



# Unicast Reverse Path Forwarding in Strict Mode on the Cisco 12000 Series Internet Router

---

**Part Number OL-15426-01, May 30, 2008**

The Unicast Reverse Path Forwarding (Unicast RPF) in Strict Mode feature is a network security tool designed for use at the edge of a service-provider network to mitigate network attacks and provide protection from:

- Data packets with malformed or forged IP source addresses received at the router (known as *source address IP spoofing*)
- Data packets received from known IP addresses in multiple, shifting attacks

Starting in Cisco IOS Release 12.0(33)S, Unicast RPF is supported for IPv4 traffic filtering in strict mode, in addition to loose mode, on the Cisco 12000 series Internet router. Strict mode verifies that the source address of an IPv4 packet both exists in the routing table and is reachable by a path through the input interface before forwarding a packet. (Loose mode only verifies that the source IPv4 address exists in the routing table.)

## 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 Unicast RPF in Strict Mode on the Cisco 12000 Router](#)” section on page 22.

## 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

- [Prerequisites for Unicast Reverse Path Forwarding in Strict Mode on the Cisco 12000 Series Internet Router, page 2](#)



---

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

© 2008 Cisco Systems, Inc. All rights reserved.

- [Restrictions for Unicast Reverse Path Forwarding in Strict Mode on the Cisco 12000 Series Router, page 3](#)
- [Unicast Reverse Path Forwarding in Strict Mode on the Cisco 12000 Router, page 4](#)
- [Configuring Unicast RPF in Strict Mode on the Cisco 12000 Router, page 9](#)
- [Monitoring and Maintaining Unicast RPF, page 12](#)
- [Configuration Examples for Unicast RPF in Strict Mode on the Cisco 12000 Router, page 12](#)
- [Additional References, page 14](#)
- [Command Reference, page 15](#)
- [Feature Information for Unicast RPF in Strict Mode on the Cisco 12000 Router, page 22](#)

## Prerequisites for Unicast Reverse Path Forwarding in Strict Mode on the Cisco 12000 Series Internet Router

Note the following prerequisites when you configure the Unicast RPF in Strict Mode feature on the Cisco 12000 series Internet router.

### Supported Line Cards

Cisco IOS Release 12.0(33)S introduces support for the Unicast RPF in Strict Mode feature on all IP Services Engine (ISE/Engine 3) and Engine 5 line cards in the Cisco 12000 series Internet router. For information about the ISE and Engine 5 service interface processors (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](#).



#### Note

---

ISE and Engine 5 line cards already support Unicast RPF in loose

---

On the Cisco 12000 series Internet router, Unicast RPF is supported on other Engine types as follows:

- Engine 4 line cards do not support Unicast RPF.
- Engine 4+ line cards support Unicast RPF only in loose mode, but only on main interfaces. Subinterfaces are not supported.
- Engine 6 line cards support Unicast RPF only in loose mode.

For information on the differences between loose and strict checking modes, see [“Strict Versus Loose Checking Mode” section on page 5](#).

### Cisco Express Forwarding

The Unicast RPF in Strict Mode feature requires Cisco express forwarding (CEF) to function properly. CEF is enabled, by default, 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 is an input-side function that is enabled on an interface or subinterface that supports any type of encapsulation and operates on IPv4 packets received by the router. CEF must be enabled globally in the router—Unicast RPF 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 Reverse Path Forwarding in Strict Mode on the Cisco 12000 Series Router

The following restrictions apply when you configure the Unicast RPF in Strict Mode feature on the Cisco 12000 series Internet router.

## IPv4 Input Traffic Only

The Unicast RPF in Strict Mode feature supports the filtering only of IPv4 traffic in the ingress direction.

## Strict Versus Loose Checking Mode

The Unicast RPF in Strict Mode feature filters ingress IPv4 traffic in strict checking mode and forwards packets only if the following conditions are satisfied. (For more information, see [“Strict Versus Loose Checking Mode”](#) section on page 5.)

- An IPv4 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 Forwarding Information Base (FIB) that matches the route to the receiving interface. Adding a route in the FIB can be done via static route, network statement, or dynamic routing.
- IPv4 source addresses at the receiving interface must match the routing entry for the interface.

## Customer-Facing Interfaces

The Unicast RPF in Strict Mode feature is used only on customer-facing interfaces (or subinterfaces) on the 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 issue.

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 is the path selected for packets returning to the router. Hence, we do not recommend that you apply Unicast RPF if a chance of asymmetric routing exists. Instead, place Unicast RPF only at the edge of a network. Or, for an Internet service provider (ISP), place Unicast RPF at the customer edge of the network.

### Access List Option

Cisco 12000 series hardware-forwarding engines, such as ISE and Engine 5 line cards, do not support the access-list option with the Unicast RPF in Strict Mode feature as other platforms. The access-list option allows you to specify a numbered access control list (ACL) when you enable Unicast RPF so that the ACL is used as an additional filter to determine if a packet with a malformed or forged IP source address should be dropped or forwarded.

### IP Prefix Load Balancing and Accounting

The Unicast RPF in Strict Mode feature supports up to eight interfaces on which per-packet load balancing is configured on the same line card. If you configure load balancing for a specified IP prefix on more than eight interfaces, Unicast RPF is performed in loose checking mode.

The IP prefix accounting and Unicast RPF in Strict Mode features are not supported together on the same line card.

## Unicast Reverse Path Forwarding in Strict Mode on the Cisco 12000 Router

To configure and use Unicast Reverse Path Forwarding in Strict Mode on the Cisco 12000 series router, you should understand the following concepts:

- [Enhanced Security at Network Edge, page 4](#)
- [Strict Versus Loose Checking Mode, page 5](#)
- [Unicast RPF in Strict Mode Feature Description, page 6](#)
- [Implementing Unicast RPF in Strict Mode on the Cisco 12000 Router, page 8](#)

### Enhanced Security at Network Edge

The Unicast Reverse Path Forwarding (Unicast RPF) in Strict Mode feature is used on customer-facing interfaces (or subinterfaces) in a Cisco 12000 series router, which is deployed as a provider edge (PE) router at the edge of a service-provider network.

Unicast RPF in strict mode provides protection from the following types of network attacks by discarding IPv4 packets that either lack a verifiable IPv4 source address or use a valid, reachable IPv4 address as the source of an attack:

- Source IP address spoofing—Unicast RPF filters ingress traffic so that IPv4 packets with invalid source addresses are discarded; for example, forged source IPv4 addresses.
- Source IP-based black holes—Unicast RPF dynamically changes ingress traffic filtering to drop traffic received from one or more valid IPv4 addressees that are identified as the source of multiple, shifting attacks.

### Protection from Source IP Address Spoofing

Packets with forged (spoofed) source IP addresses are often used to conduct attacks on a network by evading traceability and bypassing access controls. Common denial-of-service (DoS) attacks take advantage of forged or rapidly changing source IP addresses to thwart efforts to locate or filter the attacks. Forged IP addresses are also used to direct an attack at a forged source (known as a *reflection attack*).

By implementing ingress traffic filtering as specified in RFC 2827, the Unicast RPF in Strict Mode feature renders DoS attacks based on forged source addresses ineffective by forwarding only packets that have source addresses that are valid and consistent with the IP routing table.

RFC 2827 defines the ingress traffic filtering requirements designed to discard packets with invalid source IP addresses. Common examples of invalid source IP addresses include:

- Valid IP network addresses that do not originate in the network
- IP address allocated for private intranets or non allocated IP address ranges (as specified by RFC 1918)

To be most effective in preventing source IP addresses spoofing, enable Unicast RPF in strict mode on a PE router at the edge of your network. Ingress traffic filtering on a PE router minimizes the range of valid IP addresses and discards anomalous IPv4 packets as close to their origin as possible.

After you secure a network from the use of invalid source IP addresses, DoS attacks may start from valid, reachable IP addresses, which permits the identification of the originator. See the [“Protection Using Black Hole Filtering”](#) section on page 5 for more information.

## Protection Using Black Hole Filtering

To dynamically and efficiently drop traffic from a specific, valid IP address that is identified as the source of an attack, the Unicast RPF in Strict mode feature uses two additional ingress traffic filtering techniques:

- Source IP-based black hole filtering
- Source IP-based Remote Triggered Black Hole (RTBH) filtering

These traffic filtering techniques provide network security that reacts quickly to mitigate multiple, shifting attacks, including Denial of Service (DoS), Distributed DoS (DDoS), and worm attacks, that originate from a particular IPv4 address. All incoming IPv4 traffic from a known IPv4 address that is identified as the source of an attack is dropped.

As an advanced security feature, you can place black holes in a network in which traffic is forwarded and dropped. Once an attack has been detected, black holing can be used to drop all attack traffic at the edge of a service-provider network, based on source IP addresses. The attack traffic is forwarded to a null0 interface. Null0 is a pseudo-interface that is always up and can never forward or receive traffic.

RTBH filtering is a technique that uses routing protocol updates to manipulate route tables at the network edge or anywhere else in the network to specifically drop undesirable traffic before it enters the service-provider network. For more information, refer to [Remotely Triggered Black Hole Filtering—Destination-based and Source-based](#).

## Strict Versus Loose Checking Mode

On the Cisco 12000 series Internet router, in Cisco IOS Release 12.0(32)S and earlier releases, the Unicast RPF feature is supported only in loose checking mode to filter IPv4 traffic. Starting in Cisco IOS Release 12.0(33)S, Unicast RPF in strict mode is also supported. The differences between the two modes are as follows:

- Strict checking mode verifies that the source IPv4 address of an IPv4 packet exists in the routing table and that the source IPv4 address is reachable by a path through the input interface (the interface on which the packet enters the router). To configure strict checking mode, use one of the following commands:

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



**Note** Although 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, you are recommended to use the newer version of the command (**ip verify unicast source reachable-via rx**) as described in this document.

- Loose (exist-only) checking mode only verifies that a source IPv4 address exists in the routing table and that a valid path through any interface exists in the Forwarding Information Base (FIB). Loose mode is enabled by using the **ip verify unicast source reachable-via any** command.

## Unicast RPF in Strict Mode Feature Description

When the Unicast RPF in Strict Mode feature is enabled on an interface:

1. The router examines all IPv4 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** As an input function, the Unicast RPF in Strict Mode feature is applied only on the input interface of a Cisco 12000 series Internet router and is most effective when used on a customer-facing interface on a PE router.

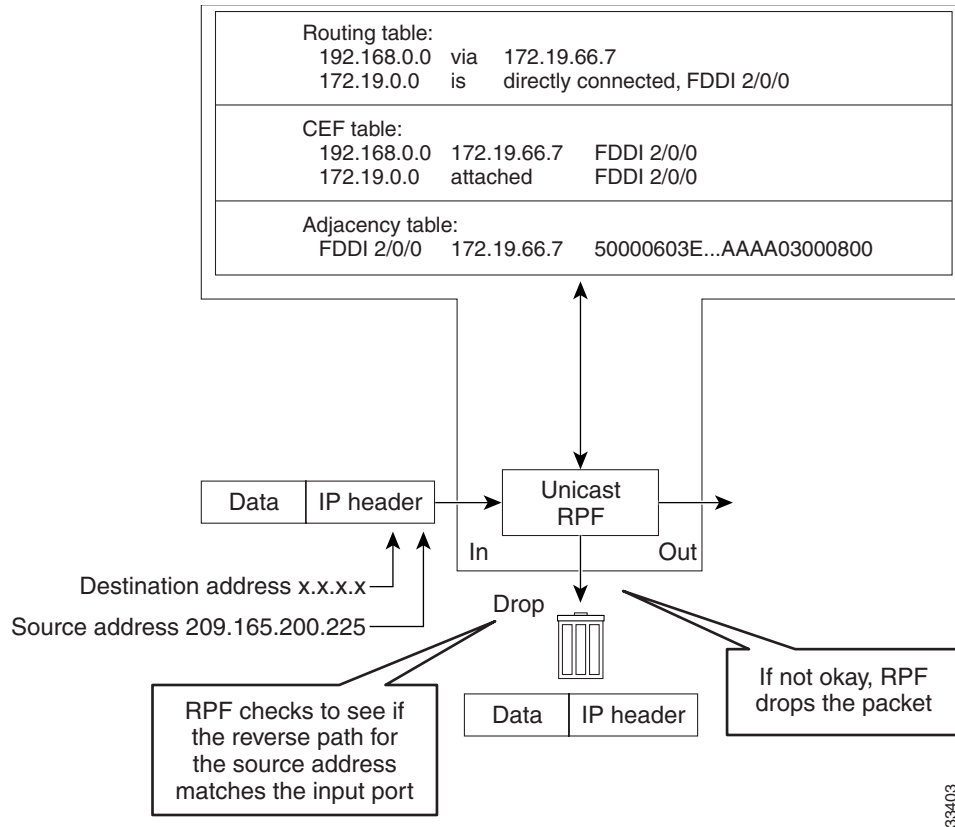
2. Unicast RPF in strict mode checks to see if any IPv4 packet received at an interface arrives on the best return path (return route) to the source of the packet by performing a reverse lookup in the CEF table:
  - If the IPv4 packet was received from one of the best reverse path routes, the packet 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 IPv4 packet is received at the interface on which you have configured Unicast RPF in strict mode, the following actions occur:
  - a. Unicast RPF in strict mode 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 IPv4 packet is forwarded.

**Figure 1** illustrates how Unicast RPF in strict mode and CEF work together to validate IP source addresses by verifying packet return paths. In the example, a customer sends a packet with a source address of 192.168.1.1 from interface FDDI 2/0/0. Unicast RPF checks the FIB to see if 192.168.1.1 has a path to FDDI 2/0/0:

- If a matching path exists, the packet is forwarded.
- If no matching path exists, the packet is dropped.



**Figure 2 Unicast RPF Dropping Packets That Fail Verification**



For information about Unicast RPF working with CEF to validate IPv4 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 in Strict Mode on the Cisco 12000 Router

On the Cisco 12000 series Internet router, the Unicast RPF in Strict Mode feature is implemented as follows:

- Only IPv4 traffic in the ingress direction (input interfaces) is supported.
- Only ISE/Engine 3 and Engine 5 line cards are supported. (ISE and Engine 5 line cards already support Unicast RPF in loose mode.)
- You can configure the Unicast RPF in Strict Mode feature on main interfaces, subinterfaces, and interfaces configured for the following features:
  - MPLS VPN (see the [Configuring MPLS Layer 3 VPNs](#) chapter in *Cisco IOS Multiprotocol Label Switching Configuration Guide*, Release 12.4)
  - Inter-Autonomous Systems for MPLS VPNs (see [Providing VPN Connectivity Across Multiple Autonomous Systems with MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS](#))
  - [Link Bundling on Cisco 12000 Series Internet Routers](#)

- Multilink interfaces (for Multilink Frame Relay and Multilink PPP, see [Cisco 12000 Series Router SIP and SPA Software Configuration Guide](#))
- [Inter-AS 10B Hybrid for MPLS VPN over IP Tunnels](#)
- Optional self-ping and allow-default functions are supported:
  - The self-ping option allows the Cisco 12000 series Internet router to ping its own interfaces and enable source IP-based black hole filtering to mitigate a DoS attack.
  - The allow-default flag sets the lookup operation to match the default route in the CEF routing table and use it to verify incoming IPv4 packets.
- All Layer 2 encapsulation and transport types are supported, including ATM AAL5, ATM cell relay, Ethernet (VLAN and port modes), Frame Relay, HDLC, and PPP over MPLS; for more information, refer to [Any Transport over MPLS](#).
- The Unicast RPF in Strict Mode feature supports up to eight interfaces on which per-packet load balancing is configured on the same line card. If you configure load balancing for a specified IP prefix on more than eight interfaces, Unicast RPF is performed in loose checking mode.
- IP prefix accounting and the Unicast RPF in Strict Mode feature are not supported together on the same line card.
- Multicast traffic is not supported. (Multicast traffic has its own Reverse Path Forwarding check).
- The CISCO-IP-URPF-MIB supports the display global and per-interface statistics for packets dropped by Unicast RPF.



---

**Note** The interface and subinterface dropped packet counters are not totally accurate. One out of sixty-seven IPv4 packets are punted to the CPU.

---

- Unicast RPF is not supported on an interface configured for generic route encapsulation (GRE) tunneling or Layer 2 tunneling, such as L2TPv3.
- Virtual Private Network routing and forwarding (VRF) tables are not supported in the path lookup.
- Unicast RPF does not support the access-list option as other platforms, which allows you to configure an ACL as an additional filter to verify incoming IPv4 packets.

Although the Unicast RPF in Strict Mode feature filters only IPv4 packets in IP or MPLS traffic, you can configure IOS software features that manage other traffic on the same interface, such as IP forwarding, MPLS features, Frame Relay switching, ATM switching, and Any Transport over ATM (AToM) connections. However, Unicast RPF filtering is only applied to incoming traffic on IP routing interfaces and not on packets processed by Frame Relay or ATM switching or transmitted over AToM pseudowire connections.

## Configuring Unicast RPF in Strict Mode on the Cisco 12000 Router

This section describes the procedures for configuring and verifying the Unicast RPF in Strict Mode feature to filter IPv4 packets on the Cisco 12000 series Internet router.

- [Configuring Unicast RPF in Strict Mode, page 10](#)
- [Verifying Unicast RPF in Strict Mode, page 11](#)

# Configuring Unicast RPF in Strict Mode

## Strict and Loose Checking Modes

Strict checking mode verifies that the source IPv4 address of an IPv4 packet exists in the routing table and that the path to the source IPv4 address is reachable through the input interface on which the packet was received. Loose mode also checks to see that a source IPv4 address exists in the routing table but permits any IPv4 packets that are reachable on a path through any interface on the router. Loose checking mode is already supported in ISE and Engine 5 line cards.

By using the **ip verify unicast source reachable-via** command, you can configure Unicast RPF in either strict checking or loose checking mode as follows:

- **ip verify unicast source reachable-via rx** configures Unicast RPF in strict mode.
- **ip verify unicast source reachable-via any** configures Unicast RPF in loose mode.



**Note** To allow the Cisco 12000 series Internet router to be compatible with Cisco IOS Release 12.3T and 12.2S software trains, the earlier version of the command, **ip verify unicast reverse-path**, is also supported. However, to enable Unicast RPF, we recommend that you use the current version: **ip verify unicast source reachable-via**.

## Prerequisites

The Unicast RPF in Strict Mode feature requires Cisco express forwarding (CEF) to function properly. However, on the Cisco 12000 series Internet router, CEF is enabled by default in distributed mode on hardware-forwarding line cards, such as ISE (Engine 3) and Engine 5.

## Restrictions

In Cisco IOS Release 12.0(33)S and later releases, the Unicast RPF in Strict Mode feature is supported on all ISE (Engine 3) and Engine 5 line cards in the Cisco 12000 series Internet router, except for the following ISE SPAs:

- 2-port clear channel T3/E3 ISE SPA (SPA-2XT3/E3)
- 4-port clear channel T3/E3 ISE SPA (SPA-4XT3/E3)
- 2-port channelized T3/E3 ISE SPA (SPA-2XCT3/DS0)
- 4-port channelized T3 to DS0 SPA (SPA-4XCT3/DS0)

For information about the ISE and Engine 5 service interface processors (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](#).

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/subslot/port*
4. **ip verify unicast source reachable-via rx** [**allow-default**] [**allow-self-ping**] [**list**]
5. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; <b>enable</b></p>	Enables privileged EXEC mode. If prompted, enter your password.
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# <b>configure terminal</b></p>	Enters global configuration mode.
Step 3	<pre>interface type slot/subslot/port</pre> <p><b>Example:</b> Router(config)# <b>interface gigabitethernet 2/0/0</b></p>	<p>Specifies an input interface on which you want to apply Unicast RPF and enters interface configuration mode.</p> <ul style="list-style-type: none"> <li>The <i>type</i> argument is the type of interface to be configured.</li> <li>The <i>slot/subslot/port</i> argument specifies the slot and port numbers of a SPA interface</li> </ul> <p><b>Note</b> 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	<pre>ip verify unicast source reachable-via rx [allow-default] [allow-self-ping] [list]</pre> <p><b>Example:</b> Router(config-if)# <b>ip verify unicast source reachable rx allow-default</b></p>	<p>Enables the Unicast RPF feature in strict checking mode to filter IPv4 packets.</p> <p>The <b>allow-default</b> keyword allows the lookup in the routing table to match the default route and use it for IPv4 packet verification.</p> <p>The <b>allow-self-ping</b> keyword allows a router to ping its own interface and is necessary to enable a denial-of-service (DoS) black hole. (In black holing, DoS packets are forwarded to and dropped from the null0 interface that is always up and can never forward or receive traffic.)</p> <p><b>Note</b> The optional <i>list</i> argument that allows you to specify an ACL and use an additional filter on incoming IPv4 packets is not supported on the Cisco 12000 router.</p>
Step 5	<pre>exit</pre> <p><b>Example:</b> Router(config-if)# <b>exit</b></p>	Exits interface configuration mode. Repeat Steps 3 and 4 for each interface on which you want to apply Unicast RPF in strict checking mode.

## Verifying Unicast RPF in Strict Mode

To verify that Unicast RPF in strict mode is operational, use the **show cef interface** command. The following example shows that Unicast RPF is enabled on interface serial2/0/0.

## SUMMARY STEPS

1. **enable**
2. **show cef interface** *type interface-number*
3. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> <b>enable</b>	Enables privileged EXEC mode. If prompted, enter your password.
Step 2	<b>show cef interface</b> <i>type number</i>  <b>Example:</b> Router# <b>show cef interface 2/0/0</b>	Displays the operational status of Cisco Express Forwarding (CEF) status on all interfaces or a specified interface, including information about whether Unicast RPF is enabled or not.
Step 3	<b>exit</b>  <b>Example:</b> Router(config-if)# <b>exit</b>	Exits privileged EXEC mode.

## Monitoring and Maintaining Unicast RPF

To display additional information about the Unicast RPF in Strict Mode feature configured on an interface, use the following **show** commands in privileged EXEC mode.

Command	Purpose
Router# <b>show ip interface</b> <i>type number</i>	Displays the total number of dropped packets on a specific interface.
Router# <b>show ip traffic</b>	Display global router statistics about the total number of dropped packets on all interfaces on the router. The Unicast RPF drop count is included in the IP statistics section.
Router(config-if)# <b>no ip verify unicast</b>	Disables Unicast RPF on an interface.

## Configuration Examples for Unicast RPF in Strict Mode on the Cisco 12000 Router

This section contains the following configuration examples for Unicast RPF in strict mode:

- [Configuring Unicast RPF in Strict Mode—Examples](#)
- [Verifying Unicast RPF in Strict Mode—Examples](#)

## Configuring Unicast RPF in Strict Mode—Examples

The following example shows how to configure the Unicast RPF in Strict Mode feature on an input Engine 5 Gigabit Ethernet interface in a Cisco 12000 series Internet router:

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

The next example shows how to disable the Unicast RPF in Strict Mode feature:

```
Router# configure terminal
Router(config)# interface gigabitethernet 3/1/1
Router(config-if)# no ip verify unicast
```

## Verifying Unicast RPF in Strict Mode—Examples

To verify that Unicast RPF 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 is enabled if the line starting with IPv4 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:
    IPv4 unicast RPF: acl=None, drop=0, sdrop=0
    IPv4: 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
  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 in Strict Mode feature.

### Related Documents

Related Topic	Document Title
Configuring Unicast RPF	<a href="#">“Configuring Unicast Reverse Path Forwarding”</a> 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	<i>Understanding Cisco Express Forwarding</i> “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	<i>Cisco IOS Security Command Reference, Release 12.3</i>
Configuration and troubleshooting procedures for the SPA interface processors (SIPs) and shared port adapters (SPAs) supported on a Cisco 12000 series Internet router.	<i>Cisco 12000 Series Router SIP and SPA Software Configuration Guide (IOS)</i>

### Standards

Standard	Title
No new or modified standards are supported by this feature.	—

### MIBs

MIB	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 at: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### RFCs

RFC	Title
RFC 1918	Address Allocation for Private Internets
RFC 2827	Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing

## 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, tools, and technical documentation. Registered Cisco.com users can log in from this page to access more content.	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Command Reference

This section documents modified commands only:


- **ip verify unicast source reachable-via**

## ip verify unicast source reachable-via

To enable Unicast Reverse Path Forwarding (Unicast RPF), use the **ip verify unicast source reachable-via** command in interface configuration mode. To disable Unicast RPF, use the **no** form of this command.

```
ip verify unicast source reachable-via {rx | any} [allow-default] [allow-self-ping] [list] [12-src]
[phys-if]
```

```
no ip verify unicast source reachable-via
```

Syntax Description		
<b>rx</b>	Examines incoming packets to determine whether the source address is in the Forwarding Information Base (FIB) and permits the packet only if the source is reachable through the interface on which the packet was received (sometimes referred to as strict mode).	
<b>any</b>	Examines incoming packets to determine whether the source address is in the FIB and permits the packet if the source is reachable through any interface (sometimes referred to as loose mode).	
<b>allow-default</b>	(Optional) Allows the use of the default route for RPF verification.	
<b>allow-self-ping</b>	(Optional) Allows a router to ping its own interface or interfaces.	
		
	<b>Caution</b>	Use caution when enabling the <b>allow-self-ping</b> keyword. This keyword opens a denial-of-service (DoS) hole.
<i>list</i>	(Optional) Specifies a numbered access control list (ACL) in the following ranges:	<ul style="list-style-type: none"> <li>• 1 to 99 (IP standard access list)</li> <li>• 100 to 199 (IP extended access list)</li> <li>• 1300 to 1999 (IP standard access list, expanded range)</li> <li>• 2000 to 2699 (IP extended access list, expanded range)</li> </ul>
<b>12-src</b>	(Optional) Enables source IPv4 and source MAC address binding.	
<b>phys-if</b>	(Optional) Enables physical input interface verification.	

**Command Default** Unicast RPF is disabled.  
Source IPv4 and source MAC address binding is disabled

**Command Modes** Interface configuration (config-if)

**Command History**

Release	Modification
11.1(CC), 12.0	This command was introduced. This command was not included in Cisco IOS Release 11.2 or 11.3.
12.1(2)T	Added access control list (ACL) support using the <i>list</i> argument. Added per-interface statistics on dropped or suppressed packets.
12.0(15)S	This command replaced the <b>ip verify unicast reverse-path</b> command, and the following keywords were added: <b>allow-default</b> , <b>allow-self-ping</b> , <b>rx</b> , and <b>any</b> .
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC	The <b>l2-src</b> keyword was added to support the source IPv4 and source MAC address binding feature on Cisco 7600 series routers.  The <b>phys-if</b> keyword was added to support physical input interface verification. Together, both keywords support the Unicast RPF IP and MAC Address Spoof Prevention feature.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

**Usage Guidelines**

Use the **ip verify unicast source reachable-via** interface 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 DoS attacks based on source IP address spoofing.

To use Unicast RPF, enable Cisco Express Forwarding or distributed Cisco Express Forwarding in the router. There is no need to configure the input interface for Cisco Express Forwarding. As long as Cisco Express Forwarding is running on the router, individual interfaces can be configured with other switching modes.

**Note**

It is important for Cisco Express Forwarding to be configured globally on the router. Unicast RPF does not work without Cisco Express Forwarding.

**Note**

Unicast RPF is an input function and is applied on the interface of a router only in the ingress direction.

When Unicast RPF is enabled on an interface, the router examines all packets that are received on that interface. The router checks to make sure that the source address appears in the FIB. If the **rx** keyword is selected, the source address must match the interface on which the packet was received. If the **any** keyword is selected, the source address must be present only in the FIB. This ability to “look backwards” is available only when Cisco Express Forwarding is enabled on the router because the lookup relies on the presence of the FIB. Cisco Express Forwarding generates the FIB as part of its operation.

**Note**

If the source address of an incoming packet is resolved to a null adjacency, the packet will be dropped. The null interface is treated as an invalid interface by the new form of the Unicast RPF command. The older form of the command syntax did not exhibit this behavior.

Unicast RPF checks to determine whether any packet that is received at a router interface arrives on one of the best return paths 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, 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 **ip verify unicast source reachable-via** 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 that are used by the **ip verify unicast source reachable-via** command. Log information can be used to gather information about the attack, such as source address, time, and so on.

### Strict Mode RPF

If the source address is in the FIB and reachable only through the interface on which the packet was received, the packet is passed. The syntax for this method is **ip verify unicast source reachable-via rx**.

### Exists-Only (or Loose Mode) RPF

If the source address is in the FIB and reachable through any interface on the router, the packet is passed. The syntax for this method is **ip verify unicast source reachable-via any**.

Because this Unicast RPF option passes packets regardless of which interface the packet enters, it is often used on Internet service provider (ISP) routers that are “peered” with other ISP routers (where asymmetrical routing typically occurs). Packets using source addresses that have not been allocated on the Internet, which are often used for spoofed source addresses, are dropped by this Unicast RPF option. All other packets that have an entry in the FIB are passed.

### allow-default

Normally, sources found in the FIB but only by way of the default route will be dropped. Specifying the **allow-default** keyword option will override this behavior. You must specify the **allow-default** keyword in the command to permit Unicast RPF to successfully match on prefixes that are known through the default route to pass these packets.

### allow-self-ping

This keyword allows the router to ping its own interface or interfaces. By default, when Unicast RPF is enabled, packets that are generated by the router and destined to the router are dropped, thereby, making certain troubleshooting and management tasks difficult to accomplish. Issue the **allow-self-ping** keyword to enable self-pinging.



### Caution

Caution should be used when enabling the **allow-self-ping** keyword because this option opens a potential DoS hole.

### Using RPF in Your Network

Use Unicast RPF strict mode on interfaces where only one path allows packets from valid source networks (networks contained in the FIB). Also, use Unicast RPF strict mode when a router has multiple paths to a given network, as long as the valid networks are switched through the incoming interfaces. Packets for invalid networks will be dropped. For example, routers at the edge of the network of an ISP

are likely to have symmetrical reverse paths. Unicast RPF strict mode is applicable in certain multihomed situations, provided that optional Border Gateway Protocol (BGP) attributes, such as weight and local preference, are used to achieve symmetric routing.

**Note**

With 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) and as long as the route is in the FIB. Unicast RPF also functions where Enhanced Internet Gateway Routing Protocol (EIGRP) variants are being used and unequal candidate paths back to the source IP address exist.

Use Unicast RPF loose mode on interfaces where asymmetric paths allow packets from valid source networks (networks contained in the FIB). 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.

**IP and MAC Address Spoof Prevention on Cisco 7600 Series Routers**

In Release 12.2(33)SRC and later, use the **l2-src** keyword to enable source IPv4 and source MAC address binding and the **phys-if** keyword to verify the source IP input interface. To disable source IPv4 and source MAC address binding, use the **no** form of the **ip verify unicast source reachable-via** command. The **phys-if** keyword can be used on Gigabit virtual interfaces (GVI) interfaces; the **l2-src** keyword can be used on GVI and Ethernet-like interfaces.

If an inbound packet fails either of these security checks, it will be dropped and the Unicast RPF dropped-packet counter will be incremented. The only exception occurs if a numbered access control list has been specified as part of the Unicast RPF command in strict mode, and the ACL permits the packet. In this case the packet will be forwarded and the Unicast RPF suppressed-drops counter will be incremented.

**Note**

Neither the **l2-src** nor the **phys-if** keywords can be used with the loose uRPF command, **ip verify unicast source reachable-via any** command.

Possible keyword combinations for Unicast PRF include the following:

```
allow-default
allow-self-ping
l2-src
phys-if
<ACL-number>
allow-default allow-self-ping
allow-default l2-src
allow-default phys-if
allow-default <ACL-number>
allow-self-ping l2-src
allow-self-ping phys-if
allow-self-ping <ACL-number>
l2-src phys-if
l2-src <ACL-number>
phys-if <ACL-number>
allow-default allow-self-ping l2-src
allow-default allow-self-ping phys-if
allow-default allow-self-ping <ACL-number>
allow-default l2-src phys-if
allow-default l2-src <ACL-number>
allow-default phys-if <ACL-number>
allow-self-ping l2-src phys-if
allow-self-ping l2-src <ACL-number>
```

```

allow-self-ping phys-if <ACL-number>
l2-src phys-if <ACL-number>
allow-default allow-self-ping l2-src phys-if
allow-default allow-self-ping l2-src <ACL-number>
allow-default allow-self-ping phys-if <ACL-number>
allow-default l2-src phys-if <ACL-number>
allow-self-ping l2-src phys-if <ACL-number>
allow-default allow-self-ping l2-src phys-if <ACL-number>

```

## Examples

### Single-homed ISP Connection with Unicast RPF

The following example uses a very simple single-homed ISP connection to demonstrate the concept of Unicast RPF. In this example, an ISP peering router is connected through a single serial interface to one upstream ISP. Hence, traffic flows into and out of the ISP will be symmetric. Because traffic flows will be symmetric, a Unicast RPF strict-mode deployment can be configured.

```

ip cef
! or "ip cef distributed" for Route Switch Processor+Versatile Interface Processor-
(RSP+VIP-) based routers.
!
interface Serial5/0/0
description - link to upstream ISP (single-homed)
ip address 192.168.200.225 255.255.255.252
no ip redirects
no ip directed-broadcasts
no ip proxy-arp
ip verify unicast source reachable-via

```

### ACLs and Logging with Unicast RPF

The following example demonstrates the use of ACLs and logging with Unicast RPF. In this example, extended ACL 197 provides entries that deny or permit network traffic for specific address ranges. Unicast RPF is configured on interface Ethernet 0 to check packets arriving at that interface.

For example, packets with a source address of 192.168.201.10 arriving at interface Ethernet 0 are dropped because of the deny statement in ACL 197. 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 192.168.201.100 arriving at interface Ethernet 0 are forwarded because of the permit statement in ACL 197. ACL information about dropped or suppressed packets is logged (the logging option is turned on for the ACL entry) to the log server.

```

ip cef distributed
!
int eth0/1/1
ip address 192.168.200.1 255.255.255.0
ip verify unicast source reachable-via rx 197
!
int eth0/1/2
ip address 192.168.201.1 255.255.255.0
!
access-list 197 deny ip 192.168.201.0 0.0.0.63 any log-input
access-list 197 permit ip 192.168.201.64 0.0.0.63 any log-input
access-list 197 deny ip 192.168.201.128 0.0.0.63 any log-input
access-list 197 permit ip 192.168.201.192 0.0.0.63 any log-input
access-list 197 deny ip host 0.0.0.0 any log-input
access-list 197 deny ip 172.16.0.0 0.255.255.255 any log-input
access-list 197 deny ip 10.0.0.0 0.255.255.255 any log-input
access-list 197 deny ip 172.16.0.0 0.15.255.255 any log-input
access-list 197 deny ip 192.168.0.0 0.0.255.255 any log-input

```

### MAC Address Binding on Cisco 7600 Series Routers

The following example enables source IPv4 and source MAC address binding on VLAN 10.

```
Router# configure terminal  
Router(config)# interface VLAN 10  
Router(config-if)# ip address 10.0.0.1 255.255.255.0  
Router(config-if)# ip verify unicast source reachable-via rx 12-src
```

#### Related Commands

Command	Description
<b>ip cef</b>	Enables Cisco Express Forwarding on the route processor card.

# Feature Information for Unicast RPF in Strict Mode on the Cisco 12000 Router

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 feature in a Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Unicast RPF in Strict Mode on the Cisco 12000 Router Feature Information

Feature Name	Cisco IOS Release	Feature Information
Unicast RPF in Strict Mode on the Cisco 12000 Series Internet Router	12.0(33)S	<p>The Unicast RPF in Strict Mode on the Cisco 12000 router provides enhanced filtering capacity on incoming IPv4 traffic and greater protection from DoS attacks.</p> <p>In Cisco IOS Release 12.0(33)S, this feature was introduced on the Cisco 12000 router.</p> <p>The following commands were introduced or modified by this feature: <b>ip verify unicast reachable-via</b></p>

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0805R)

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

coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.

