Configuring Network Security

This chapter contains network security information unique to Cisco IOS Release 12.2SX, which supplements the network security information and procedures in these publications:

- *Cisco IOS Security Configuration Guide*, Release 12.2, at this URL:

  http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/fsecur_c.html
- *Cisco IOS Security Command Reference*, Release 12.2, at this URL

  http://www.cisco.com/en/US/docs/ios/12_2/security/command/reference/fsecur_r.html

Note For complete syntax and usage information for the commands used in this chapter, see these publications:

- The Cisco IOS Master Command List, at this URL:

  http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html
- The Release 12.2 publications at this URL:

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html

Tip For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Participate in the Technical Documentation Ideas forum

This chapter consists of these sections:

Configuring MAC Address-Based Traffic Blocking

To block all traffic to or from a MAC address in a specified VLAN, perform this task:

Command	Purpose
`Router(config)# mac-address-table static mac_address vlan vlan_ID drop`	Blocks all traffic to or from the configured MAC address in the specified VLAN.
`Router(config)# no mac-address-table static mac_address vlan vlan_ID`	Clears MAC address-based blocking.

This example shows how to block all traffic to or from MAC address 0050.3e8d.6400 in VLAN 12:

```
Router# configure terminal
Router(config)# mac-address-table static 0050.3e8d.6400 vlan 12 drop
```

Configuring TCP Intercept

TCP intercept flows are processed in hardware.

For configuration procedures, see the *Cisco IOS Security Configuration Guide*, Release 12.2, "Traffic Filtering and Firewalls," "Configuring TCP Intercept (Preventing Denial-of-Service Attacks)," at this URL:

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfdenl.html

Configuring Unicast Reverse Path Forwarding Check

These sections describe configuring unicast reverse path forwarding check (unicast RPF check):

Understanding PFC3 Unicast RPF Check Support

The unicast RPF check verifies that the source address of received IP packets is reachable. The unicast RPF check discards IP packets that lack a verifiable IP source prefix (route), which helps mitigate problems that are caused by traffic with malformed or forged (spoofed) IP source addresses.

For unicast RPF check without ACL filtering, the PFC3 provides hardware support for the RPF check of traffic from multiple interfaces.

For unicast RPF check with ACL filtering, the PFC determines whether or not traffic matches the ACL. The PFC sends the traffic denied by the RPF ACL to the route processor (RP) for the unicast RPF check. Packets permitted by the ACL are forwarded in hardware without a unicast RPF check.

Unicast RPF Check Guidelines and Restrictions

These sections describe the unicast RPF check guidelines and restrictions:

General Unicast RPF Check Guidelines and Restrictions

When configuring unicast RPF check, follow these guidelines and restrictions:

- The PFC does not provide hardware support for the unicast RPF check for policy-based routing (PBR) traffic. (CSCea53554)
- Unicast RPF does not provide complete protection against spoofing. Spoofed packets can enter a network through unicast RPF-enabled interfaces if an appropriate return route to the source IP address exists.
- The switch applies the same unicast RPF mode to all interfaces where unicast RPF check is configured. Any change that you make in the unicast RPF mode on any interfaces is applied to all interfaces where the unicast RPF check is configured.
- The “allow default” options of the unicast RPF modes do not offer significant protection against spoofing.
  - Strict unicast RPF Check with Allow Default—Received IP traffic that is sourced from a prefix that exists in the routing table passes the unicast RPF check if the prefix is reachable through the input interface. If a default route is configured, any IP packet with a source prefix that is not in the routing table passes the unicast RPF check if the ingress interface is a reverse path for the default route.
  - Loose unicast RPF Check with Allow Default—If a default route is configured, any IP packet passes the unicast RPF check.
- Avoid configurations that overload the route processor with unicast RPF checks.
  - Do not configure unicast RPF to filter with an ACL.
  - Do not configure the global unicast RPF “punt” check mode.

Unicast RPF Check Configuration Guidelines and Restrictions

Although the software supports up to 16 reverse-path interfaces, implement these limits in your configuration:

- Unicast RPF Strict Mode—The unicast RPF strict mode provides the greatest security against spoofed traffic. If, on all unicast RPF-check enabled interfaces, the switch receives valid IP traffic through interfaces that are reverse paths for the traffic, then strict mode is an option in these circumstances:
  - If, on a maximum of 24 interfaces, divided into four groups of six interfaces each, the switch receives valid IP packets that have up to six reverse-path interfaces per source prefix, configure the unicast RPF strict mode with the **mls ip cef rpf multipath interface-group** command.

    This option requires you to identify the source prefixes and the interfaces that serve as reverse paths for the source prefixes and to configure interface groups for those reverse path interfaces. All of the reverse-path interfaces for each source prefix must be in the same interface group.

You can configure four interface groups, with each group containing up to six reverse-path interfaces. There is no limit on the number of source prefixes that an interface group can support.

To ensure that no more than six reverse-path interfaces exist in the routing table for each prefix, enter the **maximum-paths 6** command in config-router mode when configuring OSPF, EIGRP, or BGP.

IP traffic with one or two reverse-path interfaces that is received on uPPF-check enabled interfaces outside the interface groups passes the unicast RPF check if the ingress interface and at most one other interface are reverse paths.

With maximum paths set to six, IP traffic with more than two reverse-path interfaces that is received on uPPF-check enabled interfaces outside the interface groups always pass the unicast RPF check.

- If, on any number of interfaces, the switch receives valid IP packets that have one or two reverse path interfaces per source prefix, configure the unicast RPF strict mode with the **mls ip cef rpf multipath pass** command.

  To ensure that no more than two reverse-path interfaces exist in the routing table for each prefix, enter the **maximum-paths 2** command in config-router mode when configuring OSPF, EIGRP, or BGP.

- Unicast RPF Loose Mode with the Pass Global Mode—The unicast RPF loose mode provides less protection than strict mode, but it is an option on switches that receive valid IP traffic on interfaces that are not reverse paths for the traffic. The unicast RPF loose mode verifies that received traffic is sourced from a prefix that exists in the routing table, regardless of the interface on which the traffic arrives.

Configuring Unicast RPF Check

These sections describe how to configure unicast RPF check:

Configuring the Unicast RPF Check Mode

There are two unicast RPF check modes:

- Strict check mode, which verifies that the source IP address exists in the FIB table and verifies that the source IP address is reachable through the input port.
- Exist-only check mode, which only verifies that the source IP address exists in the FIB table.

Note The most recently configured mode is automatically applied to all ports configured for unicast RPF check.

To configure unicast RPF check mode, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface {{vlan vlan_ID} | {type[1] slot/port} | {port-channel number}}`	Selects an interface to configure. **Note** Based on the input port, unicast RPF check verifies the best return path before forwarding the packet on to the next destination.
Step 2	`Router(config-if)# ip verify unicast source reachable-via {rx | any} [allow-default] [list]`	Configures the unicast RPF check mode.
Step 3	`Router(config-if)# exit`	Exits interface configuration mode.
Step 4	`Router# show mls cef ip rpf`	Verifies the configuration.

1. *type* = **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

When configuring the unicast RPF check mode, note the following information:

- Use the **rx** keyword to enable strict check mode.
- Use the **any** keyword to enable exist-only check mode.
- Use the **allow-default** keyword to allow use of the default route for RPF verification.
- Use the *list* option to identify an access list.
  - If the access list denies network access, spoofed packets are dropped at the port.
  - If the access list permits network access, spoofed packets are forwarded to the destination address. Forwarded packets are counted in the interface statistics.
  - If the access list includes the logging action, information about the spoofed packets is sent to the log server.

Note When you enter the **ip verify unicast source reachable-via** command, the unicast RPF check mode changes on all ports in the switch.

This example shows how to enable unicast RPF exist-only check mode on Gigabit Ethernet port 4/1:

```
Router(config)# interface gigabitethernet 4/1
Router(config-if)# ip verify unicast source reachable-via any
Router(config-if)# end
Router#
```

This example shows how to enable unicast RPF strict check mode on Gigabit Ethernet port 4/2:

```
Router(config)# interface gigabitethernet 4/2
Router(config-if)# ip verify unicast source reachable-via rx
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show running-config interface gigabitethernet 4/2
Building configuration...
Current configuration : 114 bytes
!
interface GigabitEthernet4/2
ip address 42.0.0.1 255.0.0.0
ip verify unicast reverse-path
no cdp enable
```

```
end
Router# show running-config interface gigabitethernet 4/1
Building configuration...
Current configuration : 114 bytes
!
interface GigabitEthernet4/1
ip address 41.0.0.1 255.0.0.0
→ ip verify unicast reverse-path (RPF mode on g4/1 also changed to strict-check RPF mode)
no cdp enable
end
Router#
```

Configuring the Multiple-Path Unicast RPF Check Mode

To configure the multiple-path unicast RPF check mode, perform this task:

	Command	Purpose
Step 1	`Router(config)# mls ip cef rpf mpath {punt | pass | interface-group}`	Configures the multiple path RPF check mode.
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# show mls cef ip rpf`	Verifies the configuration.

When configuring multiple path RPF check, note the following information:

- **punt** mode (default)—The PFC3 performs the unicast RPF check in hardware for up to two interfaces per prefix. Packets arriving on any additional interfaces are redirected (punted) to the RP for unicast RPF check in software.
- **pass** mode—The PFC3 performs the unicast RPF check in hardware for single-path and two-path prefixes. Unicast RPF check is disabled for packets coming from multipath prefixes with three or more reverse-path interfaces (these packets always pass the unicast RPF check).
- **interface-group** mode—The PFC3 performs the unicast RPF check in hardware for single-path and two-path prefixes. The PFC3 also performs the unicast RPF check for up to four additional interfaces per prefix through user-configured multipath unicast RPF check interface groups. Unicast RPF check is disabled for packets coming from other multipath prefixes that have three or more reverse-path interfaces (these packets always pass the unicast RPF check).

This example shows how to configure punt as the multiple path RPF check mode:

```
Router(config)# mls ip cef rpf mpath punt
```

Configuring Multiple-Path Interface Groups

To configure multiple-path unicast RPF interface groups, perform this task:

	Command	Purpose
Step 1	`Router(config)# mls ip cef rpf interface-group [0 | 1 | 2 | 3] interface1 [interface2 [interface3 [interface4]]]`	Configures a multiple path RPF interface group.
Step 2	`Router(config)# mls ip cef rpf interface-group group_number`	Removes an interface group.

	Command	Purpose
Step 3	`Router(config)# end`	Exits configuration mode.
Step 4	`Router# show mls cef ip rpf`	Verifies the configuration.

This example shows how to configure interface group 2:

```
Router(config)# mls ip cef rpf interface-group 2 fastethernet 3/3 fastethernet 3/4
fastethernet 3/5 fastethernet 3/6
```

Enabling Self-Pinging

With unicast RPF check enabled, by default the switch cannot ping itself.

To enable self-pinging, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface {{vlan` *vlan_ID*`} | {`*type*[1] *slot/port*`} | {port-channel` *number*`}}`	Selects the interface to configure.
Step 2	`Router(config-if)# ip verify unicast source reachable-via any allow-self-ping`	Enables the switch to ping itself or a secondary address.
Step 3	`Router(config-if)# exit`	Exits interface configuration mode.

1. *type* = **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to enable self-pinging:

```
Router(config)# interface gigabitethernet 4/1
Router(config-if)# ip verify unicast source reachable-via any allow-self-ping
Router(config-if)# end
```

Tip For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Participate in the Technical Documentation Ideas forum