetFlow Data Export, twice as much memory is required to convert the flows to Version 9 export format and then export them.

The table below provides the definitions of the terms used in the figures below.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>encapsulation</td>
<td>Adding the GRE tunnel header and trailer to the beginning and end respectively, of the packet being transmitted over the GRE tunnel.</td>
</tr>
</tbody>
</table>

### Table 1: Where to Configure NetFlow Accounting and Which NetFlow Commands to Configure

<table>
<thead>
<tr>
<th>Encapsulation/De-encapsulation</th>
<th>Router</th>
<th>Ingress Physical Interface</th>
<th>Ingress Tunnel Interface</th>
<th>Egress Physical Interface</th>
<th>Egress Tunnel Interface</th>
<th>Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Direction</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unicast over GRE (encap)</td>
<td>C650002</td>
<td>ip flow ingress on interface gigabit 3/1</td>
<td>No configuration</td>
<td>ip flow egress on interface tunnel 0</td>
<td>Flow (1) Flow (2)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C3825 to C3745</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unicast over GRE (decap)</td>
<td>C65003</td>
<td>ip flow ingress on interface gigabit 5/2</td>
<td>ip flow ingress on interface tunnel 0</td>
<td>No configuration</td>
<td>No configuration</td>
<td>Flow (1) Flow (2)</td>
</tr>
<tr>
<td></td>
<td>C3825 to C3745</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multicast over GRE (encap)</td>
<td>C650002</td>
<td>ip flow ingress on interface gigabit 3/1</td>
<td>No configuration</td>
<td>ip flow egress on interface 6/2</td>
<td>Flow (1) Flow (2) Flow (3)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C3825 to 3C745</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multicast over GRE (decap)</td>
<td>C65003</td>
<td>ip flow ingress on interface gigabit 5/2</td>
<td>ip flow ingress on interface tunnel 0</td>
<td>ip flow egress on interface 1/1</td>
<td>No configuration</td>
<td>Flow (1) Flow (2) Flow (3)</td>
</tr>
<tr>
<td></td>
<td>C3825 to C3745</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### NetFlow Accounting on GRE IP Tunnel Interfaces

#### Information About NetFlow Accounting for Unicast and Multicast on GRE IP Tunnel Interfaces

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>de-encapsulation</td>
<td>Removing the GRE tunnel header and trailer from the beginning and end respectively, of the packet being received from the GRE tunnel.</td>
</tr>
<tr>
<td>ingress</td>
<td>The inbound path of traffic. For example, the ingress interface is the interface over which traffic is received.</td>
</tr>
<tr>
<td>egress</td>
<td>The outbound path of traffic. For example, the egress interface is the interface over which traffic is transmitted.</td>
</tr>
<tr>
<td>ID</td>
<td>Destination IP address.</td>
</tr>
<tr>
<td>IS</td>
<td>Source IP address.</td>
</tr>
<tr>
<td>TD</td>
<td>Destination IP address for the tunnel interface.</td>
</tr>
<tr>
<td>TS</td>
<td>Source IP address for the tunnel interface.</td>
</tr>
<tr>
<td>MD</td>
<td>Multicast destination IP address.</td>
</tr>
<tr>
<td>MS</td>
<td>Multicast source IP address.</td>
</tr>
<tr>
<td>payload</td>
<td>The packet data.</td>
</tr>
</tbody>
</table>

The figure below shows the packet encapsulation process for unicast IPv4 traffic that is received on interface Gigabit Ethernet 3/1 on c65002 in the figure above. The first flow is the result of NetFlow accounting for the traffic after it is received on physical interface 3/1 (ingress NetFlow). The second flow is the result of NetFlow accounting for the traffic as it is being transmitted on the GRE tunnel interface T0 (egress NetFlow).

**Figure 2**  
*Unicast IPv4 Traffic over an IPv4 Unicast GRE Tunnel (Encapsulation)*

The figure below shows the packet de-encapsulation process for unicast IPv4 traffic that is received on interface Gigabit Ethernet 3/1 on c65002 in the Sample Network with a GRE IPv4 Tunnel figure. The first flow is the result of NetFlow accounting for the traffic after it is received on the physical interface 5/2
(ingress NetFlow). The second flow is the result of NetFlow accounting for the traffic as it is being received and de-encapsulated on the tunnel interface T0 (ingress NetFlow).

**Figure 3**  **Unicast IPv4 Traffic over an IPv4 Unicast GRE Tunnel (De-encapsulation)**

During de-encapsulation, only ingress features of the tunnel are applied on the packets, and during encapsulation, only egress features of the tunnel are applied.

Multicast replication can happen in either ingress or egress mode. GRE encapsulation of multicast flows is done on the line card on which the ingress physical interface resides, irrespective of the ingress or egress replication mode. So in the case of both ingress and egress multicast replication modes, egress flows are created on the ingress line card.

The examples in the figures below show how and why multiple flows are created during GRE handling of packets. In the figure below, Flow 1 is created when packets are received by physical interface 3/1. Flows 2 and 3 are created as part the multicast replication process using the internal virtual local area networks (VLANs) that are required for NetFlow accounting to keep track of the multicast traffic.

**Figure 4**  **Multicast IPv4 Traffic over an IPv4 Unicast GRE Tunnel (Encapsulation)**
In the figure below, Flow 1 is created when packets are received over physical interface 5/2. Flow 2 is created as part of the de-encapsulation process. Flow 3 is created as the multicast traffic is replicated and forwarded on interface 1/1.

**Figure 5  Multicast IPv4 Traffic over an IPv4 Unicast GRE Tunnel (De-encapsulation)**

---

### How to Configure NetFlow Accounting for Unicast and Multicast on GRE Tunnel Interfaces

- Sample Network, page 8
- Configuring a GRE IP Tunnel, page 8
- Verifying the Status of the GRE IP Tunnel, page 12
- Configuring NetFlow Accounting on a GRE IP Tunnel Interface, page 13
- Configuring NetFlow Accounting on the Physical Interfaces, page 14
- Verifying NetFlow Accounting, page 16
- Configuring NetFlow Data Export Using the Version 9 Export Format, page 18
- Verifying That NetFlow Data Export Is Operational, page 21
Sample Network

The tasks in this section use the sample network shown in the figure below.

Figure 6  Sample Network with a GRE IPv4 Tunnel

Configuring a GRE IP Tunnel

To configure a GRE IP tunnel as shown in Configuring a GRE IP Tunnel, page 8, perform the task in this section.

Ensure that the physical interface to be used as the tunnel source in this task is up and configured with the appropriate IP address. For hardware technical descriptions and information about installing interfaces, see the hardware installation and configuration documentation for your product.

Note  GRE tunnel keepalive is not supported in cases where virtual route forwarding (VRF) is applied to a GRE tunnel.
SUMMARY STEPS

1. enable
2. configure terminal
3. interface type number
4. bandwidth kbps
5. ip address address mask
6. keepalive [period [retries]]
7. tunnel source {ip-address | interface-type interface-number}
8. tunnel destination {hostname | ip-address}
9. tunnel key key-number
10. tunnel mode gre ip
11. ip mtu bytes
12. ip tcp mss mss-value
13. tunnel path-mtu-discovery [age-timer {aging-mins|infinite}]}
14. end
15. Repeat steps 1-14 on the router that hosts the other end of the GRE tunnel

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 interface type number</td>
<td>Specifies the interface type and number and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# interface tunnel 0</td>
<td>• To configure a tunnel, use tunnel for the type argument.</td>
</tr>
</tbody>
</table>
### Command or Action

**Step 4** bandwidth kbps

Sets the current bandwidth value for an interface and communicates it to higher-level protocols. Specifies the tunnel bandwidth to be used to transmit packets.

**Example:**

```
Router(config-if)# bandwidth 1000
```

- Use the `kbps` argument to set the bandwidth, in kilobits per second (kbps).

**Note** This is a routing parameter only; it does not affect the physical interface. The default bandwidth setting on a tunnel interface is 9.6 kbps. You should set the bandwidth on a tunnel to an appropriate value.

**Step 5** ip address address mask

Specifies an IP address for the interface.

**Example:**

```
Router(config-if)# ip address 192.168.3.1 255.255.255.0
```

**Step 6** keepalive [period [retries]]

(Optional) Specifies the number of times that the device will continue to send keepalive packets without response before bringing the tunnel interface protocol down.

**Example:**

```
Router(config-if)# keepalive 3 7
```

- GRE keepalive packets may be configured either on only one side of the tunnel or on both.
- If GRE keepalive is configured on both sides of the tunnel, the `period` and `retries` arguments can be different at each side of the link.

**Note** This command is supported only on GRE point-to-point tunnels.

**Note** The GRE tunnel keepalive feature should not be configured on a VRF tunnel. This combination of features is not supported.

**Step 7** tunnel source {ip-address | interface-type interface-number}

Configures the tunnel source.

**Example:**

```
Router(config-if)# tunnel source GigabitEthernet6/2
```

- Use the `ip-address` argument to specify the source IP address.
- Use the `interface-type` and `interface-number` arguments to specify the interface to use.

**Note** The tunnel source and destination IP addresses must be defined on two separate devices.

**Step 8** tunnel destination {hostname | ip-address}

Configures the tunnel destination.

**Example:**

```
Router(config-if)# tunnel destination 10.5.9.62
```

- Use the `hostname` argument to specify the name of the host destination.
- Use the `ip-address` argument to specify the IP address of the host destination.

**Note** The tunnel source and destination IP addresses must be defined on two separate devices.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 9</td>
<td>tunnel key key-number</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# tunnel key 1000</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 10</td>
<td>tunnel mode gre ip</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# tunnel mode gre ip</td>
</tr>
<tr>
<td>Step 11</td>
<td>ip mtu bytes</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# ip mtu 1400</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 12</td>
<td>ip tcp mss mss-value</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# ip tcp mss 250</td>
</tr>
<tr>
<td>Step 13</td>
<td>tunnel path-mtu-discovery [age-timer {aging mins</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# tunnel path-mtu-discovery</td>
</tr>
<tr>
<td>Step 14</td>
<td>end</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# end</td>
</tr>
</tbody>
</table>
Verifying the Status of the GRE IP Tunnel

To verify the tunnel configuration and operation, perform the following optional task:

SUMMARY STEPS

1. enable
2. ping ip-address
3. ping ip-address
4. show interfaces tunnel number [accounting]

DETAILED STEPS

Step 1  enable
Enables privileged EXEC mode. Enter your password if prompted.

Example:

Router> enable

Step 2  ping ip-address
To verify that each router has IP connectivity to the tunnel endpoint on the other router, ping the IP address of the remote tunnel endpoint from the local router.

Example:

c65002# ping
192.168.3.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20 ms

Step 3  ping ip-address
To verify that each router has IP connectivity to the tunnel endpoint on the other router, ping the IP address of the remote tunnel endpoint from the local router.

Example:

c65003# ping
192.168.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!

Step 4  show interfaces tunnel number [accounting]
Displays the status and statistics of the tunnel interface
Configuring NetFlow Accounting on a GRE IP Tunnel Interface

To configure NetFlow on a GRE IP tunnel interface, perform the following task:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. ip multicast netflow output-counters
4. interface tunnel number
5. ip flow {ingress | egress}
6. end

**Example:**

c65002# show interface tunnel 0
Tunnel0 is up, line protocol is up
Hardware is Tunnel
Internet address is 192.168.3.1/24
MTU 1514 bytes, BW 1000 Kbit, DLY 50000 usec,
  reliability 255/255, txload 115/255, rxload 57/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 10.4.9.62 (GigabitEthernet6/2), destination 10.5.9.62
Tunnel protocol/transport GRE/IP
  Key disabled, sequencing disabled
Checksumming of packets disabled
Tunnel TTL 255, Fast tunneling enabled
Path MTU Discovery, ager 10 mins, min MTU 92
Last input 00:07:35, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 4139000 bits/sec, 659 packets/sec
5 minute output rate 4117000 bits/sec, 669 packets/sec
L2 Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes
L3 in Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes mcast
L3 out Switched: ucast: 0 pkt, 0 bytes mcast: 0 pkt, 0 bytes
245049 packets input, 192533770 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicasts)
  0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
251500 packets output, 196216398 bytes, 0 underruns
  0 output errors, 0 collisions, 0 interface resets
  0 output buffer failures, 0 output buffers swapped out
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong> ip multicast netflow output-counters</td>
<td>(Optional) Enables NetFlow accounting for the number of bytes and packets of multicast traffic forwarded from an ingress flow.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# ip multicast netflow output-counters</td>
</tr>
<tr>
<td><strong>Step 4</strong> interface tunnel <em>number</em></td>
<td>Specifies the tunnel interface and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# interface tunnel 0</td>
</tr>
<tr>
<td><strong>Step 5</strong> ip flow *(ingress</td>
<td>Configures NetFlow accounting on the interface.</td>
</tr>
<tr>
<td>egress)*</td>
<td>• <em>ingress</em> --Configures NetFlow accounting for traffic that is received by the interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>• <em>egress</em> --Configures NetFlow accounting for traffic that is transmitted by the interface.</td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# ip flow egress</td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Exits interface configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# end</td>
</tr>
</tbody>
</table>

### Configuring NetFlow Accounting on the Physical Interfaces

To configure NetFlow accounting on one or more physical interfaces, perform the following task:
### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ip multicast netflow output-counters`
4. `interface type number`
5. Do one of the following:
   - `ip flow {ingress | egress}`
6. `exit`
7. Repeat Steps 4 through 6 to enable NetFlow on other interfaces.
8. `end`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Example:</strong>&lt;br&gt;<code>Router&gt; enable</code></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Example:</strong>&lt;br&gt;<code>Router# configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>ip multicast netflow output-counters</code></td>
<td>(Optional) Enables NetFlow accounting for the number of bytes and packets of multicast traffic forwarded from an ingress flow.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Example:</strong>&lt;br&gt;<code>Router(config)# ip multicast netflow output-counters</code></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>interface type number</code></td>
<td>Specifies the interface on which you want to enable NetFlow and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Example:</strong>&lt;br&gt;<code>Router(config)# interface gigabitethernet 3/1</code></td>
</tr>
</tbody>
</table>

---

**Configuring NetFlow Accounting on the Physical Interfaces**

**How to Configure NetFlow Accounting for Unicast and Multicast on GRE Tunnel Interfaces**
### Command or Action

**Step 5** Do one of the following:

- `ip flow {ingress | egress}`

**Example:**

```
Router(config-if)# ip flow ingress
```

- `ip flow egress`

**Example:**

```
Router(config-if)# ip flow egress
```

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>Enables NetFlow on the interface.</td>
</tr>
<tr>
<td>Do one of the following:</td>
<td></td>
</tr>
<tr>
<td>`ip flow {ingress</td>
<td>egress}`</td>
</tr>
<tr>
<td><code>ip flow egress</code></td>
<td>Enables NetFlow on the interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config-if)# ip flow ingress</code></td>
<td>Enables NetFlow on the interface.</td>
</tr>
<tr>
<td><code>Router(config-if)# ip flow egress</code></td>
<td>Enables NetFlow on the interface.</td>
</tr>
</tbody>
</table>

**Step 6** `exit`

**Example:**

```
Router(config-if)# exit
```

(Optional) Exits interface configuration mode and returns to global configuration mode.

**Note** You need to use this command only if you want to enable NetFlow on another interface.

**Step 7** Repeat Steps 4 through 6 to enable NetFlow on other interfaces.

(Optional) --

**Step 8** `end`

**Example:**

```
Router(config-if)# end
```

Exits the current configuration mode and returns to privileged EXEC mode.

---

### Verifying NetFlow Accounting

To verify that NetFlow accounting for the tunnel interface is working, perform the following task.

**Note** This task uses the sample network shown in the figure below.

**SUMMARY STEPS**

1. `enable`
2. `show ip cache flow`
3. `show mls net ip module number`
DETAILED STEPS

Step 1  
**enable**
Enables privileged EXEC mode. Enter your password if prompted.

Example:
Router> enable

Step 2  
**show ip cache flow**
The `show ip cache flow` command displays the NetFlow statistics in the cache. The tunnel interface (Tu0) appears in several rows of the statistics, indicating that NetFlow accounting is operational for the tunnel interface.

Example:
c65003# show ip cache flow

Displaying software-switched flow entries on the MSFC in Module 5:
IP packet size distribution (3721891 total packets):
1-32  64  96  128  160  192  224  256  288  320  352  384  416  448  480
  .000 .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  1.00 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 6 added
5394 ager polls, 0 flow alloc failures
Active flows timeout in 30 minutes
Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 33992 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 0 chunks added
  last clearing of statistics 05:58:56
Protocol  Total     Flows   Packets  Bytes  Packets Active(Sec) Idle(Sec)
--------  Flows   Flows  /Sec  /Flow /Pkt  /Sec /Flow /Flow
ICMP      4       0.0     046293 1499  75.4  626.5  12.3
Total: 4  0.0  046293 1499  75.4  626.5  12.3
SrcIf SrcIPaddress  DstIf  DstIPaddress  Pr SrcP  DstP  Pkts
Fa3/1  192.168.22.2  Tu0*  192.168.10.2  01 0000 0000  1052K
Fa3/1  192.168.22.2  Tu0  192.168.10.2  01 0000 0000  1052K

Displaying hardware-switched flow entries in the PFC (Active) Module 5:
SrcIf SrcIPaddress  DstIf  DstIPaddress  Pr SrcP  DstP  Pkts
Tu0  10.4.9.62  G16/2  10.5.9.62  0 0 0 0 0 0 0 0 0 0 0 155K
--- --- --- --- --- --- --- --- --- --- --- --- --- --- ---
Fa3/1 192.168.22.2  Tu0  192.168.10.2  01 0000 0000  1764K
Tu0  192.168.10.2  Fa3/1 192.168.22.2  01 0000 0000 695K
Tu0  192.168.10.2  Fa3/1 192.168.22.2  01 0008 0000  66K
Tu0  192.168.10.2  Fa3/1 192.168.22.2  11 F378 F566  90K
Fa3/1 192.168.22.2  Tu0  192.168.10.2  11 F566 F378  90K

Step 3  
**show mls net ip module** number
The `show mls net ip module` command displays information about the hardware-switched NetFlow flows. The tunnel interface (Tu0) appears in several rows of the statistics, indicating that NetFlow accounting is operational for the tunnel interface.

Example:
c65003# show mls net ip module 5
Displaying NetFlow entries in Active Supervisor EARL in module 5
## Configuring NetFlow Data Export Using the Version 9 Export Format

To configure NetFlow Data Export using the Version 9 data export format, perform the following task:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. mls flow ip {destination | destination-source | full | interface-destination-source | interface-full | source}
4. mls nde sender
5. ip flow-export destination {ip-address | hostname} udp-port
6. Repeat Step 5 once to configure a second NetFlow export destination.
7. ip flow-export source interface-type interface-number
8. ip flow-export version 9 [ origin-as | peer-as ] [ bgp-nexthop ]
9. ip flow-export template refresh-rate packets
10. ip flow-export template timeout-rate minutes
11. ip flow-export template options export-stats
12. ip flow-export template options refresh-rate packets
13. ip flow-export template options timeout-rate minutes
14. end

<table>
<thead>
<tr>
<th>DstIP</th>
<th>SrcIP</th>
<th>Prot:SrcPort:DstPort</th>
<th>Src i/f</th>
<th>:AdjPtr</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.0.0.2</td>
<td>10.4.9.254</td>
<td>udp:646 :646</td>
<td>Gi6/2</td>
<td>:0x0</td>
</tr>
<tr>
<td>46</td>
<td>2852</td>
<td>00:30:28</td>
<td>Multicast</td>
<td>:0x0</td>
</tr>
<tr>
<td>238</td>
<td>17450</td>
<td>00:30:28</td>
<td>L3 - Dynamic</td>
<td>:0x0</td>
</tr>
<tr>
<td>224.0.0.13</td>
<td>172.31.0.2</td>
<td>103:0</td>
<td>Gi6/2</td>
<td>:0x0</td>
</tr>
<tr>
<td>7</td>
<td>172.31.0.2</td>
<td>00:30:21</td>
<td>Multicast</td>
<td>:0x0</td>
</tr>
<tr>
<td>10.4.9.255</td>
<td>172.31.0.2</td>
<td>00:29:38</td>
<td>Multicast</td>
<td>:0x0</td>
</tr>
<tr>
<td>204</td>
<td>16320</td>
<td>00:30:31</td>
<td>Multicast</td>
<td>:0x0</td>
</tr>
<tr>
<td>3</td>
<td>138</td>
<td>00:28:09</td>
<td>L3 - Dynamic</td>
<td>:0x0</td>
</tr>
<tr>
<td>10.4.9.255</td>
<td>10.4.9.2</td>
<td>udp:138 :138</td>
<td>Fa3/1</td>
<td>:0x0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>00:30:28</td>
<td>Multicast</td>
<td>:0x0</td>
</tr>
<tr>
<td>224.0.0.13</td>
<td>192.168.3.2</td>
<td>103:0</td>
<td>Tu0</td>
<td>:0x0</td>
</tr>
<tr>
<td>2</td>
<td>138</td>
<td>00:29:38</td>
<td>Multicast</td>
<td>:0x0</td>
</tr>
<tr>
<td>224.192.16.1</td>
<td>172.31.0.1</td>
<td>icmp:0</td>
<td>Fa3/1</td>
<td>:0x0</td>
</tr>
<tr>
<td>20435</td>
<td>940010</td>
<td>00:30:32</td>
<td>Multicast</td>
<td>:0x0</td>
</tr>
<tr>
<td>224.0.0.1</td>
<td>192.168.3.2</td>
<td>2:0</td>
<td>Tu0</td>
<td>:0x0</td>
</tr>
<tr>
<td>2</td>
<td>138</td>
<td>00:29:49</td>
<td>Multicast</td>
<td>:0x0</td>
</tr>
<tr>
<td>10.4.9.255</td>
<td>10.4.9.2</td>
<td>udp:137 :137</td>
<td>Fa3/1</td>
<td>:0x0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>00:30:10</td>
<td>L3 - Dynamic</td>
<td>:0x0</td>
</tr>
</tbody>
</table>
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enters privileged EXEC mode.  
  • Enter your password if prompted. |
<p>| <strong>Example:</strong> | |
| Router&gt; enable | |
| <strong>Step 2</strong> configure terminal | Enters global configuration mode. |
| <strong>Example:</strong> | |
| Router# configure terminal | |
| <strong>Step 3</strong> mls flow ip {destination | destination-source | full | interface-destination-source | interface-full | source} | Specifies the flow mask for NetFlow data export. |
| <strong>Example:</strong> | |
| Router(conf)# mls flow ip interface-full | |
| <strong>Step 4</strong> mls nde sender | Enables multi-layer switching (MLS) NetFlow data export (NDE). |
| <strong>Example:</strong> | |
| Router(config)# mls nde sender | |
| <strong>Step 5</strong> ip flow-export destination {ip-address | hostname} udp-port | Specifies the IP address or hostname of the NetFlow collector and the UDP port on which the NetFlow collector is listening. |
| <strong>Example:</strong> | |
| Router(config)# ip flow-export destination 172.16.10.2 99 | |
| <strong>Step 6</strong> Repeat Step 5 once to configure a second NetFlow export destination. | (Optional) You can configure a maximum of two export destinations for NetFlow. |
| <strong>Step 7</strong> ip flow-export source interface-type interface-number | (Optional) Specifies the interface from which the source IP address is derived for the UDP datagrams that are sent by NetFlow data export to the destination host. |
| <strong>Example:</strong> | |
| Router(config)# ip flow-export source gigabitethernet 6/2 | |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 8</strong> ip flow-export version 9 [ origin-as</td>
<td>peer-as ] [ bgp-nexthop ]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# ip flow-export version 9</td>
<td></td>
</tr>
<tr>
<td><strong>Caution</strong> Entering this command on a Cisco 12000 Series Internet Router 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.</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 9** ip flow-export template refresh-rate packets | (Optional) Enables the export of information in NetFlow cache entries. |
| **Example:** | |
| Router(config)# ip flow-export template refresh-rate 15 | |
| **Example:** | |
| **Step 10** ip flow-export template timeout-rate minutes | (Optional) Enables the export of information in NetFlow cache entries. |
| **Example:** | |
| Router(config)# ip flow-export template timeout-rate 90 | |
| **Step 11** ip flow-export template options export-stats | (Optional) Enables the export of information in NetFlow cache entries. |
| **Example:** | |
| Router(config)# ip flow-export template options export-stats | |
### Command or Action

<table>
<thead>
<tr>
<th>Step 12</th>
<th>ip flow-export template options refresh-rate packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(config)# ip flow-export template options refresh-rate 25</td>
</tr>
</tbody>
</table>

(Optional) Enables the export of information in NetFlow cache entries.  
- The **template** keyword specifies template-specific configurations.  
- The **options** keyword specifies template options.  
- The **refresh-rate packets** keyword-argument pair specifies the number of packets exported before the templates are resent. Range is 1 to 600 packets. The default is 20 packets.

<table>
<thead>
<tr>
<th>Step 13</th>
<th>ip flow-export template options timeout-rate minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(config)# ip flow-export template options timeout-rate 120</td>
</tr>
</tbody>
</table>

(Optional) Enables the export of information in NetFlow cache entries.  
- The **template** keyword specifies template-specific configurations.  
- The **options** keyword specifies template options.  
- The **timeout-rate minutes** keyword-argument pair specifies the time elapsed before the templates are resent. Range is 1 to 3600 minutes. The default is 30 minutes.

<table>
<thead>
<tr>
<th>Step 14</th>
<th>end</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(config)# end</td>
</tr>
</tbody>
</table>

Exits the current configuration mode and returns to privileged EXEC mode.

---

**Verifying That NetFlow Data Export Is Operational**

To verify that NetFlow data export is operational, perform the following optional task.

**SUMMARY STEPS**

1. `show ip flow export`
2. `show ip flow export template`

**DETAILED STEPS**

### Step 1

**show ip flow export**

Use this command to display the statistics for the NetFlow data export, including statistics for the main cache and for all other enabled caches. The following is sample output from this command:

**Example:**

```
Router# show ip flow export
Flow export v9 is enabled for main cache
Export source and destination details :
VRF ID : Default
  Source(1)     10.4.9.62 (GigabitEthernet6/2)
  Source(2)     10.4.9.62 (GigabitEthernet6/2)
  Destination(1) 172.16.10.2 (99)
  Destination(2) 172.16.10.3 (99)
Version 9 flow records
```
11 flows exported in 11 udp datagrams
0 flows failed due to lack of export packet
0 export packets were sent up to process level
0 export packets were dropped due to no fib
0 export packets were dropped due to adjacency issues
0 export packets were dropped due to fragmentation failures
0 export packets were dropped due to encapsulation fixup failures
0 export packets were dropped enqueuing for the RP
0 export packets were dropped due to IPC rate limiting
0 export packets were dropped due to Card not being able to export

Step 2
**show ip flow export template**

Use this command to display the statistics for the NetFlow data export (such as the template timeout rate and the refresh rate) for the template-specific configurations. The following is sample output from this command:

```
Example:

Router# show ip flow export template
Template Options Flag = 1
  Total number of Templates added = 1
  Total active Templates = 1
  Flow Templates active = 0
  Flow Templates added = 0
  Option Templates active = 1
  Option Templates added = 1
  Template ager polls = 0
  Option Template ager polls = 388
Main cache version 9 export is enabled
Template export information
  Template timeout = 90
  Template refresh rate = 15
Option export information
  Option timeout = 120
  Option refresh rate = 25
```

### Configuration Examples for NetFlow Accounting for Unicast and Multicast on GRE Tunnel Interfaces

- Configuring a GRE IP Tunnel Example, page 22
- Configuring NetFlow Accounting on a GRE IP Tunnel Example, page 23

### Configuring a GRE IP Tunnel Example

The following example shows how to configure a GRE IP tunnel:

```
interface Tunnel0
  tunnel mode gre ip
  bandwidth 1000
  ip address 192.168.3.1 255.255.255.0
  tunnel source GigabitEthernet6/2
  tunnel destination 10.5.9.62
  tunnel path-mtu-discovery
```
The following display output shows that the GRE IP tunnel is operational because the tunnel is transmitting and receiving traffic:

c65002# show interface tunnel 0
Tunnel0 is up, line protocol is up
Hardware is Tunnel
Internet address is 192.168.3.1/24
MTU 1514 bytes, BW 1000 Kbit, DLY 50000 usec,
reliability 255/255, txload 90/255, rxload 98/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 10.4.9.62 (GigabitEthernet6/2), destination 10.5.9.62
Tunnel protocol/transport GRE/IP
Key disabled, sequencing disabled
Checksumming of packets disabled
Tunnel TTL 255, Fast tunneling enabled
Path MTU Discovery, ager 10 mins, min MTU 92
Last input 00:11:44, output 00:11:44, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Input queue: 0/75/0/0 (size/max/drops/flushes); Total input drops: 1
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 380000 bits/sec, 125 packets/sec
5 minute output rate 347000 bits/sec, 125 packets/sec
L2 Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes
L3 in Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes mcast
L3 out Switched: ucast: 0 pkt, 0 bytes mcast: 0 pkt, 0 bytes
334121 packets input, 2452613051 bytes, 0 no buffer
Received 0 broadcasts (0 IP multiscasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
3399211 packets output, 2431569783 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out

Configuring NetFlow Accounting on a GRE IP Tunnel Example

The following display output shows that NetFlow accounting is operational because the flow cache has NetFlow statistics data in it:

c65002# show ip cache flow
Displaying software-switched flow entries on the MSFC in Module 5:
IP packet size distribution (3721891 total packets):
  1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
  .000 .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 .000 .000 .000 .000
IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 6 added
5394 ager polls, 0 flow alloc failures
Active flows timeout in 30 minutes
Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 33992 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
0 alloc failures, 0 force free
1 chunk, 0 chunks added
last clearing of statistics 05:58:56

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Total Flows</th>
<th>Packets /Sec</th>
<th>Bytes /Pkt</th>
<th>Packets Active(Sec)</th>
<th>Idle(Sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP</td>
<td>4</td>
<td>0.0</td>
<td>406293</td>
<td>75.4</td>
<td>626.5</td>
</tr>
<tr>
<td>Total:</td>
<td>4</td>
<td>0.0</td>
<td>406293</td>
<td>75.4</td>
<td>626.5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SrcIf</th>
<th>SrcIPaddress</th>
<th>DstIf</th>
<th>DstIPaddress</th>
<th>Pr</th>
<th>SrcP</th>
<th>DstP</th>
<th>Pkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa3/1</td>
<td>192.168.22.2</td>
<td>Tu0*</td>
<td>192.168.10.2</td>
<td>01</td>
<td>0000</td>
<td>0000</td>
<td>1052K</td>
</tr>
<tr>
<td>Fa3/1</td>
<td>192.168.22.2</td>
<td>Tu0</td>
<td>192.168.10.2</td>
<td>01</td>
<td>0000</td>
<td>0000</td>
<td>1052K</td>
</tr>
</tbody>
</table>

Displaying hardware-switched flow entries in the PFC (Active) Module 5:

<table>
<thead>
<tr>
<th>SrcIf</th>
<th>SrcIPaddress</th>
<th>DstIf</th>
<th>DstIPaddress</th>
<th>Pr</th>
<th>SrcP</th>
<th>DstP</th>
<th>Pkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tu0</td>
<td>10.4.9.62</td>
<td>Gi6/2</td>
<td>10.5.9.62</td>
<td>2F</td>
<td>0000</td>
<td>0000</td>
<td>155K</td>
</tr>
<tr>
<td>--</td>
<td>0.0.0.0</td>
<td>---</td>
<td>0.0.0.0</td>
<td>00</td>
<td>0000</td>
<td>0000</td>
<td>1764K</td>
</tr>
<tr>
<td>Fa3/1</td>
<td>192.168.22.2</td>
<td>Tu0</td>
<td>192.168.10.2</td>
<td>01</td>
<td>0000</td>
<td>0000</td>
<td>65K</td>
</tr>
</tbody>
</table>

The following display output shows that NetFlow accounting is operational because there are statistics for the hardware-switched NetFlow flows.

c65003# show mls net ip mod 5

Displaying NetFlow entries in Active Supervisor EARL in module 5

<table>
<thead>
<tr>
<th>DstIP</th>
<th>SrcIP</th>
<th>Prot:SrcPort:DstPort</th>
<th>Src i/f</th>
<th>:AdjPtr</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.0.0.2</td>
<td>10.4.9.254</td>
<td>udp :646</td>
<td>Gi6/2</td>
<td>:0x0</td>
</tr>
<tr>
<td>238</td>
<td>17450</td>
<td>00:30:28</td>
<td>Multicast</td>
<td>:0x0</td>
</tr>
<tr>
<td>224.0.0.13</td>
<td>172.31.0.2</td>
<td>:0</td>
<td>Gi6/2</td>
<td>:0x0</td>
</tr>
<tr>
<td>224.0.0.5</td>
<td>192.168.255.254</td>
<td>89</td>
<td>Fa3/1</td>
<td>:0x0</td>
</tr>
<tr>
<td>204</td>
<td>16320</td>
<td>00:30:31</td>
<td>Multicast</td>
<td>:0x0</td>
</tr>
<tr>
<td>224.0.0.1</td>
<td>172.31.0.2</td>
<td>2</td>
<td>Gi6/2</td>
<td>:0x0</td>
</tr>
<tr>
<td>10.4.9.255</td>
<td>10.4.9.2</td>
<td>udp :138</td>
<td>Fa3/1</td>
<td>:0x0</td>
</tr>
<tr>
<td>224.0.0.13</td>
<td>192.168.3.2</td>
<td>103</td>
<td>Tu0</td>
<td>:0x0</td>
</tr>
<tr>
<td>224.192.16.1</td>
<td>172.31.0.1</td>
<td>:0</td>
<td>Fa3/1</td>
<td>:0x0</td>
</tr>
<tr>
<td>20435</td>
<td>940010</td>
<td>00:30:32</td>
<td>Multicast</td>
<td>:0x0</td>
</tr>
<tr>
<td>224.0.0.1</td>
<td>192.168.3.2</td>
<td>2</td>
<td>00:29:49</td>
<td>Multicast</td>
</tr>
</tbody>
</table>

Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Cisco IOS 12.2SX on Cisco Catalyst 6500 series switches</td>
<td>Catalyst 6500 Release 12.2SXH and Later Software Configuration Guide</td>
</tr>
</tbody>
</table>
Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>There are no standards associated with this feature. --</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>There are no MIBs associated with this feature. --</td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 2784</td>
<td>Generic Routing Encapsulation (GRE)</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
</tr>
</tbody>
</table>

Feature Information for Configuring NetFlow Accounting for Unicast and Multicast on GRE IP Tunnel Interfaces

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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.
Table 3  Feature Information for Flexible NetFlow

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Configuration Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring NetFlow Accounting for Unicast and Multicast on GRE Tunnel Interfaces</td>
<td>12.2(33)SXI</td>
<td>The Configuring NetFlow Accounting for Unicast and Multicast on GRE Tunnel Interfaces feature allows NetFlow statistics to be gathered on traffic that is transmitted over a GRE IP tunnel interface. The following section provides information for configuring this feature: No commands were introduced or modified for this feature.</td>
</tr>
</tbody>
</table>

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2011 Cisco Systems, Inc. All rights reserved.