Router IP Traffic Export Packet Capture Enhancements

First Published: November 17, 2006
Last Updated: November 17, 2006

IP Traffic Export allows you to configure your router to export IP packets received on multiple, simultaneous WAN or LAN interfaces. The unaltered IP packets are exported on a single LAN or VLAN interface, thereby, easing deployment of protocol analyzers and monitoring devices.

The Router IP Traffic Export Packet Capture Enhancements feature allows you to configure your router to capture IP packets in a buffer within the router, and then to dump these packets into a specified memory device.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for IP Traffic Export" section on page 25.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Contents

Corporate Headquarters
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Restrictions for IP Traffic Export

Platform Restrictions

IP traffic export is intended only for software switching platforms; distributed architectures are not supported.

IP traffic capture is supported only on the Cisco 1841, Cisco 2800 series, and Cisco 3800 series integrated services routers.

IP Packet Forwarding Performance Impact

When IP traffic export is enabled, a delay is incurred on the outbound interface when packets are captured and transmitted across the interface. Performance delays increase with the increased number of interfaces that are monitored and the increased number of destination hosts.

Exported Traffic Limitation

- The MAC address of the device that is receiving the exported traffic must be on the same VLAN or directly connected to one of the router interfaces. (Use the **show arp** command to determine the MAC address of device that is directly connected to an interface.)
- The outgoing interface for exported traffic must be Ethernet (10/100/1000). (Incoming (monitored) traffic can traverse any interface.)

Information About IP Traffic Export

To use the IP traffic export, you should understand the following concept:

- Benefits of IP Traffic Export, page 2

Benefits of IP Traffic Export

Simplified Cisco IDS Deployment

Without the ability to export IP traffic, the Cisco Intrusion Detection System (Cisco IDS) probe must be inline with the network device to monitor traffic flow. IP traffic export eliminates the probe placement limitation, allowing users to place a Cisco IDS probe in any location within their network or direct all exported traffic to a VLAN that is dedicated for network monitoring. Allowing users to choose the optimal location of their Cisco IDS probe reduces processing burdens.

Also, because packet processing that was performed on the network device can now be performed away from the network device, the need to enable Cisco IDS with the Cisco IOS software is eliminated.

IP Traffic Export Functionality Benefits

Users can configure their router to perform the following tasks:

- Filter copied packets using an access control list (ACL)
- Filter copied packets via sampling, which allows you to export one in every few packets in which you are interested. Use this option when you do not need to export all incoming traffic. Also, sampling is useful when a monitored ingress interface can send traffic faster than the egress interface can transmit it.
- Configure bidirectional traffic on an interface. (By default, only incoming traffic is exported or captured.)

How to Use IP Traffic Export

This section contains the following procedures:

- Configuring IP Traffic Export, page 3 (required)
- Configuring IP Traffic Capture, page 5 (required)
- Displaying IP Traffic Export Configuration Data, page 9 (required)

Configuring IP Traffic Export

Use this task to configure IP traffic export profiles, which enable IP traffic to be exported on an ingress interface and allow you to specify profile attributes, such as the outgoing interface for exporting traffic.

Note Perform packet exporting before packet switching or filtering.

IP Traffic Export Profiles Overview

All packet export configurations are specified using IP traffic export profiles, which consist of IP-traffic-export-related command-line interfaces (CLIs) that control various attributes for both incoming and outgoing exported IP traffic. You can configure a router with multiple IP traffic export profiles. (Each profile must have a different name.) You can apply different profiles on different interfaces.

The two different IP traffic export profiles are as follows:

- The global configuration profile, which is configured by the **ip traffic-export profile** command.
- The IP traffic export submode configuration profile, which is configured by any of the following router IP Traffic Export (RITE) commands—**bidirectional**, **incoming**, **interface**, **mac-address**, and **outgoing**.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip traffic-export profile** *profile-name*
4. **interface** *interface-name*
5. **bidirectional**
6. **mac-address** *H.H.H*
7. **incoming** {**access-list** {*standard* | *extended* | *named*} | **sample one-in-every** *packet-number*}
8. **outgoing** {**access-list** {*standard* | *extended* | *named*} | **sample one-in-every** *packet-number*}
9. **exit**
10. **interface** *type number*
11. **ip traffic-export apply** *profile-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip traffic-export profile** *profile-name* **Example:** `Router(config)# ip traffic-export profile my_rite`	Creates or edits an IP traffic export profile, enables the profile on an ingress interface, and enters RITE configuration mode.
Step 4	**interface** *interface-name* **Example:** `Router(config-rite)# interface FastEthernet 0/1`	Specifies the outgoing (monitored) interface for exported traffic. **Note** If you do not enter this command, the profile will not recognize an interface in which to send the captured IP traffic.
Step 5	**bidirectional** **Example:** `Router(config-rite)# bidirectional`	(Optional) Exports incoming and outgoing IP traffic on the monitored interface. **Note** If you do not enable this command, only incoming traffic is exported.
Step 6	**mac-address** *H.H.H* **Example:** `Router(config-rite)# mac-address 00a.8aab.90a0`	Specifies the 48-bit address of the destination host that is receiving the exported traffic. **Note** If you do not enter this command, the profile will not recognize a destination host in which to send the exported packets.
Step 7	**incoming** {**access-list** {*standard* | *extended* | *named*} | **sample one-in-every** *packet-number*} **Example:** `Router(config-rite)# incoming access-list my_acl`	(Optional) Configures filtering for incoming traffic. After you create a profile using the **ip traffic-export profile,** this functionality is enabled by default.
Step 8	**outgoing** {**access-list** {*standard* | *extended* | *named*} | **sample one-in-every** *packet-number*} **Example:** `Router(config-rite)# outgoing sample one-in-every 50`	(Optional) Configures filtering for outgoing export traffic. **Note** If you enter this command, you must also enter the **bidirectional** command, which enables outgoing traffic to be exported. However, only routed traffic (such as passthrough traffic) is exported; that is, traffic that originates from the network device is not exported.
Step 9	**exit**	Exits RITE configuration mode.

	Command or Action	Purpose
Step 10	**interface** *type number* **Example:** `Router(config)# interface FastEthernet0/0`	Configures an interface type and enters interface configuration mode.
Step 11	**ip traffic-export apply** *profile-name* **Example:** `Router(config-if)# ip traffic-export apply my_rite`	Enables IP traffic export on an ingress interface.

Troubleshooting Tips

Creating an IP Traffic Export Profile

The **interface** and **mac-address** commands are required to successfully create a profile. If these commands are not entered, you will receive the following profile incomplete message when you enter the **show running config** command:

```
ip traffic-export profile newone
! No outgoing interface configured
! No destination mac-address configured
```

Applying an IP Traffic Export Profile to an interface

The following system logging messages should appear immediately after you activate and deactivate a profile from an interface (via the **ip traffic-export apply profile** command):

- Activated profile:

  ```
  %RITE-5-ACTIVATE: Activated IP traffic export on interface FastEthernet 0/0.
  ```

- Deactivated profile:

  ```
  %RITE-5-DEACTIVATE: Deactivated IP traffic export on interface FastEthernet 0/0.
  ```

If you attempt to apply an incomplete profile to an interface, you will receive the following message:

```
Router(config-if)# ip traffic-export apply newone
RITE: profile newone has missing outgoing interface
```

What to Do Next

After you configure a profile and enable the profile on an ingress interface, you can monitor IP traffic exporting events and verify your profile configurations. To complete these steps, see the "Displaying IP Traffic Export Configuration Data" section on page 9.

Configuring IP Traffic Capture

IP traffic export provides the capability to export IPO traffic over an Ethernet port. IP traffic capture provides the capability to capture IP packets in local router memory, and then dump this data to a file on an external device, such as flash memory.

IP traffic capture is supported on the Cisco 1841, Cisco 2800 series, and Cisco 3800 series integrated services routers.

The following sections describe the configuration and control of IP traffic capture:

- Configuring IP Traffic Capture, page 6 (required)
- Performing IP Traffic Capture, page 7 (required)

Configuring IP Traffic Capture

Perform the following steps to configure IP traffic capture.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip traffic-export profile** *profile-name* **mode capture**
4. **bidirectional**
5. **incoming** {**access-list** {*standard* | *extended* | *named*} | **sample one-in-every** *packet-number*}
6. **outgoing** {**access-list** {*standard* | *extended* | *named*} | **sample one-in-every** *packet-number*}
7. **length** *bytes*
8. **exit**
9. **interface** *type number*
10. **ip traffic-export apply** *profile-name* **size** *size*

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`ip traffic-export profile` *profile-name* `mode capture`
	
	Example:
	`Router(config)# ip traffic-export profile my_rite`
		Creates or edits an IP traffic export profile for capture and enters RITE configuration mode.

Step 4	`bidirectional`
	
	Example:
	`Router(config-rite)# bidirectional`
		(Optional) Captures incoming and outgoing IP traffic on the monitored interface.
		Note If you do not enable this command, only incoming traffic is captured.

	Command or Action	Purpose
Step 5	**incoming** {**access-list** {*standard* | *extended* | *named*} | **sample one-in-every** *packet-number*} **Example:** `Router(config-rite)# incoming access-list my_acl`	(Optional) Configures filtering for incoming traffic. After you have created a capture profile using **ip traffic-export profile** *name* **mode capture,** this functionality is enabled by default.
Step 6	**outgoing** {**access-list** {*standard* | *extended* | *named*} | **sample one-in-every** *packet-number*} **Example:** `Router(config-rite)# outgoing sample one-in-every 50`	(Optional) Configures filtering for outgoing captured traffic. **Note** If you enter this command, you must also enter the **bidirectional** command, which enables outgoing traffic to be captured. However, only routed traffic (such as passthrough traffic) is captured; that is, traffic that originates from the network device is not captured.
Step 7	**length** *bytes* **Example:** `Router(config-rite)# length 512`	Specifies the length of the packet in capture mode. The options are 128, 256, and 512 bytes.
Step 8	**exit** **Example:** `Router(config-rite)# exit`	Exits RITE configuration mode.
Step 9	**interface** *type number* **Example:** `Router(config)# interface FastEthernet0/0`	Configures an interface type and enters interface configuration mode.
Step 10	**ip traffic-export apply** *profile-name* **size** *size* **Example:** `Router(config-if)# ip traffic-export apply my_rite size 10000000`	Applies IP traffic capture on an ingress interface, and specifies the size of the capture buffer.

Performing IP Traffic Capture

When traffic capture is configured, perform it using with CLI commands. There are commands to clear the capture buffer, to start and stop packet capture, and to copy the capture buffer to an external memory device. These commands are:

- **traffic-export interface** *type number* **clear**
- **traffic-export interface** *type number* **start**
- **traffic-export interface** *type number* **stop**
- **traffic-export interface** *type number* **copy**

Use these commands in privileged EXEC mode at your discretion to perform the following operations:

- Clear the IP Traffic Capture Buffer, page 8
- Start IP Traffic Capture, page 8

- Stop IP Traffic Capture, page 8
- Copy IP Traffic Capture, page 9

Clear the IP Traffic Capture Buffer

To clear the packet capture buffer for the designated interface, use the **traffic-export interface clear** command.

Command or Action	Purpose
traffic-export interface *type number* **clear**	Clears the packet capture buffer.
	Note The following system logging message should appear immediately after you enter the command:
Example: `Router# traffic-export interface fastethernet0/0 clear`	`%RITE-5-CAPTURE_CLEAR: Cleared IP traffic capture buffer for interface FastEthernet0/0`

Start IP Traffic Capture

To initiate packet capture, use the **traffic-export interface start** command. This action will copy those packets designated in the traffic capture configuration into the internal capture buffer for the interface.

Command or Action	Purpose
traffic-export interface *type number* **start**	Starts packet capture on the designated interface.
	Note The following system logging message should appear immediately after you enter the command:
Example: `Router# traffic-export interface fastethernet0/0 start`	`%RITE-5-CAPTURE_START: Started IP traffic capture for interface FastEthernet0/0`

Stop IP Traffic Capture

To halt packet capture, use the **traffic-export interface stop** command.

Command or Action	Purpose
traffic-export interface *type number* **stop**	Stops packet capture on the designated interface.
	Note The following system logging message should appear immediately after you enter the command:
Example: `Router# traffic-export interface fastethernet0/0 stop`	`%RITE-5-CAPTURE_STOP: Stopped IP traffic capture for interface FastEthernet0/0`

Copy IP Traffic Capture

To copy the packet capture buffer to an external memory device, use the **traffic-export interface copy** command.

Command or Action	Purpose
traffic-export interface *type number* **copy** *memory-device* **Example:** `Router# traffic-export interface fastethernet0/0 copy tftp:`	Copies the contents of the packet capture buffer to the selected memory device. Memory device options are: • *flash:* • *tftp:* • *usbflash0:*

After you enter this command, an interactive dialog occurs.

Enter the name or address of the remote host containing the external memory device.

```
Address or name of remote host []? [name | address]
```

Enter the name of the capture buffer file in the remote host.

```
Capture buffer filename []? filename
```

An example of this dialog is:

```
Router# traffic-export interface fastethernet0/0 copy tftp:
Address or name of remote host []? 172.18.207.15
Capture buffer filename []? atmcapture
Copying capture buffer to tftp://172.18.207.15/atmcapture !!
```

Displaying IP Traffic Export Configuration Data

This task allows you to verify IP traffic export parameters such as the monitored ingress interface, which is where the IP traffic is exported, and outgoing and incoming IP packet information, such as configured ACLs. You can also use this task to monitor packets that are captured and then transmitted across an interface to a destination host. Use this optional task to help you troubleshoot any problems with your exported IP traffic configurations.

SUMMARY STEPS

1. **enable**
2. **debug ip traffic-export events**
3. **show ip traffic-export** [**interface** *interface-name* | **profile** *profile-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug ip traffic-export events** **Example:** `Router# debug ip traffic-export events`	Enables debugging messages for exported IP traffic packets events.
Step 3	**show ip traffic-export** [**interface** *interface-name* | **profile** *profile-name*] **Example:** `Router# show ip traffic-export`	Displays information related to exported IP traffic events. • **interface** *interface-name*—Only data associated with the monitored ingress interface is shown. • **profile** *profile-name*—Only flow statistics, such as exported packets and the number of bytes, are shown.

Examples

The following sample output from the **show ip traffic-export** command is for the profile "one." This example is for a single, configured interface. If multiple interfaces are configured, the information below is displayed for each interface.

```
Router# show ip traffic-export

Router IP Traffic Export Parameters
Monitored Interface             FastEthernet0/0
        Export Interface                FastEthernet0/1
        Destination MAC address 0030.7131.abfc
        bi-directional traffic export is off
Input IP Traffic Export Information     Packets/Bytes Exported    0/0
        Packets Dropped           0
        Sampling Rate             one-in-every 1 packets
        No Access List configured
        Profile one is Active
```

Configuration Examples for IP Traffic Export

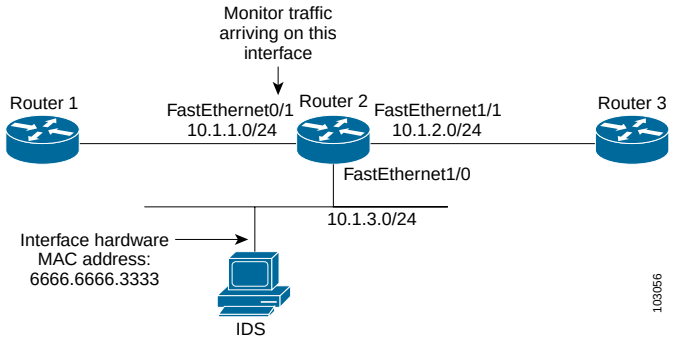
This section includes the following configuration examples:

- Exporting IP Traffic Configuration: Example, page 11
- Capturing IP Traffic Configuration: Example, page 12

Exporting IP Traffic Configuration: Example

Figure 1 and the following sample output from the **show running-config** command illustrate how to configure Router 2 to export the incoming traffic from Router 1 to Cisco IDS:

Figure 1 Traffic Export Example




```
Router2# show running-config

Building configuration...

Current configuration :2349 bytes

! Last configuration change at 20:35:39 UTC Wed Oct 8 2003
! NVRAM config last updated at 20:35:39 UTC Wed Oct 8 2003
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service udp-small-servers
!
hostname rite-3745
!
boot system flash:c3745-js-mz.123-1.8.PI2d
no logging console
enable password lab
!
no aaa new-model
ip subnet-zero
!
no ip domain lookup
!
ip cef
!
ip traffic-export profile my_rite
  interface FastEthernet1/0
  mac-address 6666.6666.3333
!
interface FastEthernet0/0
 ip address 10.0.0.94 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.1.1.2 255.255.255.0
```

```
 duplex auto
 speed auto
 ip traffic-export apply my_rite
!
interface FastEthernet1/0
 ip address 10.1.3.2 255.255.255.0
 no ip redirects
 no cdp enable
!
interface FastEthernet1/1
 ip address 10.1.2.2 255.255.255.0
 duplex auto
 speed auto
!
router ospf 100
 log-adjacency-changes
 network 10.1.0.0 0.0.255.255 area 0
!
ip http server
ip classless
!
snmp-server engineID local 0000000902000004C1C59140
snmp-server community public RO
snmp-server enable traps tty
!
control-plane
!
dial-peer cor custom
!
gateway
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
line vty 0 4
 password lab
 login
!
ntp clock-period 17175608
ntp server 10.0.0.2
!
end
```

Capturing IP Traffic Configuration: Example

The following sample output from the **show running-config** command also refers to Figure 1. It illustrates how to configure Router 2 to locally capture the incoming traffic from Router 1, rather than export it.

```
Router2# show running-config

Building configuration...

Current configuration :2349 bytes

! Last configuration change at 20:35:39 UTC Wed Oct 8 2003
! NVRAM config last updated at 20:35:39 UTC Wed Oct 8 2003
!
version 12.3
```

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service udp-small-servers
!
hostname rite-3745
!
boot system flash:c3745-js-mz.123-1.8.PI2d
no logging console
enable password lab
!
no aaa new-model
ip subnet-zero
!
no ip domain lookup
!
ip cef
!
ip traffic-export profile my_rite mode capture
 length 512
!
interface FastEthernet0/0
 ip address 10.0.0.94 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.1.1.2 255.255.255.0
 duplex auto
 speed auto
 ip traffic-export apply my_rite size 10000000
!
interface FastEthernet1/0
 ip address 10.1.3.2 255.255.255.0
 no ip redirects
 no cdp enable
!
interface FastEthernet1/1
 ip address 10.1.2.2 255.255.255.0
 duplex auto
 speed auto
!
router ospf 100
 log-adjacency-changes
 network 10.1.0.0 0.0.255.255 area 0
!
ip http server
ip classless
!
snmp-server engineID local 0000000902000004C1C59140
snmp-server community public RO
snmp-server enable traps tty
!
control-plane
!
dial-peer cor custom
!
gateway
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
```

```
line vty 0 4
 password lab
 login
!
ntp clock-period 17175608
ntp server 10.0.0.2
!
end
```

Additional References

The following sections provide references related to IP Traffic Export.

Related Documents

Related Topic	Document Title
Configuring Cisco IDS	The chapter "Configuring Cisco IOS Firewall Intrusion Detection System" in the section "Traffic Filtering and Firewalls" of the *Cisco IOS Security Configuration Guide*.
Configuring IP	The chapter "Configuring IP Services" in the section "IP Addressing and Services" of the *Cisco IOS IP Configuration Guide*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents new and modified commands only.

- **ip traffic-export apply**
- **ip traffic-export profile**
- **length (RITE)**
- **traffic-export**

ip traffic-export apply

To apply an IP traffic export profile or an IP traffic capture profile to a specific interface, use the **ip traffic-export apply profile** command in interface configuration mode. To remove an IP traffic export profile or an IP traffic capture profile from an interface, use the **no** form of this command.

ip traffic-export apply *profile-name*

no ip traffic-export apply *profile-name*

Cisco 1841, Cisco 2800 Series, and Cisco 3800 Series

ip traffic-export apply *profile-name* **size** *size*

no ip traffic-export apply *profile-name*

Syntax Description

profile-name	Name of the profile that is to be applied to a specified interface. The *profile-name* argument must match a name that was specified in the **ip traffic-export profile** command.
size	Optional. Used in IP traffic capture mode to set up a local capture buffer.
size	Optional. Specifies the size of the local capture buffer, in bytes.

Defaults

If you do not use this command, a sucessfully configured profile is not active.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.4(11)T	This command was updated to incorporate the **size** keyword and *size* argument for IP traffic capture mode on the Cisco 1841, Cisco 2800 series, and Cisco 3800 series routers.

Usage Guidelines

After you configure at least one export profile, use the **ip traffic-export apply profile** command to activate IP traffic export on the specified ingress interface.

After you configure a capture profile, use the **ip traffic-export apply profile** command to activate IP traffic capture on the specified ingress interface, and to specify the size of the local capture buffer.

Examples

The following example shows how to apply the export profile “corp1” to interface Fast Ethernet 0/0.

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list spam_acl
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp1
```

The following example shows how to apply the capture profile “corp2” to interface Fast Ethernet 0/0, and specify a capture buffer of 10,000,000 bytes.

```
Router(config)# ip traffic-export profile corp2 mode_capture
Router(config-rite)# bidirectional
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# length 512
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp2 size 10000000
```

After a profile is activated on the interface, a logging message such as the following will appear:

```
%RITE-5-ACTIVATE: Activated IP traffic export on interface FastEthernet 0/0.
```

After a profile is removed from the interface, a logging message such as the following will appear:

```
%RITE-5-DEACTIVATE: Deactivated IP traffic export on interface FastEthernet 0/0.
```

If you attempt to apply an incomplete profile to an interface, you will receive the following message:

```
Router(config-if)# ip traffic-export apply newone
RITE: profile newone has missing outgoing interface
```

Related Commands

Command	Description
ip traffic-export profile	Creates or edits an IP traffic export profile and enables the profile on an ingress interface.
traffic-export	Controls the operation of IP traffic capture mode.

ip traffic-export profile

To create or edit an IP traffic export profile or an IP traffic capture profile and enable the profile on an ingress interface, use the **ip traffic-export profile** command in global configuration mode. To remove an IP traffic export profile from your router configuration, use the **no** form of this command.

ip traffic-export profile *profile-name*

no ip traffic-export profile *profile-name*

Cisco 1841, Cisco 2800 Series, and Cisco 3800 Series Routers

ip traffic-export profile *profile-name* **mode_capture**

no ip traffic-export profile *profile-name*

Syntax Description

profile-name	IP traffic export profile name.
mode_capture	Optional. Creates an IP traffic capture profile.

Defaults

A profile does not exist.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.4(11)T	This command was updated to incorporate the optional **mode_capture** keyword on the Cisco 1841, Cisco 2800 series, and Cisco 3800 series routers.

Usage Guidelines

The **ip traffic-export profile** command allows you to begin a profile that can be configured to capture or export IP packets as they arrive on or leave from a selected router ingress interface.

When exporting IP packets, a designated egress interface exports IP packets out of the router. So, the router can export unaltered IP packets to a directly connected device.

When capturing IP packets, the packets are stored in local router memory. They may then be dumped to an external device.

IP Traffic Export Profiles

All exported IP traffic configurations are specified by profiles, which consist of RITE-related command-line interface (CLI) commands that control various attributes of both incoming and outgoing IP traffic. You can configure a router with multiple profiles. (Each profile must have a different name.) You can apply different profiles on different interfaces.

The two profiles to configure are:

- Global configuration profile, which you configure using the **ip traffic-export profile** command.
- Submode configuration profile, which you configure using any of the following RITE commands—**bidirectional**, **incoming**, **interface**, **mac-address**, and **outgoing**.

Use **interface** and **mac-address** commands to successfully create a profile. If you do not issue these commands, the user will receive a profile incomplete messages such as the following:

```
ip traffic-export profile newone
! No outgoing interface configured
! No destination mac-address configured
```

After you configure your profiles, you can apply the profiles to an interface with the **ip traffic-export apply profile** command, which will activate it.

IP Traffic Capture Profiles

On the Cisco 1841, Cisco 2800 series, and Cisco 3800 series routers, you can also configure IP traffic capture. A captured IP traffic configuration is specified by a profile, which consists of RITE-related command-line interface (CLI) commands that control various attributes of both incoming and outgoing IP traffic.

The two profiles that you should configure are:

- Global configuration profile, which you configure using the **ip traffic-export profile mode_capture** command.
- Submode configuration profile, which you configure using any of the following RITE commands—**bidirectional**, **incoming**, **length**, and **outgoing**.

After you configure your profiles, you can apply the profiles to an interface with the **ip traffic-export apply profile** command, which will activate it.

When the IP traffic capture profile is applied to an interface, use the **traffic-export** command to control the capture of the traffic.

Examples

The following example shows how to configure the profile “corp1,” which sends captured IP traffic to host “00a.8aab.90a0” at the interface “FastEthernet 0/1.” This profile is also configured to export 1 in every 50 packets and to allow incoming traffic only from the access control list (ACL) “ham_ACL.”

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp1
```

The following example shows how to configure the profile “corp2,” which captures IP traffic and stores it in a local router memory buffer of 10,000,000 bytes. This profile also captures 1 in every 50 packets and allows incoming traffic only from the access control list (ACL) “ham_ACL.”

```
Router(config)# ip traffic-export profile corp2 mode_capture
Router(config-rite)# bidirectional
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# length 512
Router(config-rite)# exit
```

```
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp2 size 10000000
```

Related Commands

Command	Description
bidirectional	Enables incoming and outgoing IP traffic to be exported or captured across a monitored interface.
incoming	Configures filtering for incoming export or capture traffic.
interface (RITE)	Specifies the outgoing interface for exporting traffic
ip traffic-export apply profile	Applies an IP traffic export or IP traffic capture profile to a specific interface.
length	Specifies the length of the packet in capture mode.
mac-address	Specifies the Ethernet address of the destination host in traffic export.
outgoing	Configures filtering for outgoing export or capture traffic.
traffic-export interface	Controls the operation of IP traffic capture mode.

length (RITE)

To specify the length the captured portion of the packets being captured in IP traffic export capture mode, use the **length** command in RITE configuration mode. To return to the default condition of capturing entire packets, use the **no** form of this command.

length *bytes*

no length

Syntax Description

bytes	The length in bytes of the packet captured in IP traffic export capture mode. Acceptable values are 128, 256, and 512.

Command Default

When you do not use this command, the entire packet is captured.

Command Modes

RITE configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use this command to limit the length of the portion of the packets being captured in IP traffic export capture mode. The captured portion of the packets are limited to 128, 256, or 512 bytes. If you do not use the **length** command, entire packets are captured.

Examples

The following example shows the use of the **length** command in the configuration of IP traffic export capture mode profile “corp2”:

```
Router(config)# ip traffic-export profile corp2 mode_capture
Router(config-rite)# bidirectional
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# length 512
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp2 size 10000000
```

Related Commands

Command	Description
bidirectional	Enables incoming and outgoing IP traffic to be exported or captured across a monitored interface.
incoming	Configures filtering for incoming IP traffic export or IP traffic capture traffic.

Command	Description
ip traffic-export apply profile	Applies an IP traffic export or IP traffic capture profile to a specific interface.
ip traffic-export profile	Creates an IP traffic export or IP traffic capture profile on an ingress interface.
outgoing	Configures filtering for outgoing IP traffic export or IP traffic capture traffic.
traffic-export interface	Controls the operation of IP traffic capture mode.

traffic-export

To control the operation of IP traffic capture mode in IP traffic export, use the **traffic-export** command in privileged EXEC mode.

traffic-export interface *type number* { **start** | **stop** | **clear** | **copy** *memory-device* }

Syntax Description

type number	Type and number of the interface over which the packets being captured travel.
start	Initiates a packet capture sequence.
stop	Halts a packet capture sequence.
clear	Clears the packet capture buffer.
copy	Copies the contents of the packet capture buffer to an external device.
memory-device	External memory device to which captured packets are transmitted. Options are *flash:*, *tftp:*, or *usbflash0:*.

Command Default

This command has no defaults.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use the **traffic-export** command to control the operation of IP traffic capture mode in IP traffic export. The operator uses CLI commands to start or stop capture of packets flowing across a monitored interface, to copy the captured packets to an external memory device, or to clear the internal buffer which holds the captured packets.

Examples

The following example illustrates the use of the **traffic-export** command to initiate the capture of packets on interface FastEthernet 0/0.

```
Router# traffic-export interface fastethernet 0/0 start
%RITE-5-CAPTURE_START: Started IP traffic capture for interface FastEthernet0/0
router#
```

The following example illustrates the use of the **traffic-export** command to halt the packet capture sequence on interface FastEthernet 0/0.

```
Router# traffic-export interface fastethernet 0/0 stop
%RITE-5-CAPTURE_STOP: Stopped IP traffic capture for interface FastEthernet0/0
router#
```

The following example illustrates the use of the **traffic-export** command to copy the contents of the packet capture buffer to an external memory device. The example of the interactive dialog identifies the external memory device and the remote host in which it resides.

```
Router# traffic-export interface fastethernet0/0 copy tftp:
Address or name of remote host []? 172.18.207.15
Capture buffer filename []? atmcapture
Copying capture buffer to tftp://172.18.207.15/atmcapture !!
router#
```

The following example illustrates the use of the **traffic-export** command to clear the packet capture buffer that is in local memory.

```
Router# traffic-export interface fastethernet 0/0 clear
%RITE-5-CAPTURE_CLEAR: Cleared IP traffic capture buffer for interface FastEthernet0/0

router#
```

Related Commands

Command	Description
ip traffic-export apply profile	Applies an IP traffic export or IP traffic capture profile to a specific interface.
ip traffic-export profile	Creates an IP traffic export or IP traffic capture profile on an ingress interface.

Feature Information for IP Traffic Export

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for IP Traffic Export

Feature Name	Releases	Feature Information
Router IP Traffic Export	12.2(25)S 12.3(4)T	IP traffic over selected interfaces may be exported over a LAN or VLAN interface for monitoring or analysis. The following sections provide information about this feature: • Configuring IP Traffic Export, page 3
Router IP Traffic Export Packet Capture Enhancements	12.4(11)T	IP traffic over selected interfaces may be captured in local router memory and then dumped to external memory. This feature is supported only on Cisco 1841, Cisco 2800 series, and Cisco 3800 series routers. The following sections provide information about this feature: • Configuring IP Traffic Capture, page 5