



Unicast Reverse Path Forwarding for IPv6 on the Cisco 12000 Series Internet Router

The Unicast Reverse Path Forwarding (Unicast RPF) for IPv6 feature reduces problems caused by the introduction of malformed or forged (spoofed) IPv6 source addresses into a network by discarding IPv6 packets that lack a verifiable IPv6 source address. When enabled on a customer-facing interface (or subinterface) of a Cisco 12000 series 10G Engine 5 SPA Interface Processor (10G SIP), this feature filters IPv6 traffic to protect a service-provider network and its customer.

Feature History for Unicast RPF for IPv6

| Release | Modification |
|-----------|--|
| 12.0(31)S | This feature was introduced in the Cisco 12000 series Internet router on the 10G Engine 5 SPA Interface Processor. |

Finding Support Information for Platforms and Cisco IOS Software Images

To find information about platform support and Cisco IOS software image support, access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for Unicast RPF for IPv6, page 2](#)
- [Restrictions for Unicast RPF for IPv6, page 2](#)
- [Implementing Unicast RPF for IPv6, page 3](#)
- [Configuring Unicast RPF for IPv6 in Strict Checking Mode, page 6](#)
- [Configuration Examples for Unicast RPF for IPv6, page 9](#)
- [Additional References, page 10](#)
- [Command Reference, page 11](#)



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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

Prerequisites for Unicast RPF for IPv6

- Supported line cards

In Cisco IOS Release 12.0(31)S, the Unicast RPF for IPv6 feature is supported only on the 10G Engine 5 SPA Interface Processor (10G SIP) in the Cisco 12000 series Internet router.

For information about the modular services cards (SIPs) and shared port adapters (SPAs) supported on the Cisco 12000 series Internet router, refer to the [Cisco 12000 Series Router SIP and SPA Hardware Installation Guide](#).

- Cisco express forwarding

The Unicast RPF for IPv6 feature requires Cisco express forwarding (CEF) to function properly on the Cisco 12000 series Internet router.

It is not necessary to configure an input interface for CEF switching because Unicast RPF has been implemented as a search through the Forwarding Information Base (FIB) using the source IP address. As long as CEF is running on the router, individual interfaces can be configured with other switching modes. Unicast RPF for IPv6 is an input-side function that is enabled on an interface or subinterface that supports any type of encapsulation and operates on IPv6 packets received by the router. It is necessary that CEF is enabled globally in the router—Unicast RPF for IPv6 does not work without CEF.

For more information about CEF, refer to the [Cisco IOS Switching Services Configuration Guide](#), Release 12.3.

Restrictions for Unicast RPF for IPv6

The following restrictions apply to the Unicast RPF for IPv6 feature on the 10G SIP in the Cisco 12000 series Internet router:

- Customer-facing interfaces on PE routers

The Unicast RPF for IPv6 feature is designed to be used only on customer-facing interfaces (or subinterfaces) of the 10G SIP in a Cisco 12000 series Internet router, which is deployed as a provider edge (PE) node. We recommend that you do not enable Unicast RPF on:

- A Cisco 12000 series Internet router used as a core router in a service-provider network
- On a core-facing interface of a PE node

Because traffic in the core network arrives through a customer-facing interface on a PE router, enabling Unicast RPF on a core router or core-facing interface is redundant.

In addition, core-facing interfaces are likely to have routing asymmetry, meaning multiple routes to the source of a packet. Only apply Unicast RPF where there is natural or configured symmetry. If administrators carefully plan the interfaces on which they activate Unicast RPF, routing asymmetry is not a serious problem.

PE routers at the edge of a service-provider network are more likely to have symmetrical reverse paths than routers in the core network. Routers that are in the core network have no guarantee that the best forwarding path out of the router will be the path selected for packets returning to the router. Hence, it is not recommended that you apply Unicast RPF where there is a chance of asymmetric routing. It is simplest to place Unicast RPF for IPv6 only at the edge of a network or, for an Internet service provider (ISP), at the customer edge of the network.

- IPv4 packets

On the Cisco 12000 series Internet router, the Unicast RPF for IPv6 feature does not filter IPv4 traffic.

- Loose versus strict checking modes

On the Cisco 12000 series Internet router, the Unicast RPF for IPv6 feature does not support loose checking mode as on other platforms. Only strict checking mode is supported.

- Strict checking mode verifies that the source IPv6 address of an IPv6 packet exists in the routing table and that the source IPv6 address is reachable by a path through the input interface. To configure strict checking mode, use one of the following commands:

```
ipv6 verify unicast source reachable-via rx  
ipv6 verify unicast reverse-path
```

**Note**

Starting in Cisco IOS Release 12.0(31)S, the Cisco 12000 series Internet router supports both commands to enable Unicast RPF to be compatible with the Cisco IOS Release 12.3T and 12.2S software trains.

- Loose (exist-only) checking mode only verifies that a source IPv6 address exists in the routing table, and is enabled using the **ipv6 verify unicast source reachable-via any** command.

Implementing Unicast RPF for IPv6

To configure the Unicast RPF for IPv6 feature on the Cisco 12000 series Internet router, you should understand the following concepts:

- [Unicast RPF for IPv6 on the Cisco 12000 Series Internet Router, page 3](#)
- [Implementing Unicast RPF for IPv6, page 4](#)
- [Unicast RPF for IPv6 on a Network Access Server—Example, page 4](#)
- [Routing Table Requirements, page 5](#)
- [Restrictions on Using Unicast RPF, page 6](#)

Unicast RPF for IPv6 on the Cisco 12000 Series Internet Router

When the Unicast RPF for IPv6 feature is enabled on an interface:

1. The Cisco 12000 series Internet router examines all IPv6 packets received as input on that interface to make sure that the source address and source interface appear in the routing table and match the interface on which the packet was received. This ability to “look backwards” is available only when Cisco express forwarding (CEF) is enabled on the router, because the lookup relies on the presence of the Forwarding Information Base (FIB). CEF generates the FIB as part of its operation.

**Note**

Unicast RPF for IPv6 is an input function and is applied only on the input interface of a Cisco 12000 series Internet router at the upstream end of a connection.

2. Unicast RPF for IPv6 checks to see if any IPv6 packet received at an interface arrives on the best return path (return route) to the source of the packet by performing a reverse lookup in the CEF table:
 - If the IPv6 packet was received from one of the best reverse path routes, the packet is forwarded as normal.
 - If no reverse path route exists on the same interface from which the packet was received, it might mean that the source address was modified.
 - If Unicast RPF does not find a reverse path for the packet, the packet is dropped.
3. When an IPv6 packet is received at the interface on which you have configured Unicast RPF for IPv6, the following actions occur:
 - a. Unicast RPF for IPv6 checks to see if the packet has arrived on the best return path to the source, which it does by doing a reverse lookup in the FIB table.
 - b. CEF table (FIB) lookup is carried out for packet forwarding.
 - c. The IPv6 packet is forwarded.

For information about how Unicast RPF for IPv6 works with CEF to validate IPv6 source addresses by verifying packet return paths, refer to [Configuring Unicast Reverse Path Forwarding](#) in the *Cisco IOS Security Configuration Guide*, Release 12.3.

Implementing Unicast RPF for IPv6

On the Cisco 12000 series Internet router, Unicast RPF for IPv6 is implemented as follows:

- The IPv6 packet must be received at an interface with the best return path (route) to the packet source (a process called symmetric routing). There must be a route in the FIB matching the route to the receiving interface. Adding a route in the FIB can be done via static route, network statement, or dynamic routing.
- IPv6 source addresses at the receiving interface must match the routing entry for the interface.
- Unicast RPF for IPv6 is an input function and is applied only on the input interface of a router at the upstream end of a connection.

Given these implementation principles, Unicast RPF for IPv6 becomes a tool that network administrators can use not only for their customers but also for their downstream network or ISP, even if the downstream network or ISP has other connections to the Internet.

For guidelines to use when deploying Unicast RPF for IPv6 on the Cisco 12000 series Internet router, refer to [Configuring Unicast Reverse Path Forwarding](#) in the *Cisco IOS Security Configuration Guide*, Release 12.3.

Unicast RPF for IPv6 on a Network Access Server—Example

In a service-provider network, aggregation routers are ideal places to use Unicast RPF for IPv6 with single-homed clients. A “single-homed” environment has only one access point out of the network; that is, one upstream connection. Networks having one access point offer the best example of symmetrical routing, which means that the interface at which a packet enters the network is also the best return path to the source of the IPv6 packet.

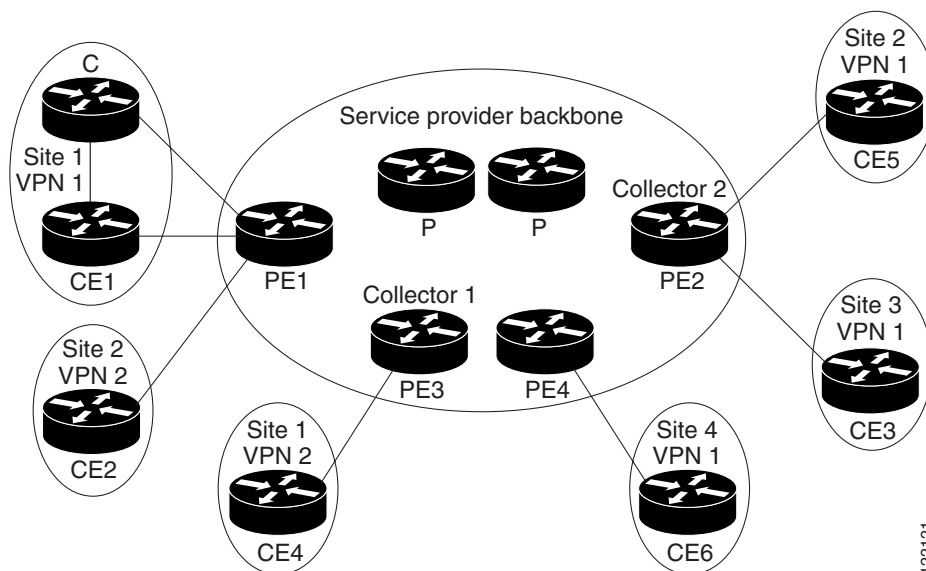
Unicast RPF for IPv6 is best used:

- At the network perimeter for Internet, intranet, or extranet environments, or in ISP environments for customer network terminations.
- On leased-line or PSTN/ISDN/xDSL customer connections into the Internet.

In fact, dialup connections are reputed to be the greatest source of DoS attacks using forged IPv6 addresses. If the network access server supports CEF, Unicast RPF for IPv6 works. In this topology, the customer aggregation routers need not have the full Internet routing table. Aggregation routers need the routing prefixes information (IP address block); hence, information configured or redistributed in the Interior Gateway Protocol (IGP) or Internal Border Gateway Protocol (IBGP) (depending on the way that you add customer routes into your network) are enough for Unicast RPF for IPv6 to function.

Figure 1 illustrates the application of Unicast RPF for IPv6 to the aggregation and access Cisco 12000 series Internet routers for an ISP point-of-presence (POP) with routers providing dialup customer connections.

Figure 1 Unicast RPF for IPv6 Applied to POP Aggregation Routers



In this example, Unicast RPF for IPv6 is applied upstream from the customer dialup connection router on the receiving (input) interfaces of the ISP aggregation routers.

Routing Table Requirements

To work correctly, Unicast RPF for IPv6 needs proper information in the CEF tables. This requirement does not mean that the Cisco 12000 series Internet router must have the entire Internet routing table. The amount of routing information required in the CEF tables depends on the:

- Location of the Unicast RPF for IPv6 configuration
- Functions the router performs in the network

For example:

- In an ISP environment, a router that is a leased-line aggregation router for customers needs only the information based on the static routes redistributed into the IGP or IBGP (depending on which technique is used in the network). Unicast RPF for IPv6 is configured on the customer interfaces—hence the requirement for minimal routing information.
- A single-homed ISP could place Unicast RPF for IPv6 on the gateway link to the Internet. The full Internet routing table is required. Requiring the full routing table helps protect the ISP from external DoS attacks that use addresses that are not in the Internet routing table.

Restrictions on Using Unicast RPF

Do not use Unicast RPF for IPv6 on core-facing interfaces that are internal to the network. Core-facing interfaces are likely to have multiple routes to the source of a packet. For the best return path (route) to the packet source, only apply Unicast RPF for IPv6 to the interface on which IPv6 packets are received. If administrators carefully plan for the interfaces on which they enable Unicast RPF for IPv6, then routing asymmetry is not a serious problem.

For example, routers:

- At the *edge* of the network of an ISP are more likely to have symmetrical reverse paths than routers that are in the core of the ISP network.
- In the *core* of the ISP network have no guarantee that the best forwarding path out of the router will be the path selected for packets returning to the router.

Hence, we do not recommend that you apply Unicast RPF for IPv6 in cases in which a chance of asymmetric routing exists. Only deploy Unicast RPF for IPv6 on a Cisco 12000 series Internet router at the edge of a network, or for an ISP at the customer edge of the network.

Configuring Unicast RPF for IPv6 in Strict Checking Mode

This section describes the procedures for configuring the Unicast RPF for IPv6 feature in strict checking mode to filter IPv6 packets on the Cisco 12000 series Internet router.

Strict checking mode verifies that the source IPv6 address of an IPv6 packet exists in the routing table and that the source IPv6 address is reachable by a path through the input interface. To configure strict checking mode for IPv6, use one of the following commands:

- **ipv6 verify unicast source reachable-via rx**
- **ipv6 verify unicast reverse-path**

Starting in Cisco IOS Release 12.0(31)S, the Cisco 12000 series Internet router supports both commands to enable Unicast RPF to be compatible with the Cisco IOS Release 12.3T and 12.2S software trains.



Note

On the Cisco 12000 series Internet router, it is not necessary to enable Cisco Express Forwarding for IPv6 (CEFv6) using the **ipv6 cef** command because CEF is enabled by default in distributed mode on Cisco 12000 series line cards. The line cards can perform the express forwarding by themselves, relieving the main route processor (GRP or PRP) of involvement in the switching operation.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface *slot/port***
4. **ipv6 verify unicast source reachable-via rx**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|---|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | interface <i>type slot/subslot/port</i> Example: Router(config)# interface gigabitethernet 2/0/0 | Specifies an input interface on which you want to apply Unicast RPF for IPv6 and enters interface configuration mode. <ul style="list-style-type: none"> • The <i>type</i> argument is the type of interface to be configured. • The <i>slot/subslot/port</i> argument specifies the slot and port numbers of a SPA interface <p>Note When you configure a SPA on the Cisco 12000 series Internet router, the interface address is in the format <i>slot/subslot/port</i>.</p> |
| Step 4 | ipv6 verify unicast source reachable-rx Example: Router(config-if)# ipv6 verify unicast reverse-path | Enables the Unicast RPF for IPv6 feature in strict checking mode to filter IPv6 packets. |
| Step 5 | exit Example: Router(config-if)# exit | Exits interface configuration mode. Repeat Steps 3 and 4 for each interface on which you want to apply Unicast RPF for IPv6 in strict checking mode. |

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface *slot/port***
4. **ipv6 verify unicast reverse-path**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | <code>enable</code> Example: Router> <code>enable</code> | Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted. |
| Step 2 | <code>configure terminal</code> Example: Router# <code>configure terminal</code> | Enters global configuration mode. |
| Step 3 | <code>interface type slot/subslot/port</code> Example: Router(config)# <code>interface gigabitethernet 2/0/0</code> | Specifies an input interface on which you want to apply Unicast RPF for IPv6 and enters interface configuration mode. <ul style="list-style-type: none"> The <i>type</i> argument is the type of interface to be configured. The <i>slot/subslot/port</i> argument specifies the slot and port numbers of a SPA interface. Note When you configure a SPA on the Cisco 12000 series Internet router, the interface address is in the format <i>slot/subslot/port</i> . |
| Step 4 | <code>ipv6 verify unicast reverse-path</code> Example: Router(config-if)# <code>ipv6 verify unicast reverse-path</code> | Enables the Unicast RPF for IPv6 feature in strict checking mode to filter IPv6 packets on a Cisco 12000 series Internet router. |
| Step 5 | <code>exit</code> Example: Router(config-if)# <code>exit</code> | Exits interface configuration mode. Repeat Steps 3 and 4 for each interface on which you want to apply Unicast RPF for IPv6 with reverse-path checking. |

Monitoring and Maintaining Unicast RPF for IPv6

To display information about the Unicast RPF for IPv6 feature configured on an interface, use the following show commands in privileged EXEC mode. For more information, refer to the “[Basic Connectivity for IPv6](#)” section in the *Cisco IOS IPv6 Command Reference*.

| Command | Purpose |
|--|--|
| Router# <code>show ip cef interface type number</code> | Displays detailed CEF status for a specified interface. |
| Router# <code>show ipv6 cef</code> | Display entries in the IPv6 Forwarding Information Base (FIB). |
| Router# <code>show ipv6 cef summary</code> | Displays a summary of the entries in the IPv6 FIB. |

Configuration Examples for Unicast RPF for IPv6

This section contains the following configuration examples for Unicast RPF for IPv6:

- [Configuring Unicast RPF for IPv6 with Strict Checking—Examples](#)
- [Verifying Unicast RPF for IPv6—Example](#)

Configuring Unicast RPF for IPv6 with Strict Checking—Examples

The following example shows how to configure the Unicast RPF for IPv6 feature in strict checking mode on an input 10G SIP Gigabit Ethernet interface in a Cisco 12000 series Internet router:

```
Router# configure terminal
Router(config)# interface gigabitethernet 3/1/1
Router(config-if)# ipv6 verify unicast source reachable-via rx
```

The next example also shows how to configure the Unicast RPF for IPv6 feature in strict checking mode on the same input interface in a Cisco 12000 series Internet router using the **ipv6 verify unicast reverse-path** command:

```
Router# configure terminal
Router(config)# interface gigabitethernet 3/1/1
Router(config-if)# ipv6 verify unicast reverse-path
```

Verifying Unicast RPF for IPv6—Example

To verify that Unicast RPF for IPv6 is operational, use the **show cef interface type slot/subslot/port internal** command in privileged EXEC mode.

As shown in the following example, Unicast RPF for IPv6 is enabled if the line starting with IPv6 unicast RPF appears. If this line is not displayed, the Unicast RPF feature is not enabled. The numbers following drop= and sdrop= show the number of IPv6 packets dropped by Unicast RPF.

```
Router# show cef interface pos 2/0/1 internal

POS2/1 is up (if_number 6)
  Corresponding hwidb fast_if_number 6
  Corresponding hwidb firstsw->if_number 6
  Internet Protocol processing disabled
  Interface is marked as point to point interface
  Interface generates an auto-adjacency
  Hardware idb is POS2/0/1 (6)
  Software idb is POS2/0/1 (6)
  Fast switching type 4, interface type 11
  IP Distributed CEF switching enabled
  IP Null turbo vector
  Input fast flags 0x0, Output fast flags 0x0, Flags 0x80041
  ifindex 5(5)
  Slot 2 Slot unit 1 VC -1
  Transmit limit accumulator 0x0 (0x0)
  IP MTU 4470
  Subblocks:
    IPv6 unicast RPF: acl=None, drop=0, sdrop=0
    IPv6: enabled 1 unreachable FALSE redirect TRUE mtu 4470 flags 0x0
      link-local address is FE80::204:6DFF:FE9A:CFFF
      Global unicast address(es):
        BBBB::1, subnet is BBBB::/64
      Input features: RPF
```

Additional References

```
ee48sb: uidb valid
  rx_uidb_index=12, tx_uidb_index=12
  if_number=6, bulk_sync_flag=0x0
Subinterface Counters Subblock active
```

Additional References

The following sections provide references related to the Unicast RPF for IPv6 feature.

Related Documents

| Related Topic | Document Title |
|---|--|
| Configuring Unicast RPF | “Configuring Unicast Reverse Path Forwarding” chapter in the <i>Cisco IOS Security Configuration Guide, Release 12.3</i> |
| Information about Cisco Express Forwarding on the Cisco 12000 series Internet Router | Understanding Cisco Express Forwarding “Cisco Express Forwarding” chapter in the <i>Cisco IOS Switching Configuration Guide, Release 12.0</i> |
| Unicast RPF configuration command for IPv4: complete command syntax, command mode, defaults, usage guidelines and examples | ip verify unicast reverse-path command reference page in the <i>Cisco IOS Security Command Reference, Release 12.3</i> |
| IPv6 | Cisco IOS IPv6 Configuration Library |
| IPv6 commands: complete command syntax, command mode, defaults, usage guidelines and examples. | “Basic Connectivity for IPv6” chapter in the <i>Cisco IOS IPv6 Command Reference</i> |
| Configuration and troubleshooting procedures for the SPA interface processors (SIPs) and shared port adapters (SPAs) supported on a Cisco 12000 series Internet router. | Cisco 12000 Series Router SIP and SPA Software Configuration Guide (IOS) |

Standards

| Standards | Title |
|---|-------|
| No new or modified standards are supported by this feature. | — |

MIBs

| MIBs | MIBs Link |
|--|--|
| No new or modified MIBs are supported 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. | — |

Technical Assistance

| Description | Link |
|--|---|
| The Cisco Technical Support website, containing 30,000 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/public/support/tac/home.shtml |

Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in Cisco IOS Release 12.0S command reference publications.

- [ipv6 verify unicast reverse-path](#), page 12
- [ipv6 verify unicast source reachable-via rx](#), page 16

ipv6 verify unicast reverse-path

To enable Unicast Reverse Path Forwarding (Unicast RPF) for IPv6, use the **ipv6 verify unicast reverse-path** command in interface configuration mode. To disable Unicast RPF, use the **no** form of this command.

```
ipv6 verify unicast reverse-path [access-list name]
```

```
no ipv6 verify unicast reverse-path [access-list name]
```

Syntax Description

access-list name (Optional) Specifies the name of the access list.

Note This keyword and argument are not supported on the Cisco 12000 series Internet router.

Defaults

Unicast RPF is disabled.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-------------|--|
| 12.2(13)T | This command was introduced. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.0(31)S | This command was integrated into Cisco IOS Release 12.0(31)S and introduced on the 10G Engine 5 SPA Interface Processor in the Cisco 12000 series Internet router. |
| 12.2(27)SBC | This command was integrated into Cisco IOS Release 12.2(27)SBC. |

Usage Guidelines

The Unicast RPF for IPv6 feature requires that Cisco Express Forwarding for IPv6 (CEFv6) is enabled on the router.

On a Cisco 12000 series Internet router, the **ipv6 verify unicast reverse-path** command is used to enable Unicast RPF for IPv6 in strict checking mode.



Note

Beginning in Cisco IOS Release 12.0(31)S, the Cisco 12000 series Internet router supports both the **ipv6 verify unicast reverse-path** and **ipv6 verify unicast source reachable-via rx** commands to enable Unicast RPF to be compatible with the Cisco IOS Release 12.3T and 12.2S software trains.

Use the **ipv6 verify unicast reverse-path** command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through a router. Malformed or forged source addresses can indicate denial-of-service (DoS) attacks based on source IP address spoofing.

When Unicast RPF is enabled on an interface, the router examines all packets received on that interface. The router checks to make sure that the source IPv6 address appears in the routing table and that it is reachable by a path through the interface on which the packet was received. Unicast RPF is an input feature and is applied only on the input interface of a router at the upstream end of a connection.

The Unicast RPF feature performs a reverse lookup in the CEF table to check if any packet received at a router interface has arrived on a path identified as a best return path to the source of the packet. If a reverse path for the packet is not found, Unicast RPF can drop or forward the packet, depending on whether an ACL is specified in the Unicast RPF command. If an ACL is specified in the command, then when (and only when) a packet fails the Unicast RPF check, the ACL is checked to determine whether the packet should be dropped (using a deny statement in the ACL) or forwarded (using a permit statement in the ACL). Whether a packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for Unicast RPF drops and in the interface statistics for Unicast RPF.

If no ACL is specified in the Unicast RPF command, the router drops the forged or malformed packet immediately and no ACL logging occurs. The router and interface Unicast RPF counters are updated.

Unicast RPF events can be logged by specifying the logging option for the ACL entries used by the Unicast RPF command. Log information can be used to gather information about the attack, such as source address, time, and so on.

**Note**

When you configure Unicast RPF for IPv6 on the Cisco 12000 series Internet router, the most recently configured checking mode is not automatically applied to all interfaces as on other platforms. You must enable Unicast RPF for IPv6 separately on each interface.

When you configure a SPA on the Cisco 12000 series Internet router, the interface address is in the format *slot/subslot/port*.

The optional **access-list** keyword for the **ipv6 verify unicast reverse-path** command is not supported on the Cisco 12000 series Internet router. For information about how Unicast RPF can be used with ACLs on other platforms to mitigate the transmission of invalid IPv4 addresses (perform egress filtering) and to prevent (deny) the reception of invalid IPv4 addresses (perform ingress filtering), refer to the “Configuring Unicast Reverse Path Forwarding” chapter in the “Other Security Features” section of the *Cisco IOS Security Configuration Guide*, Release 12.4.

**Note**

When using Unicast RPF, all equal-cost “best” return paths are considered valid. This means that Unicast RPF works in cases where multiple return paths exist, provided that each path is equal to the others in terms of the routing cost (number of hops, weights, and so on).

Do not use Unicast RPF on core-facing interfaces that are internal to the network. Internal interfaces are likely to have routing asymmetry, meaning that there are multiple routes to the source of a packet. Apply Unicast RPF only where there is natural or configured symmetry.

For example, routers at the edge of the network of an Internet service provider (ISP) are more likely to have symmetrical reverse paths than routers that are in the core of the ISP network. Routers that are in the core of the ISP network have no guarantee that the best forwarding path out of the router will be the path selected for packets returning to the router. Hence, it is not recommended that you apply Unicast RPF where there is a chance of asymmetric routing. It is simplest to place Unicast RPF only at the edge of a network or, for an ISP, at the customer edge of the network.

Examples**Unicast Reverse Path Forwarding on a Serial Interface**

The following example shows how to enable the Unicast RPF feature on a serial interface:

```
interface serial 5/0/0
  ipv6 verify unicast reverse-path
```

Unicast Reverse Path Forwarding on a Cisco 12000 Series Internet Router

The following example shows how to enable Unicast RPF for IPv6 with strict checking on a 10G SIP Gigabit Ethernet interface 2/1/2:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface gigabitEthernet 2/1/2
Router(config-if)# ipv6 verify unicast reverse-path
Router(config-if)# exit
```

Unicast Reverse Path Forwarding on a Single-Homed ISP

The following example uses a very simple single-homed ISP to demonstrate the concepts of ingress and egress filters used in conjunction with Unicast RPF. The example illustrates an ISP-allocated classless interdomain routing (CIDR) block 209.165.202.128/28 that has both inbound and outbound filters on the upstream interface. Be aware that ISPs are usually not single-homed. Hence, provisions for asymmetrical flows (when outbound traffic goes out one link and returns via a different link) need to be designed into the filters on the border routers of the ISP.

```
interface Serial 5/0/0
description Connection to Upstream ISP
ipv6 address FE80::260:3EFF:FE11:6770/64
no ipv6 redirects
ipv6 verify unicast reverse-path abc
!
ipv6 access-list abc
permit ipv6 host 2::1 any
deny ipv6 FEC0::/10 any
  ipv6 access-group abc in
  ipv6 access-group jkl out
!
access-list abc permit ip FE80::260:3EFF:FE11:6770/64 2001:0DB8:0000:0001::0001any
access-list abc deny ipv6 any any log
access-list jkl deny ipv6 host 2001:0DB8:0000:0001::0001 any log
access-list jkl deny ipv6 2001:0DB8:0000:0001:FFFF:1234::5.255.255.255 any log
access-list jkl deny ipv6 2002:0EF8:002001:0DB8:0000:0001:FFFF:1234::5172.16.0.0
0.15.255.255 any log
access-list jkl deny ipv6 2001:0CB8:0000:0001:FFFF:1234::5 0.0.255.255 any log
access-list jkl deny ipv6 2003:0DB8:0000:0001:FFFF:1234::5 0.0.0.31 any log
access-list jkl permit ipv6
```

ACL Logging with Unicast RPF

The following example demonstrates the use of ACLs and logging with Unicast RPF. In this example, extended ACL abc provides entries that deny or permit network traffic for specific address ranges. Unicast RPF is configured on interface Ethernet 0/0 to check packets arriving at that interface.

For example, packets with a source address of 8765:4321::1 arriving at interface Ethernet 0 are dropped because of the deny statement in ACL “abc.” In this case, the ACL information is logged (the logging option is turned on for the ACL entry) and dropped packets are counted per-interface and globally. Packets with a source address of 1234:5678::1 arriving at interface Ethernet 0/0 are forwarded because of the permit statement in ACL abc. ACL information about dropped or suppressed packets is logged (the logging option is turned on for the ACL entry) to the log server.

```
!
```

```
interface ethernet 0/0
ipv6 address FE80::260:3EFF:FE11:6770/64 link-local
ipv6 verify unicast reverse-path abc
!
ipv6 access-list abc
permit ipv6 1234:5678::/64 any log-input
deny ipv6 8765:4321::/64 any log-input
```

Related Commands

| Command | Description |
|---------------------------------------|--|
| ip cef | Enables CEF on the route processor card. |
| ip verify unicast reverse-path | Enables Unicast RPF for IPv4 traffic. |
| ipv6 cef | Enables CEF for IPv6 interfaces. |

ipv6 verify unicast source reachable-via rx

To enable Unicast RPF for IPv6 in strict checking mode on a Cisco 12000 series Internet router, use the **ipv6 verify unicast source reachable-via rx** command in interface configuration mode. To disable Unicast RPF, use the **no** form of this command.

ipv6 verify unicast source reachable-via rx

no ipv6 verify unicast source reachable-via rx

Syntax Description

This command has no arguments or keywords.

Defaults

Unicast RPF is disabled.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-----------|--|
| 12.0(31)S | This command was introduced on the 10G Engine 5 SPA Interface Processor in the Cisco 12000 series Internet router. |

Usage Guidelines

Use the **ipv6 verify unicast source reachable-via rx** command to enable the Unicast RPF for IPv6 feature in strict checking mode.



Note

Starting in Cisco IOS Release 12.0(31)S, the Cisco 12000 series Internet router supports both the **ipv6 verify unicast reverse-path** and **ipv6 verify unicast source reachable-via rx** commands to enable Unicast RPF to be compatible with Cisco IOS Release 12.3T and 12.2S software.

1. The Unicast RPF feature verifies that the source IPv6 address exists in the routing table and that the source IPv6 address is reachable by a path through the input interface.
2. When Unicast RPF is enabled on an interface, the router examines all packets received on that interface. The router checks to make sure that the source address appears in the routing table and matches the interface on which the packet was received. Unicast RPF is an input feature and is applied only on the input interface of a router at the upstream end of a connection.
3. The Unicast Reverse Path Forwarding feature performs a reverse lookup in the CEF table to see if any packet received at a router interface has arrived on a path identified as a best return paths to the source of the packet. The feature does this by performing a reverse lookup in the CEF table.
4. If Unicast RPF does not find a reverse path for the packet, Unicast RPF drops the packet.

**Note**

When you configure Unicast RPF for IPv6 on the Cisco 12000 series Internet router, the most recently configured checking mode is not automatically applied to all interfaces as on other platforms. You must enable Unicast RPF for IPv6 separately on each interface.

When you configure a SPA on the Cisco 12000 series Internet router, the interface address is in the format *slot/subslot/port*.

The optional *access-list*, **allow-self-ping**, **allow-default**, and **any** (enables loose checking mode) parameters, that are supported in the **ip verify unicast source reachable-via** command for IPv4 traffic on other platforms, are not supported for the **ipv6 verify unicast source reachable-via rx** command on the Cisco 12000 series Internet router.

The Unicast RPF for IPv6 feature requires that Cisco Express Forwarding for IPv6 (CEFv6) is enabled on the router.

Do not use Unicast RPF for IPv6 on core-facing interfaces that are internal to the network. Internal interfaces are likely to have routing asymmetry, meaning that there are multiple routes to the source of a packet.

Only apply Unicast RPF for IPv6 where there is natural or configured symmetry. For example, Cisco 12000 series Internet routers:

- At the *edge* of a service-provider network are more likely to have symmetrical reverse paths than routers that are in the core of the network.
- In the *core* of a service-provider network have no guarantee that the best forwarding path out of the router will be the path selected for packets returning to the router.

Hence, it is not recommended that you apply Unicast RPF for IPv6 RPF where there is a chance of asymmetric routing. Only place Unicast RPF for IPv6 at the edge of a network, or for a service provider at the customer edge of the network.

Examples

The following example shows how to enable Unicast RPF for IPv6 in strict checking mode on a 10G SIP Gigabit Ethernet interface.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface gigabitEthernet 1/2/1
Router(config-if)# ipv6 verify unicast source reachable-via rx
Router(config-if)# exit
```

Related Commands

| Command | Description |
|---|--|
| ip verify unicast source reachable-via | Enables Unicast RPF for IPv4 traffic in loose or strict checking mode. |

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0711R)
partnership relationship between Cisco and any other company. (0/11R)

Copyright © 2005 Cisco Systems, Inc. All rights reserved.