



# Unicast Reverse Path Forwarding

---

This feature module describes the Unicast Reverse Path Forwarding (RPF) feature, which helps to mitigate problems caused by malformed or forged IP source addresses passing through a router. This document includes information on the benefits of the new feature, supported platforms, related documents, and so on.

This document includes the following sections:

- Feature Overview, page 1
- Supported Platforms, page 11
- Supported Standards, MIBs, and RFCs, page 11
- Prerequisites, page 12
- Configuration Tasks, page 12
- Monitoring and Maintaining Unicast RPF, page 14
- Configuration Examples, page 15
- Command Reference, page 17

## Feature Overview

The Unicast RPF feature helps to mitigate problems that are caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address. For example, a number of common types of denial-of-service (DoS) attacks, including Smurf and Tribe Flood Network (TFN), can take advantage of forged or rapidly changing source IP addresses to allow attackers to thwart efforts to locate or filter the attacks. For Internet service providers (ISPs) that provide public access, Unicast RPF deflects such attacks by forwarding only packets that have source addresses that are valid and consistent with the IP routing table. This action protects the network of the ISP, its customer, and the rest of the Internet.

## How It Works

When Unicast RPF is enabled on an interface, the router examines all 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 “look backwards” ability 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 is an input function and is applied only on the input interface of a router at the upstream end of a connection.

---

Unicast RPF checks to see if any packet received at a router interface arrives on one of the best return paths to the source of the packet. Unicast RPF does this by doing a reverse lookup in the CEF table. If the packet was received from one of the best reverse path routes, the packet is forwarded as normal. If there is no reverse path route on the same interface from which the packet was received, it might mean that the source address was modified or forged. If Unicast RPF does not find a reverse path for the packet, the packet is dropped.

**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 EIGRP variants are being used and unequal candidate paths back to the source IP address exist.

---

When a packet is received at the interface where Unicast RPF and access control lists (ACLs) have been configured, the following actions occur:

1. Input ACLs configured on the inbound interface are checked.
2. Unicast RPF checks to see if the packet has arrived on one of the best return paths to the source, which it does by doing a reverse lookup in the FIB table.
3. CEF table (FIB) lookup is carried out for packet forwarding.
4. Output ACLs are checked on the outbound interface.
5. The packet is forwarded.

Figure 1 illustrates how Unicast RPF and CEF work together to validate IP source addresses by verifying packet return paths. In this example, a customer has sent a packet having 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 there is a matching path, the packet is forwarded. If there is no matching path, the packet is dropped.

**Figure 1 Unicast RPF Validating IP Source Addresses**

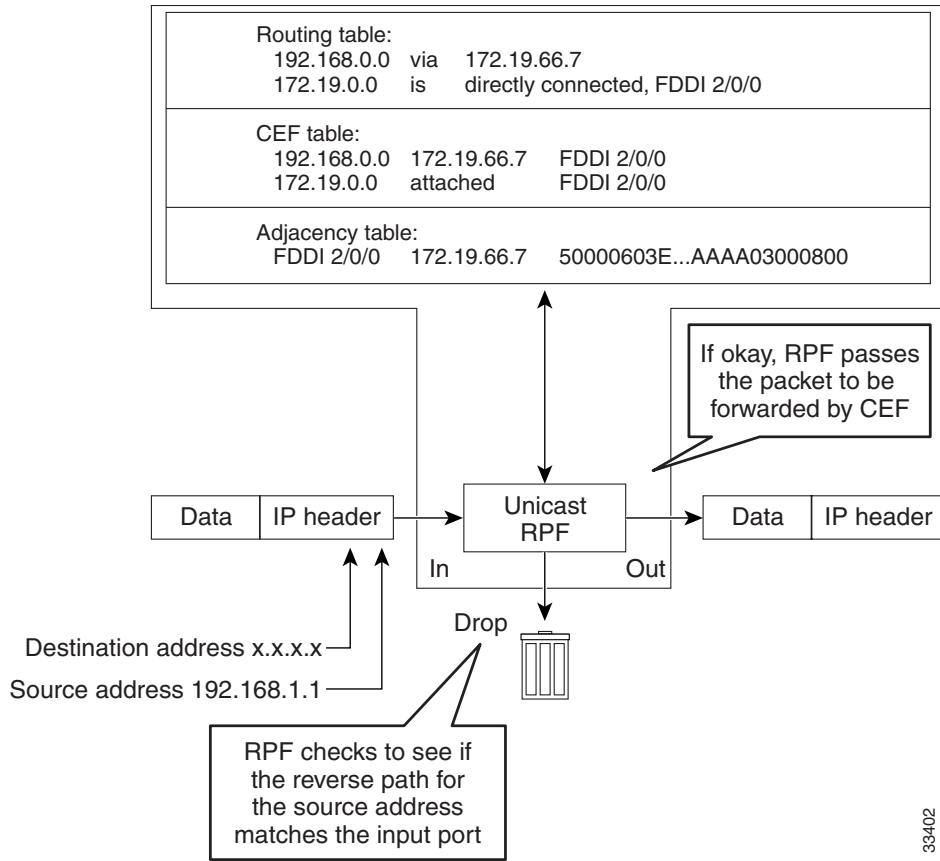
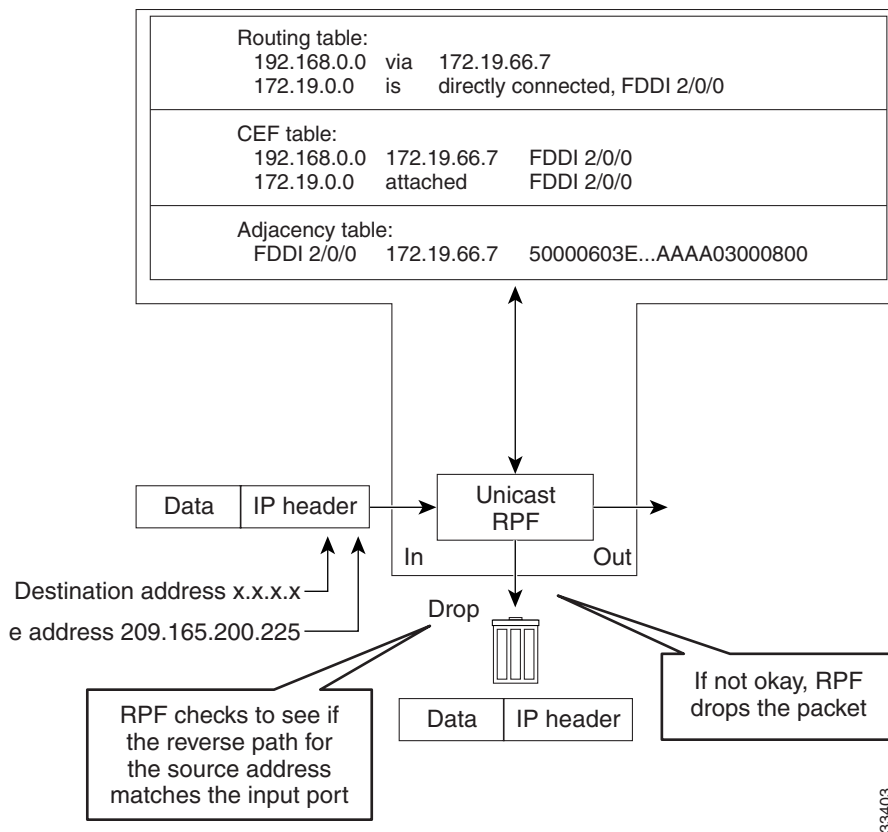


Figure 2 illustrates how Unicast RPF drops packets that fail validation. In this example, a customer has sent a packet having a source address of 209.165.200.225, which is received at interface FDDI 2/0/0. Unicast RPF checks the FIB to see if 209.165.200.225 has a return path to FDDI 2/0/0. If there is a matching path, the packet is forwarded. In this case, there is no reverse entry in the routing table that routes the customer packet back to source address 209.165.200.225 on interface FDDI 2/0/0, and so the packet is dropped.

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



## Implementing Unicast RPF

Unicast RPF has several key implementation principles:

- The packet must be received at an interface that is one of the best return paths 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.
- IP source addresses at the receiving interface must match the routing entry for the interface.
- Unicast RPF 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 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.



### Caution

Using optional BGP attributes such as weight, local preference, and so on, the best path back to the source address can be modified, which would affect the operation of Unicast RPF.

This section provides information about the implementation of Unicast RPF:

- Security Policy and Unicast RPF
- Where to Use Unicast RPF
- Routing Tables Requirements
- Where Not to Use Unicast RPF
- Unicast RPF with BOOTP and DHCP

## Security Policy and Unicast RPF

Consider the following points in determining your policy for deploying Unicast RPF:

- Unicast RPF must be applied at the interface downstream from the larger portion of the network, preferably at the edges of your network.
- The further downstream you apply Unicast RPF, the finer the granularity you have in mitigating address spoofing and in identifying the sources of spoofed addresses. For example, applying Unicast RPF on an aggregation router helps mitigate attacks from many downstream networks or clients and is simple to administer, but it does not help identify the source of the attack. Applying Unicast RPF at the network access server helps limit the scope of the attack and trace the source of the attack; however, deploying Unicast RPF across many sites does add to the administration cost of operating the network.
- The more entities that deploy Unicast RPF across Internet, intranet, and extranet resources, the better the chances of mitigating large-scale network disruptions throughout the Internet community, and the better the chances of tracing the source of an attack.
- Unicast RPF will not inspect IP packets encapsulated in tunnels, such as GRE, LT2P, or PPTP. Unicast RPF must be configured at a home gateway so that Unicast RPF processes network traffic only after the tunneling and encryption layers have been stripped off the packets.

## Where to Use Unicast RPF

Unicast RPF can be used in any “single-homed” environment where there is essentially only one access point out of the network; that is, one upstream connection. Networks having one access point offer the best example of symmetric routing, which means that the interface where a packet enters the network is also the best return path to the source of the IP packet. Unicast RPF is best used at the network perimeter for Internet, intranet, or extranet environments, or in ISP environments for customer network terminations.

The following sections provide a look at implementing Unicast RPF in two network environments:

- Enterprise Networks with a Single Connection to an ISP
- Network Access Server Application (Applying Unicast RPF in PSTN/ISDN PoP Aggregation Routers)

### Enterprise Networks with a Single Connection to an ISP

In enterprise networks, one objective of using Unicast RPF for filtering traffic at the input interface (a process called *ingress filtering*) is for protection from malformed packets arriving from the Internet. Traditionally, local networks that have one connection to the Internet would use ACLs at the receiving interface to prevent spoofed packets from the Internet from entering their local network.

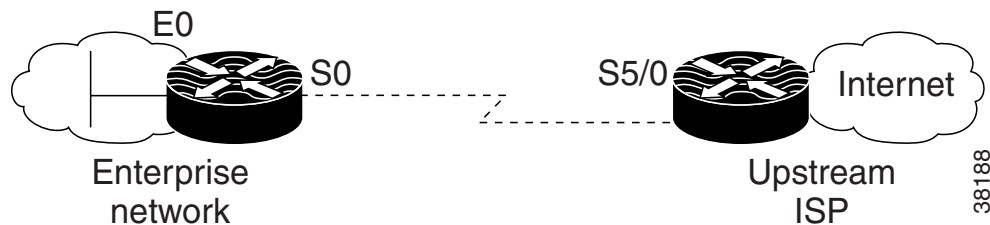
ACLs work well for many single-homed customers; however, there are trade-offs when ACLs are used as ingress filters, including two commonly referenced limitations:

- Packet per second (PPS) performance at very high packet rates
- Maintenance of the ACL (whenever there are new addresses added to the network)

Unicast RPF is one tool that addresses both of these limitations. With Unicast RPF, ingress filtering is done at CEF PPS rates. This processing speed makes a difference when the link is more than 1 Mbps. Additionally, since Unicast RPF uses the FIB, no ACL maintenance is necessary, and thus the administration overhead of traditional ACLs is reduced. The following figure and example demonstrate how this is configured.

Figure 3 illustrates an enterprise network that has a single link to an upstream ISP. In this example, Unicast RPF is applied at interface S0 on the enterprise router for protection from malformed packets arriving from the Internet. Unicast RPF is also applied at interface S5/0 on the ISP router for protection from malformed packets arriving from the enterprise network.

**Figure 3 Enterprise Network Using Unicast RPF for Ingress Filtering**



Using Figure 3, a typical configuration (assuming that CEF is turned on) on the ISP router would be as follows:

```
ip cef
interface loopback 0
  description Loopback interface on Gateway Router 2
  ip address 192.168.3.1 255.255.255.255
  no ip redirects
  no ip directed-broadcast
  no ip proxy-arp
interface Serial 5/0
  description 128K HDLC link to ExampleCorp WT50314E R5-0
  bandwidth 128
  ip unnumbered loopback 0
  ip verify unicast reverse-path
  no ip redirects
  no ip directed-broadcast
  no ip proxy-arp
ip route 192.168.10.0 255.255.252.0 Serial 5/0
```

The gateway router configuration of the enterprise network (assuming that CEF is turned on) would look similar to the following:

```
ip cef
interface Ethernet 0
  description ExampleCorp LAN
  ip address 192.168.10.1 255.255.252.0
  no ip redirects
  no ip directed-broadcast
  no ip proxy-arp
interface Serial 0
  description 128K HDLC link to ExampleCorp Internet Inc WT50314E C0
  bandwidth 128
  ip unnumbered ethernet 0
  ip verify unicast reverse-path
  no ip redirects
  no ip directed-broadcast
  no ip proxy-arp
ip route 0.0.0.0 0.0.0.0 Serial 0
```

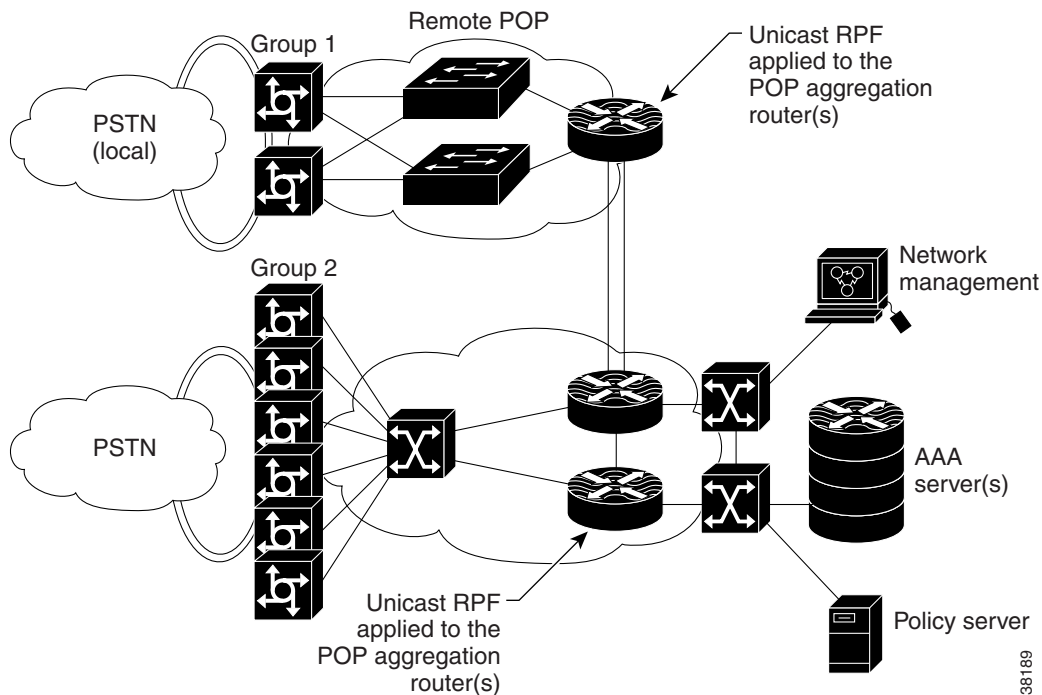
Notice that Unicast RPF works with a single default route. There are no additional routes or routing protocols. Network 192.168.10.0/22 is a connected network. Hence, packets coming from the Internet with a source address in the range 192.168.10.0/22 will be dropped by Unicast RPF.

### Network Access Server Application (Applying Unicast RPF in PSTN/ISDN PoP Aggregation Routers)

Aggregation routers are ideal places to use Unicast RPF with single-homed clients. Unicast RPF works equally well 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 IP addresses. As long as the network access server supports CEF, Unicast RPF will work. 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) would be enough for Unicast RPF to do its job.

Figure 4 illustrates the application of Unicast RPF to the aggregation and access routers for an Internet service provider (ISP) point-of-presence (POP), with the ISP routers providing dialup customer connections. In this example, Unicast RPF is applied upstream from the customer dialup connection router on the receiving (input) interfaces of the ISP aggregation routers.

**Figure 4 Unicast RPF Applied to PSTN/ISDN Customer Connections**



## Routing Tables Requirements

To work correctly, Unicast RPF needs proper information in the CEF tables. This requirement does not mean that the router must have the entire Internet routing table. The amount of routing information needed in the CEF tables depends on where Unicast RPF is configured and what 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 would be configured on the customer interfaces—hence the requirement for minimal routing information. In another scenario, a single-homed ISP could place Unicast RPF on the gateway link to the Internet. The full Internet routing table would be required. Requiring the full routing table would help protect the ISP from external DoS attacks that use addresses that are not in the Internet routing table.

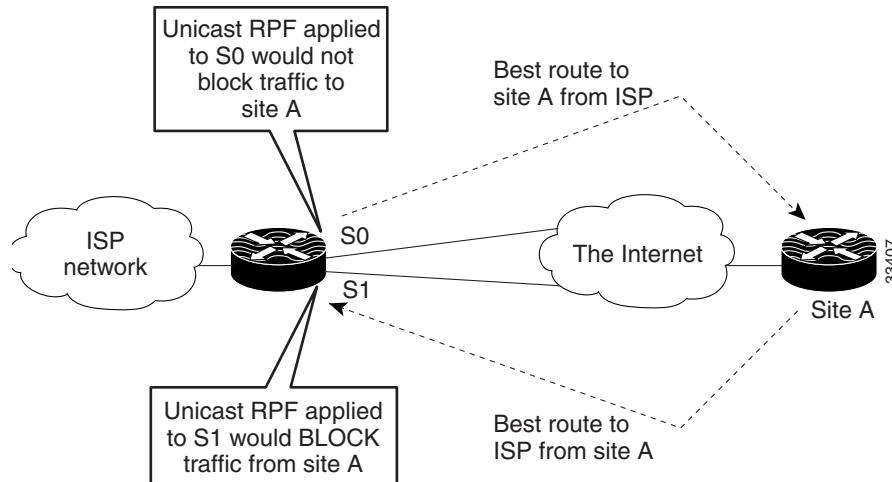
## Where Not to Use Unicast RPF

Unicast RPF should not be used on interfaces that are internal to the network. Internal interfaces are likely to have routing asymmetry (see Figure 5), meaning multiple routes to the source of a packet. Unicast RPF should be applied only where there is natural or configured symmetry. As long as administrators carefully plan which interfaces they activate Unicast RPF on, 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. 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.

Figure 5 illustrates how Unicast RPF can block legitimate traffic in an asymmetrical routing environment.

**Figure 5 Unicast RPF Blocking Traffic in an Asymmetrical Routing Environment**



## Unicast RPF with BOOTP and DHCP

Unicast RPF will allow packets with 0.0.0.0 source and 255.255.255.255 destination to pass so that Bootstrap Protocol (BOOTP) and Dynamic Host Configuration Protocol (DHCP) functions work properly.

## Benefits

### Adaptation to Changes in Routing Tables

Unicast RPF's advantage when used for IP address spoofing mitigation is that it dynamically adapts to changes in the dynamic routing tables, including static routes.

### Performance

Unicast RPF has minimal CPU overhead and operates at a rate that is a smaller percentage lower than CEF/optimum/fast switching rates. Unicast RPF has far lower impact on performance as an antispoofing tool than the access-list approach.

### Less Maintenance

Unicast RPF requires less operational maintenance than traditional anti-spoofing approaches that use IP access or extended-access lists. Unicast RPF can be added to the customer's default configuration on the ISP's router (this works only if the router has CEF configured). The following configuration template is available for router interfaces:

```
description [enter description of interface]
no ip redirect
no ip direct broadcast
no ip proxy-arp
ip verify unicast reverse-path
bandwidth [bandwidth in kbps]
```

### Load Sharing

Unicast RPF is compatible with per-packet and per-destination load sharing using CEF.

### Mitigation of Accidental Leaks of Private (RFC1918) Addresses

Unicast RPF can help mitigate accidental leaks of private (RFC1918) addresses through routers to public networks. If default routes to the Internet exist, even private addresses that should be routed to an internal router for network address translation (NAT) might accidentally be routed along the default route path to the Internet. For example, if you add a new subnet based on RFC1918 addresses but do not add it to your NAT list, it might be routed to the Internet as if it were a valid source. Most ISP routers check malformed packets and drop them; however, this checking process wastes bandwidth and resources of the ISP.

### Source Address Verification

Unicast RPF ensures that the source address of a packet is from a route advertised by another router on the specific interface. Validating that the IP source address of the packet was from the receiving interface helps to mitigate IP source address spoofing at the receiving interface. Although validating the source address does not mean that a valid address could not be the source of an attack, it does allow administrators to trace the origin of an attack. If an attack occurs, administrators can quickly shut down the offending interface. Additionally, wide implementation of Unicast RPF throughout the network or Internet would aid in tracing the source of denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks.

## Restrictions

There are some basic restrictions to applying Unicast RPF to multihomed clients:

- Clients should not be multihomed to the same router because multihoming defeats the purpose of building a redundant service for the client.
- Customers must ensure that the packets flowing up the link (out to the Internet) match the route advertised out the link. Otherwise, Unicast RPF filters those packets as malformed packets.
- Unicast RPF is available only for platform images that support CEF. Unicast RPF is supported in Cisco IOS Releases 11.1(17)CC and 12.0 and later. It is not available in Cisco IOS Releases 11.2 or 11.3.

## Related Features and Technologies

For more information about Unicast RPF related features and technologies, review the following:

- Unicast RPF requires Cisco express forwarding (CEF) to function properly on the router. For more information about CEF, refer to the “Cisco Express Forwarding” feature module in Cisco IOS Release 11.1(17)CC.
- Unicast RPF can be effective at mitigating spoofing attacks when combined with a policy of *ingress* and *egress* filtering using Cisco IOS access control lists (ACLs). For more information on network filtering, refer to RFC 2267 and to the *Cisco IOS Network Protocols Configuration Guide, Part 1*.
  - Ingress filtering applies filters to traffic received at a network interface from either internal or external networks. With ingress filtering, packets that arrive from other networks or the Internet and that have a source address that matches a local network, private, or broadcast address are dropped. In ISP environments, for example, ingress filtering can apply to traffic received at the router from either the client (customer) or the Internet.

- Egress filtering applies filters to traffic exiting a network interface (the sending interface). By filtering packets on routers that connect your network to the Internet or to other networks, you can permit only packets with valid source IP addresses to leave your network.

## Related Documents

- *Network Protocols Configuration Guide, Part 1*, Cisco IOS Release 11.1.
- RFC 2267, *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*

## Supported Platforms

- Cisco 7000 series with Route Switch Processor (RSP)
- Cisco 7200 series
- Cisco 7500 series
- Cisco 12000 series

The Unicast RPF feature runs all platforms that run Cisco IOS Release 11.1(17)CC and that support Cisco Express Forwarding (CEF).

## Supported Standards, MIBs, and RFCs

### Standards

None applicable.

### MIBs

None.

For descriptions of supported MIBs and how to use MIBs, see the Cisco MIB web site on CCO at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

### RFCs

RFC 2267, *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*

## Prerequisites

Prior to configuring Unicast RPF, configure ACLs:

- Configure ACLs to mitigate transmission of invalid IP addresses (perform egress filtering). Permit only valid source addresses to leave your network and get onto the Internet. Prevent all other source addresses from leaving your network for the Internet.
- Configure ACLs to prevent (deny) reception of invalid IP addresses (perform ingress filtering). Invalid addresses include the following types:
  - Reserved addresses
  - Loopback addresses
  - Private addresses
  - Broadcast addresses
  - Source addresses that match any addresses on the protected network (prevents spoofing)

## Configuration Tasks

The following sections describe the configuration tasks for Unicast RPF. Each task in the list is identified as either optional or required.

- Configuring Unicast RPF (Required)
- Verifying Unicast RPF (Optional)

See the end of this chapter for the section “Configuration Examples.”

## Configuring Unicast RPF

To use Unicast RPF, you must configure the router for CEF switching or CEF distributed switching. There is no need to configure the input interface for CEF switching because Unicast RPF has been implemented as a search through the 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 IP packets received by the router. It is very important that CEF be turned on globally in the router—Unicast RPF will not work without CEF.

To configure Unicast RPF, use the following commands beginning in global configuration mode:

	Command	Purpose
<b>Step 1</b>	<pre>Router(config)# ip cef or Router(config)# ip cef distributed</pre>	<p>Enables CEF or distributed CEF on the router. Distributed CEF is required for routers that use a Route/Switch Processor (RSP) and Versatile Interface Processor (VIP), which includes Unicast RPF.</p> <p>You might want to disable CEF or distributed CEF (dCEF) on a particular interface if that interface is configured with a feature that CEF or dCEF does not support. In this case, you would enable CEF globally, but disable CEF on a specific interface using the <b>no ip route-cache cef interface</b> command, which enables all but that specific interface to use express forwarding. If you have disabled CEF or dCEF operation on an interface and want to reenable it, you can do so by using the <b>ip route-cache cef</b> command in interface configuration mode.</p>
<b>Step 2</b>	<pre>Router(config)# interface type</pre>	<p>Selects the input interface on which you want to apply Unicast RPF. This is the receiving interface, which allows Unicast RPF to verify the best return path before forwarding the packet on to the next destination.</p> <p>The interface type is specific to your router and the types of interface cards installed on the router. To display a list of available interface types, enter the interface <b>?</b> command.</p>
<b>Step 3</b>	<pre>Router(config-if)# ip verify unicast reverse-path</pre>	Enables Unicast RPF on the interface.
<b>Step 4</b>	<pre>Router(config-if)# exit</pre>	Exits interface configuration mode. Repeat Steps 2 and 3 for each interface on which you want to apply Unicast RPF.

## Verifying Unicast RPF

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

```
Router-3# show cef interface serial 2/0/0
Serial2/0/0 is up (if_number 8)
  Internet address is 192.168.10.2/30
  ICMP redirects are never sent
  Per packet loadbalancing is disabled
  IP unicast RPF check is enabled
  Inbound access list is not set
  Outbound access list is not set
  Interface is marked as point to point interface
  Packets switched to this interface on linecard are dropped to next slow path
  Hardware idb is Serial2/0/0
  Fast switching type 4, interface type 6
  IP Distributed CEF switching enabled
  IP LES Feature Fast switching turbo vector
  IP Feature CEF switching turbo vector
  Input fast flags 0x40, Output fast flags 0x0, ifindex 7(7)
  Slot 2 Slot unit 0 VC -1
  Transmit limit accumulator 0x48001A02 (0x48001A02)
  IP MTU 1500
```

## Troubleshooting Tips

Failure to disable Unicast RPF before disabling CEF can break IP frame forwarding on the router. If you want to disable CEF on the router, you must first disable Unicast RPF. To disable Unicast RPF, see the section “Monitoring and Maintaining Unicast RPF.”

## Monitoring and Maintaining Unicast RPF

To monitor Unicast RPF activity, use the following commands in EXEC mode:

Command	Purpose
Router# show ip traffic	Displays statistics about IP traffic.
Router(config-if)# no ip verify unicast reverse-path	Disables Unicast RPF at the interface.



### Caution

To disable CEF, you must first disable Unicast RPF. Failure to disable Unicast RPF before disabling CEF can break IP frame forwarding on the router. If you want to disable CEF on the router, you must first disable Unicast RPF.

A counter is maintained to count the number of packets discarded because of Unicast RPF. The value of the counter is displayed as part of the output from the **show ip traffic** command. The value of the counter is the total of dropped packets for all router interfaces. The Unicast RPF drop count is included in the IP statistics section.

```
Router# show ip traffic
IP statistics:
  Rcvd: 1471590 total, 887368 local destination
        0 format errors, 0 checksum errors, 301274 bad hop count
        0 unknown protocol, 0 not a gateway
        0 security failures, 0 bad options, 0 with options
  Opts: 0 end, 0 nop, 0 basic security, 0 loose source route
        0 timestamp, 0 extended security, 0 record route
        0 stream ID, 0 strict source route, 0 alert, 0 other
  Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
        0 fragmented, 0 couldn't fragment
  Bcast: 205233 received, 0 sent
  Mcast: 463292 received, 462118 sent
  Sent: 990158 generated, 282938 forwarded
  Drop: 3 encapsulation failed, 0 unresolved, 0 no adjacency
        0 no route, 0 unicast RPF, 0 forced drop
```

If the drop counter (router drop count) is not zero, a value indicates that packets were dropped by Unicast RPF. Dropped packets can mean two things:

- Unicast RPF is dropping packets that have a bad source address (normal operation).
- Unicast RPF is dropping legitimate packets because the route is misconfigured to use Unicast RPF in environments where asymmetric routing exists; that is, where multiple paths can exist as the best return path for a source address.

## Configuration Examples

This section provides the following configuration examples:

- Enabling Unicast RPF on a Serial Interface Example
- Enabling Unicast RPF with Inbound and Outbound Filters Example

### Enabling Unicast RPF on a Serial Interface Example

The following commands enable Unicast RPF on a serial interface.

```
ip cef
! or "ip cef distributed" for RSP+VIP based routers
!
interface serial 5/0/0
 ip verify unicast reverse-path
```

### Enabling Unicast RPF with Inbound and Outbound Filters Example

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.

```
ip cef distributed
!
interface Serial 5/0/0
  description Connection to Upstream ISP
  ip address 209.165.200.225 255.255.255.252
  no ip redirects
  no ip directed-broadcast
  no ip proxy-arp
  ip verify unicast reverse-path
  ip access-group 111 in
  ip access-group 110 out
!
access-list 110 permit ip 209.165.202.128 0.0.0.31 any
access-list 110 deny ip any any log
access-list 111 deny ip host 0.0.0.0 any log
access-list 111 deny ip 127.0.0.0 0.255.255.255 any log
access-list 111 deny ip 10.0.0.0 0.255.255.255 any log
access-list 111 deny ip 172.16.0.0 0.15.255.255 any log
access-list 111 deny ip 192.168.0.0 0.0.255.255 any log
access-list 111 deny ip 209.165.202.128 0.0.0.31 any log
access-list 111 permit ip any any
```

# Command Reference

This section documents the **ip verify unicast rpf** command that configures the Unicast Reverse Path Forwarding feature.

# ip verify unicast reverse-path

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

**ip verify unicast reverse-path**

**no ip verify unicast reverse-path**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Unicast RPF is disabled.

**Command Modes** Interface configuration mode

## Command History

Release	Modification
11.1(CC)	This command was introduced.
12.0	This command was introduced.

## Usage Guidelines

Use the **ip verify unicast reverse-path** interface command to help 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 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 “look backwards” ability 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 is an input function and is applied only on the input interface of a router at the upstream end of a connection.

Unicast RPF checks to see if any packet received at a router interface arrives on the best return path (return route) to the source of the packet. Unicast RPF does this by doing a reverse lookup in the CEF table. If the packet was received from one of the best reverse path routes, the packet is forwarded as normal. If there is no reverse path route 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.

**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 EIGRP variants are being used and unequal candidate paths back to the source IP address exist.

---

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

**Note**

---

It is very important for CEF to be configured globally in the router. Unicast RPF will not work without CEF.

---

Unicast RPF should not be used on interfaces that are internal to the network. Internal interfaces are likely to have routing asymmetry, meaning multiple routes to the source of a packet. Unicast RPF should be applied only where there is natural or configured symmetry.

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. 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**

The following example enables Unicast RPF on a serial interface:

```
ip cef
! or "ip cef distributed" for RSP+VIP based routers
!
interface serial 5/0/0
 ip verify unicast reverse-path
```

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.

```
ip cef distributed
!
interface Serial 5/0/0
 description Connection to Upstream ISP
 ip address 209.165.200.225 255.255.255.252
 no ip redirects
 no ip directed-broadcast
 no ip proxy-arp
 ip verify unicast reverse-path
 ip access-group 111 in
 ip access-group 110 out
!
access-list 110 permit ip 209.165.202.128 0.0.0.31 any
access-list 110 deny ip any any log
access-list 111 deny ip host 0.0.0.0 any log
access-list 111 deny ip 127.0.0.0 0.255.255.255 any log
access-list 111 deny ip 10.0.0.0 0.255.255.255 any log
access-list 111 deny ip 172.16.0.0 0.15.255.255 any log
access-list 111 deny ip 192.168.0.0 0.0.255.255 any log
access-list 111 deny ip 209.165.202.128 0.0.0.31 any log
access-list 111 permit ip any any
```

#### Related Commands

Command	Description
<b>ip cef</b>	Enables CEF on the route processor card.



■ ip verify unicast reverse-path