Security Configuration Guide: Unicast Reverse Path Forwarding Cisco IOS Release 12.2SR

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Configuring Unicast Reverse Path Forwarding

This chapter describes the Unicast Reverse Path Forwarding (Unicast RPF) feature. The Unicast RPF feature helps to mitigate problems that are caused by malformed or forged IP source addresses that are passing through a router.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites to Configuring Unicast Reverse Path Forwarding

Prior to configuring Unicast RPF, configure ACLs:

- Configure standard or extended 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 standard or extended ACLs entries to drop (deny) packets that have invalid source IP addresses (perform ingress filtering). Invalid source IP addresses include the following types:
  - Reserved addresses
  - Loopback addresses
  - Private addresses (RFC 1918, Address Allocation for Private Internets)
  - Broadcast addresses (including multicast addresses)

    - Source addresses that fall outside the range of valid addresses associated with the protected network
- Configure standard or extended ACL entries to forward (permit) packets that fail the Unicast RPF checks to allow specific traffic from known asymmetric routed sources.

Configure ACLs to track Unicast RPF events by adding the logging option into the ACL command. During network attacks, judicious logging of dropped or forwarded packets (suppressed drops) can provide additional information about network attacks.

Restrictions to Configuring Unicast Reverse Path Forwarding

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 Release 11.2 or 11.3.

Information About Unicast Reverse Path Forwarding

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 Tribal 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.

This section covers the following information:

- How Unicast RPF Works, page 2
- Implementing Unicast RPF, page 6
- Related Features and Technologies, page 11

How Unicast RPF 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 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 or forwarded, depending on whether an access control list (ACL) is specified in the **ip verify unicast reverse-path** interface configuration command.

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 ACLs have been configured, the following actions occur:

SUMMARY STEPS

1. Input ACLs configured on the inbound interface are checked.
2. Unicast RPF 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.
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.

DETAILED STEPS

Step 1 Input ACLs configured on the inbound interface are checked.

Step 2 Unicast RPF 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.

Step 3 CEF table (FIB) lookup is carried out for packet forwarding.

Step 4 Output ACLs are checked on the outbound interface.

Step 5 The packet is forwarded.

This section provides information about Unicast RPF enhancements:

- Access Control Lists and Logging, page 4
- Per-Interface Statistics, page 4

- Access Control Lists and Logging, page 4
- Per-Interface Statistics, page 4

Access Control Lists and Logging

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 see if 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. Using the log information, administrators can see what source addresses are being used in the attack, the time the packets arrived at the interface, and so on.

Caution Logging requires CPU and memory resources. Logging Unicast RPF events for attacks having a high rate of forged packets can degrade the performance of the router.

Per-Interface Statistics

Each time a packet is dropped or forwarded at an interface, that information is counted two ways: globally on the router and at each interface where you have applied Unicast RPF. Global statistics on dropped packets provide information about potential attacks on the network; however, these global statistics do not help to specify which interface is the source of the attack.

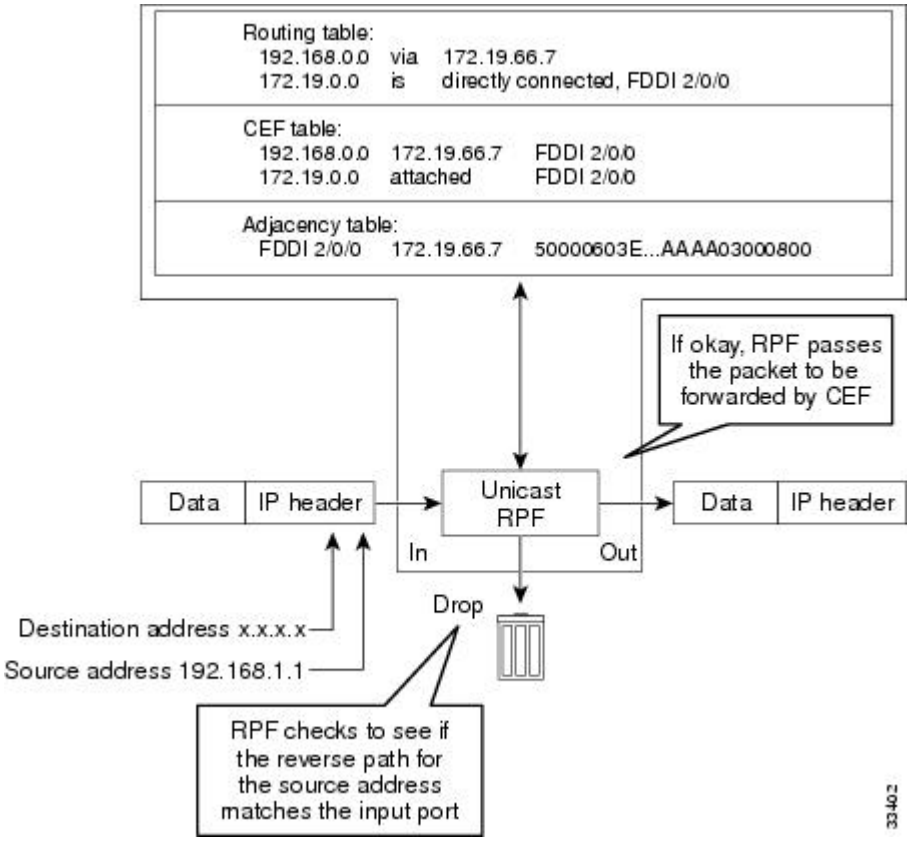
Per-interface statistics allow network administrators to track two types of information about malformed packets: Unicast RPF drops and Unicast RPF suppressed drops. Statistics on the number of packets that Unicast RPF drops help to identify the interface that is the entry point of the attack. The Unicast RPF drop count tracks the number of drops at the interface. The Unicast RPF suppressed drop count tracks the number of packets that failed the Unicast RPF check but were forwarded because of the permit permission set up in the ACL. Using the drop count and suppressed drop count statistics, a network administrator can takes steps to isolate the attack at a specific interface.

Note Judicious use of ACL logging can further identify the address or addresses that are being dropped by Unicast RPF.

The figure below 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.

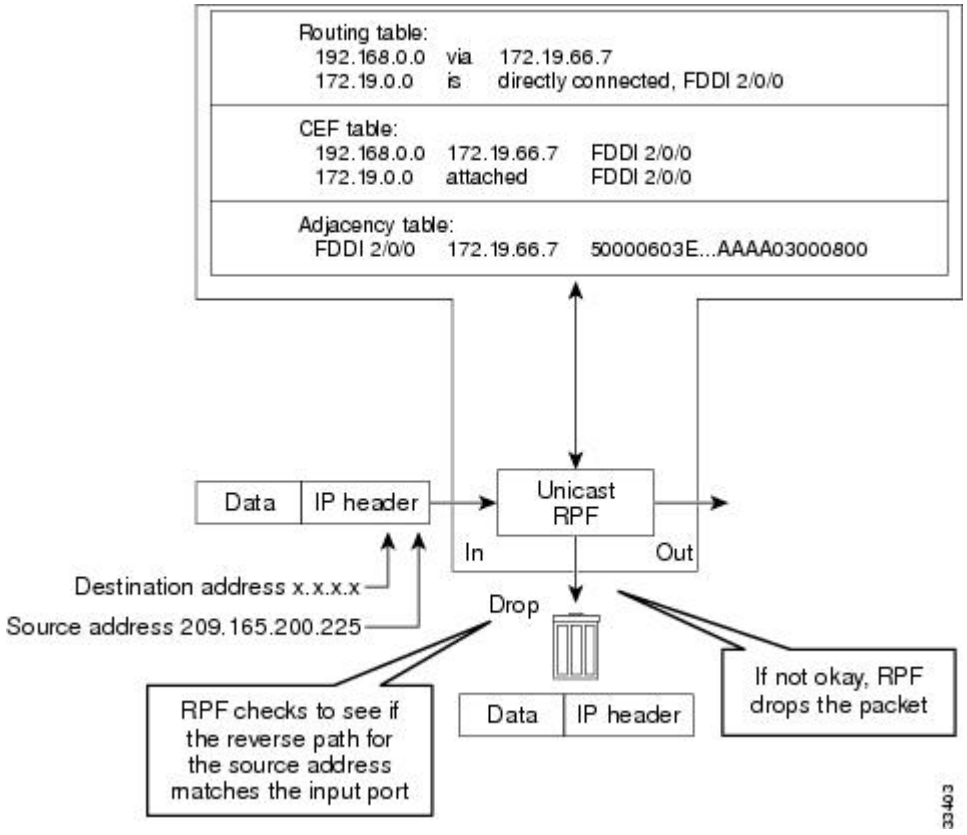
Figure 1 Unicast RPF Validating IP Source Addresses



The figure below 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 has 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. (ACLs permit Unicast RPF to be used when packets are known to be arriving by specific, less optimal asymmetric input paths.)
- 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 and local preference, the best path back to the source address can be modified. Modification would affect the operation of Unicast RPF.

This section provides information about the implementation of Unicast RPF:

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

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.

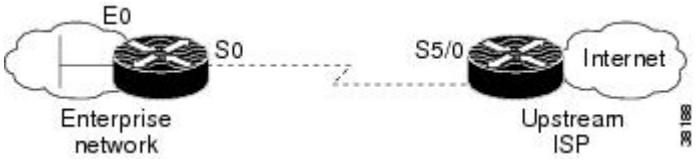
ACLs work well for many single-homed customers; however, there are trade-offs when ACLs are used as ingress filters, including two commonly referenced limitations:

- 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 Unicast RPF is configured for ingress filtering.

The figure below 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 the topography in the figure above, 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
```

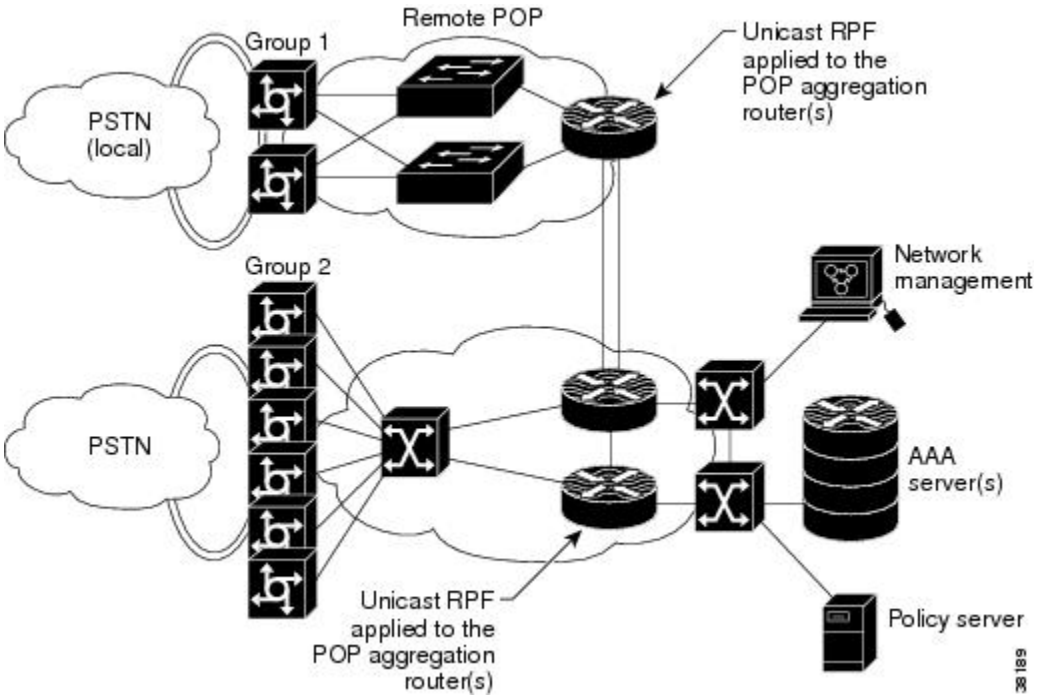
Notice that Unicast RPF works with a single default route. There are no additional routes or routing protocols. Network 192.168.10.0/22 is a connected network. Hence, packets coming from the Internet with a source address in the range 192.168.10.0/22 will be dropped by Unicast RPF.

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.

The figure below 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 Table 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.

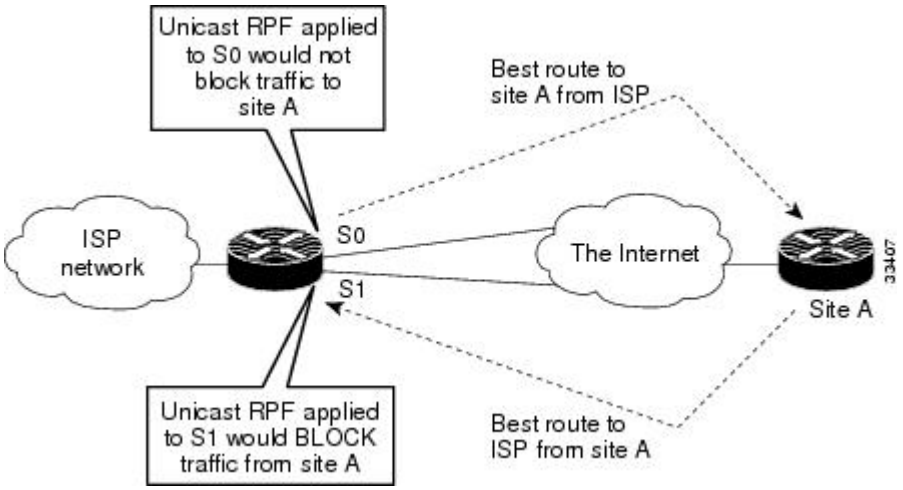
Where Not to Use Unicast RPF

Unicast RPF should not be used on interfaces that are internal to the network. Internal interfaces are likely to have routing asymmetry (see the figure below), 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, unless you use ACLs to allow the router to accept incoming packets. ACLs permit Unicast RPF to be used when packets are known to be arriving by specific, less optimal asymmetric input paths. However, 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.

The figure below 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. This enhancement was added in Cisco IOS Release 12.0 and later, but it is not in Cisco IOS Release 11.1CC.

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.
- Unicast RPF can be more effective at mitigating spoofing attacks when combined with a policy of ingress and egress filtering using Cisco IOS access control lists (ACLs).
    - 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.

For more information on network filtering, refer to RFC 2267.

- Cisco IOS software provides additional features that can help mitigate DoS attacks:
    - Committed Access Rate (CAR). CAR allows you to enforce a bandwidth policy against network traffic that matches an access list. For example, CAR allows you to rate-limit what should be low-volume traffic, such as ICMP traffic. To find out more about CAR, refer to the *Cisco IOS Quality of Service Solutions Configuration Guide* .
    - Context-based Access Control (CBAC). CBAC selectively blocks any network traffic not originated by a protected network. CBAC uses timeout and threshold values to manage session state information, helping to determine when to drop sessions that do not become fully established. Setting timeout values for network sessions helps mitigate DoS attacks by freeing up system resources, dropping sessions after a specified amount of time. For more information on CBAC, refer to the *Cisco IOS Security Configuration Guide* .
    - TCP Intercept. The TCP Intercept feature implements software to protect TCP servers from TCP SYN-flooding attacks, which are a type of DoS attack. A SYN-flooding attack occurs when a hacker floods a server with a barrage of requests for connection. Like CBAC, the TCP Intercept feature also uses timeout and threshold values to manage session state information, helping to determine when to drop sessions that do not become fully established. For more information on TCP Intercept, refer to the *Cisco IOS Security Configuration Guide*

How to Configure Unicast Reverse Path Forwarding

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:

SUMMARY STEPS

1. Router(config)# **ip cef**
2. Router(config-if)# **interface** *type*
3. Router(config-if)# **ip verify unicast reverse-path list**
4. Router(config-if)# **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **ip cef** **Example:** **Example:** or **Example:** `Router(config)#` **ip cef distributed**	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. 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 **no ip route-cache cef** interface 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 **ip route-cache cef** command in interface configuration mode.
Step 2	Router(config-if)# **interface** *type*	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. 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 ?** command.
Step 3	Router(config-if)# **ip verify unicast reverse-path list**	Enables Unicast RPF on the interface. • Use the *list* option to identify an access list. If the access list denies network access, spoofed packets are dropped at the interface. If the access list permits network access, spoofed packets are forwarded to the destination address. Forwarded packets are counted in the interface statistics. If the access list includes the logging option, information about the spoofed packets is logged to the log server. • Repeat this step for each access list that you want specify.
Step 4	Router(config-if)# **exit**	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
!The next line displays Unicast RPF packet dropping information.
 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
!The next line displays Unicast RPF packet dropping information.
 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

If you experience problems while using Unicast RPF, check the following items.

- HSRP Failure, page 13
- Dropped Boot Requests, page 13

HSRP Failure

Failure to disable Unicast RPF before disabling CEF can cause Hot Standby Router Protocol (HSRP) failure. 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.”

Dropped Boot Requests

In Cisco IOS Release 11.1(17)CC, Unicast RPF can drop BOOTP request packets that have a source address of 0.0.0.0 due to source address verification at the interface. To enable boot requests to work on the interface, you must use ACLs instead of Unicast RPF.

Monitoring and Maintaining Unicast RPF

This section describes commands used to monitor and maintain Unicast RPF.

Command	Purpose
`Router#` **show ip traffic**	Displays global router statistics about Unicast RPF drops and suppressed drops.

Command	Purpose
`Router#` **show ip interface type**	Displays per-interface statistics about Unicast RPF drops and suppressed drops.
`Router#` **show access-lists**	Displays the number of matches to a specific ACL.
`Router(config-if)#` **no ip verify unicast reverse-path list**	Disables Unicast RPF at the interface. Use the *list* option to disable Unicast RPF for a specific ACL at the interface.

Caution To disable CEF, you must first disable Unicast RPF. Failure to disable Unicast RPF before disabling CEF can cause HSRP failure. If you want to disable CEF on the router, you must first disable Unicast RPF.

Unicast RPF counts the number of packets dropped or suppressed because of malformed or forged source addresses. Unicast RPF counts dropped or forwarded packets that include the following global and per-interface information:

- Global Unicast RPF drops
- Per-interface Unicast RPF drops
- Per-interface Unicast RPF suppressed drops

The **show ip traffic** command shows the total number (global count) of dropped or suppressed packets for all interfaces on the router. 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
  ! The second line below (“0 unicast RPF”) displays Unicast RPF packet dropping
information.
  Drop:  3 encapsulation failed, 0 unresolved, 0 no adjacency
         0 no route, 0 unicast RPF, 0 forced drop
```

A nonzero value for the count of dropped or suppressed packets can mean one of two things:

- Unicast RPF is dropping or suppressing packets that have a bad source address (normal operation).
- Unicast RPF is dropping or suppressing 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.

The **show ip interface** command shows the total of dropped or suppressed packets at a specific interface. If Unicast RPF is configured to use a specific ACL, that ACL information is displayed along with the drop statistics.

```
Router> show ip interface ethernet0/1/1
   Unicast RPF ACL 197
```

```
   1 unicast RPF drop
   1 unicast RPF suppressed drop
```

The **show access-lists** command displays the number of matches found for a specific entry in a specific access list.

```
Router> show access-lists
Extended IP access list 197
     deny ip 192.168.201.0 0.0.0.63 any log-input (1 match)
     permit ip 192.168.201.64 0.0.0.63 any log-input (1 match)
     deny ip 192.168.201.128 0.0.0.63 any log-input
     permit ip 192.168.201.192 0.0.0.63 any log-input
```

Configuration Examples for Unicast Reverse Path Forwarding

Example Unicast RPF on a Leased-Line Aggregation Router

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
```

Example Unicast RPF on the Cisco AS5800 Using Dialup Ports

The following example enables Unicast RPF on a Cisco AS5800. The **interface Group-Async** command makes it easy to apply Unicast RPF on all the dialup ports.

```
ip cef
!
interface Group-Async1
 ip verify unicast reverse-path
```

Example Unicast RPF with Inbound and Outbound Filters

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
```

Example Unicast RPF with ACLs and Logging

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 Ethernet0 to check packets arriving at that interface.

For example, packets with a source address of 192.168.201.10 arriving at interface Ethernet0 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 Ethernet0 are forwarded because of the permit statement in ACL 197. ACL information about dropped or suppressed packets is logged (logging option 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 reverse-path 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
```

Feature Information for Configuring Unicast Reverse Path Forwarding

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 1 Feature Information for Configuring Unicast Reverse Path Forwarding

Feature Name	Releases	Feature Information
Configuring Unicast Reverse Path Forwarding	12.3(6) Cisco IOS XE 3.1.0SG	The Unicast RPF feature helps to mitigate problems that are caused by malformed or forged IP source addresses that are passing through a router.

Unicast Reverse Path Forwarding Loose Mode

The Unicast Reverse Path Forwarding Loose Mode feature creates a new option for Unicast Reverse Path Forwarding (Unicast RPF), providing a scalable anti-spoofing mechanism suitable for use in multihome network scenarios. This mechanism is especially relevant for Internet Service Providers (ISPs), specifically on routers that have multiple links to multiple ISPs. In addition, Unicast RPF (strict or loose mode), when used in conjunction with a Border Gateway Protocol (BGP) "trigger," provides an excellent quick reaction mechanism that allows network traffic to be dropped on the basis of either the source or destination IP address, giving network administrators an efficient tool for mitigating denial of service (DoS) and distributed denial of service (DDoS) attacks.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for Unicast RPF Loose Mode

To use Unicast RPF, you must enable Cisco Express Forwarding (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 for other switching modes.

Information About Unicast RPF Loose Mode

Unicast RPF Background

A number of common types of DoS attacks take advantage of forged or rapidly changing source IP addresses, allowing attackers to thwart efforts by ISPs to locate or filter these attacks. Unicast RPF was originally created to help mitigate such attacks by providing an automated, scalable mechanism to implement the Internet Engineering Task Force (IETF) Best Common Practices 38/Request for Comments 2827 (BCP 38/RFC 2827) anti-spoofing filtering on the customer-to-ISP network edge. By taking advantage of the information stored in the Forwarding Information Base (FIB) that is created by the CEF switching process, Unicast RPF can determine whether IP packets are spoofed or malformed by matching the IP source address and ingress interface against the FIB entry that reaches “back” to this source (a so-called “reverse lookup”). Packets that are received from one of the best reverse path routes back out of the same interface are 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, and the packet is dropped (by default).

This original implementation of Unicast RPF, known as “strict mode,” required a match between the ingress interface and the reverse path FIB entry. With Unicast RPF, all equal-cost “best” return paths are considered valid, meaning that it works for cases in which multiple return paths exist, provided that each path is equal in routing cost to the others (number of hops, weights, and so on), and as long as the route is in the FIB. Unicast RPF also functions when Enhanced Interior Gateway Routing Protocol (EIGRP) variants are being used and unequal candidate paths back to the source IP address exist. The strict mode works well for customer-to-ISP network edge configurations that have symmetrical flows (including some multihomed configurations in which symmetrical flows can be enforced).

However, some customer-to-ISP network edges and nearly all ISP-to-ISP network edges use multihomed configurations in which routing asymmetry is typical. When traffic flows are asymmetrical, that is, those in which traffic from Network A to Network B would normally take a different path from traffic flowing from Network B to Network A, the Unicast RPF check will always fail the strict mode test. Because this type of asymmetric routing is common among ISPs and in the Internet core, the original implementation of Unicast RPF was not available for use by ISPs on their core routers and ISP-to-ISP links.

Over time and with an increase in DDoS attacks on the Internet, the functionality of Unicast RPF was reviewed as a tool that ISPs can use on the ISP-to-ISP network edge (an ISP router “peered” with another ISP router) to enable dynamic BGP, triggered black-hole filtering. To provide this functionality, however, the mechanisms used with Unicast RPF had to be modified to permit its deployment on the ISP-to-ISP network edge so that asymmetrical routing is not an issue.

Loose Mode

To provide ISPs with a DDoS resistance tool on the ISP-to-ISP edge of a network, Unicast RPF was modified from its original strict mode implementation to check the source addresses of each ingress packet without regard for the specific interface on which it was received. This modification is known as “loose mode.” Loose mode allows Unicast RPF to automatically detect and drop packets such as the following:

- IETF RFC 1918 source addresses
- Other Documenting Special Use Addresses (DUSA) that should not appear in the source
- Unallocated addresses that have not been allocated by the Regional Internet Registries (RIRs)
- Source addresses that are routed to a null interface on the router

Loose mode removes the match requirement on the specific ingress interface, allowing Unicast RPF to loose-check packets. This packet checking allows the “peering” router of an ISP having multiple links to multiple ISPs to check the source IP address of ingress packets to determine whether they exist in the FIB.

If they exist, the packets are forwarded. If they do not exist in the FIB, the packets fail and are dropped. This checking increases resistance against DoS and DDoS attacks that use spoofed source addresses and unallocated IP addresses.

How to Configure Unicast RPF Loose Mode

Configuring Unicast RPF Loose Mode

To configure Unicast RPF loose mode, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef**
4. **interface** *type slot / port-adapter / port*
5. **ip verify unicast source reachable-via any**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip cef** **Example:** `Router (config)# ip cef`	Enables CEF on the route processor card.
Step 4	**interface** *type slot / port-adapter / port* **Example:** `Router (config)# interface serial5/0/0`	Configures an interface type and enters interface configuration mode.

Command or Action	Purpose
Step 5 **ip verify unicast source reachable-via any** **Example:** `Router (config-if)# ip verify unicast source reachable-via any`	Enables Unicast RPF using loose mode.

- Troubleshooting Tips, page 22

Troubleshooting Tips

CEF Not Enabled

If CEF is not enabled on your device and an attempt is made to deploy Unicast RPF, the following error message is generated:

```
Router(config-if)# ip verify unicast source reachable-via any
% CEF not enabled. Enable first.
```

Dropped Packets

If it is believed that Unicast RPF is dropping packets that are deemed valid, it may be necessary to configure an access list within Unicast RPF to pass these specific packets.

- Check to see if Unicast RPF is dropping packets using the following **show** commands.

```
Router# show ip traffic
 | include unicast RPF
```

The above command output displays the global counter for packets dropped by Unicast RPF. If the packet drop counter is increasing, Unicast RPF is dropping packets.

```
Router# show ip interface
 {
type
/
slot
/
port
} | include verif
```

The above command output displays drop counters on a per-interface basis. If the packet drop counter is increasing, Unicast RPF is dropping packets on the referenced interface.

- Configure a “classification” access list (one that is used to identify traffic types) and add it to the Unicast RPF configuration on the interface or interfaces that are in question.

In this case, the most prudent classification access list would be one that includes a series of “deny” statements covering the traffic types in question (instead of the more traditional “permit” statements that would be used, for example, in a typical classification access list that would be applied directly to an interface). The **logging** keyword may be useful for this access list as well.

- Apply the above access list to Unicast RPF on the interface in question using the following command:

```
Router (config-if)# ip verify unicast source reachable-via any 199
```

- Periodically check the counters on the above access list using the following **show** command:

```
Router# show ip access-list 199
```

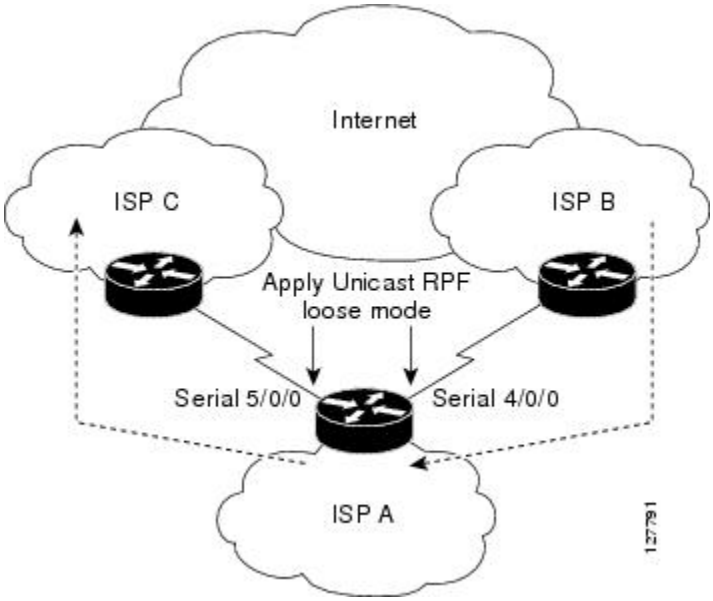
If the access list hit counters are increasing for the packet type in question, Unicast RPF is dropping the packets in question. To permit them, configure an access list using a “permit” statement for the packet type in question and apply it to Unicast RPF.

Configuration Examples for Unicast RPF Loose Mode

Example Configuring Unicast RPF Using Loose Mode

The following example (see the figure below) uses a simple dual-homed ISP to demonstrate the concept of Unicast RPF loose mode. The example illustrates an ISP (A) peering router that is connected to two different upstream ISPs (B and C) and shows that traffic flows into and out of ISP A may be asymmetric given this dual-homed configuration. Hence, provisions for asymmetrical flows (when outbound traffic goes out one link and returns via a different link) must be accounted for by the Unicast RPF deployment. In this case, it is appropriate to use the loose-mode configuration of Unicast RPF because this configuration alleviates the interface dependency of strict mode.

Figure 6 Unicast RPF Loose Mode




```
interface Serial4/0/0
 description - link to ISP B
 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 any
!
interface Serial5/0/0
 description - link to ISP C
 ip address 172.16.100.9 255.255.255.252
 no ip redirects
 no ip directed-broadcasts
 no ip proxy-arp
 ip verify unicast source reachable-via any
!
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Best practices using Unicast RPF	Internet Service Provider (ISP) Security Bootcamp/ Best Practices--CPN-Summit-2004/Paris-Sept-04

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 Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Unicast RPF Loose Mode

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 2 Feature Information for Unicast RPF Loose Mode

Feature Name	Releases	Feature Information
Unicast RPF Loose Mode	12.0(15)S 12.1(8a)E 12.2(13)T	The Unicast Reverse Path Forwarding Loose Mode feature creates a new option for Unicast Reverse Path Forwarding (Unicast RPF), providing a scalable anti-spoofing mechanism suitable for use in multihome network scenarios. This mechanism is especially relevant for Internet Service Providers (ISPs), specifically on routers that have multiple links to multiple ISPs. The following commands were introduced or modified: **ip verify unicast reverse-path**, **ip verify unicast source reachable-via**.

CISCO-IP-URPF-MIB Support

The CISCO-IP-URPF-MIB support provides Simple Network Management Protocol (SNMP) notification when a specified drop-rate threshold on a managed device is exceeded. You can use the IP Unicast Reverse Path Forwarding (RPF) feature to avert denial of service (DoS) attacks by verifying the validity of the source IP of an incoming packet. You can configure the Unicast RPF drop-rate threshold globally for a device or per interface.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for CISCO-IP-URPF-MIB Support

Before you configure CISCO-IP-URPF-MIB, you must configure the following features:

- Cisco Express Forwarding switching
- IP routing
- SNMP
- Unicast RPF

Restrictions for CISCO-IP-URPF-MIB Support

- Because Cisco IOS software does not support VPN routing and forwarding (VRF)-specific Unicast RPF counters, it does not support the following MIB objects related to VRF:
  - cipUrpfIfVrfName
  - cipUrpfVrfName
  - cipUrpfVrfIfDrops
  - cipUrpfVrfIfDiscontinuityTime
- This implementation of the CISCO-IP-URPF MIB supports only IPv4.

Information About CISCO-IP-URPF-MIB Support

Implementation of Unicast RPF Notification

Unicast RPF is a security feature that verifies the validity of the source IP of an incoming packet. When a packet arrives at an interface and its source IP is unknown in the routing table or is a known bad source address, Unicast RPF drops the packet. IP verification of the source is done to prevent the DoS attacks by detecting problems with the incoming packets on an interface. However, deploying Unicast RPF without some automated monitoring capability is a challenge.

The CISCO-IP-URPF-MIB lets you specify a Unicast RPF drop-rate threshold on interfaces of a managed device that will send an SNMP notification when the threshold is exceeded. The MIB includes objects for specifying global and per-interface drop counts and drop rates and a method to generate SNMP traps when the drop rate exceeds a configurable per-interface threshold.

Although you can configure some parameters globally, you must configure the CISCO-IP-URPF-MIB on individual interfaces.

Elements of Unicast RPF Notification

The elements described in the following sections make Unicast RPF drop-rate notification work:

- Drop-Rate Computation, page 29
- Global Scalars, page 29
- Global Tables, page 29
- Per-Interface Configuration, page 29

Drop-Rate Computation

Whenever Unicast RPF is configured on an interface, the drop-rate calculation is done periodically (at intervals specified by the cipUrpfComputeInterval object). Drop rates are computed over a constantly sliding window, whose period starts at the configured number of seconds before the calculation and ends with the performance of the calculation.

Global Scalars

The following global scalars affect how the MIB agent computes all drop rates and generates notifications:

- cipUrpfDropRateWindow--This object specifies the window of time in the recent past over which the drop rate computation occurs. If there was no window (that is, the window is the epoch since booting up), an identical drop count burst at a later time would produce a lower drop rate than the one occurring earlier.
- cipUrpfComputeInterval--This object specifies how often the drop-rate computation occurs.
- cipUrpfDropNotifyHoldDownTime--This object specifies the minimum time between notifications for a particular packet flow on an interface.

Global Tables

The CISCO-IP-URPF-MIB includes the following global tables:

- cipUrpfTable--This table contains the global drop count and drop-rate objects per packet flow. These global rates are useful for quickly determining whether the managed device had Unicast RPF activity at a specific time.
- cipUrpfVrfTable--This table contains the index drop counters by VRF (if a VRF routing table is used to determine Unicast RPF checking). The table provides a method for VRF to index all the Unicast RPF-enabled interfaces.

Per-Interface Configuration

The following MIB objects enable per-interface configuration:

- cipUrpfIfDropRateNotifyEnable--This object specifies whether the system produces the cipUrpfIfDropRateNotify notification because Unicast RPF has dropped version cipUrpfIfIpVersion IP packets on the specified interface.
- cipUrpfIfNotifyDropRateThreshold--This object specifies the drop-rate threshold value above which a notification is generated.

Per-Interface Statistics

The following MIB objects track per-interface statistics:

- cipUrpfIfMonTable--This table contains the statistics for a particular packet flow on an interface.
- cipUrpfIfDrops--This object accumulates Unicast RPF drops on an interface. Snapshots of this value are used in the drop-rate computation. The computed drop rate is specified in the cipUrpfIfDropRate object. If Unicast RPF is configured on a subinterface, drop rates are computed.

How to Configure Unicast RPF Drop-Rate Notification

Configuring Unicast RPF Drop-Rate Notification via Syslog

Perform this task to configure the Unicast RPF drop-rate threshold and computation parameters for notification via syslog.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip verify drop-rate compute window** *seconds*
4. **ip verify drop-rate compute interval** *seconds*
5. **ip verify drop-rate notify hold-down** *seconds*
6. **interface** *type number*
7. **ip verify unicast notification threshold** *packets-per-second*
8. **end**
9. **show ip interface** *type number*
10. **debug ip verify mib**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip verify drop-rate compute window** *seconds* **Example:** `Router(config)# ip verify drop-rate compute window 60`	Configures the period of time, in seconds, over which the Unicast RPF drop count used in the drop-rate computation is collected. • The range is from 30 to 300. The default is 300. **Note** The value for the compute window must be greater than or equal to that entered using the **ip verify drop-rate compute interval** command.

	Command or Action	Purpose
Step 4	**ip verify drop-rate compute interval** *seconds* **Example:** `Router(config)# ip verify drop-rate compute interval 60`	Configures the interval of time, in seconds, between Unicast RPF drop-rate computations. • The range is from 30 to 300. The default is 30. **Note** The value for the compute interval must be less than or equal to that entered using the **ip verify drop-rate compute window** command.
Step 5	**ip verify drop-rate notify hold-down** *seconds* **Example:** `Router(config)# ip verify drop-rate notify hold-down 60`	Configures the minimum time, in seconds, between Unicast RPF drop-rate notifications. • The range is from 30 to 300. The default is 300.
Step 6	**interface** *type number* **Example:** `Router(config)# interface ethernet 3/0`	Configures an interface and enters interface configuration mode.
Step 7	**ip verify unicast notification threshold** *packets-per-second* **Example:** `Router(config-if)# ip verify unicast notification threshold 750`	Configures the threshold value, in packets per second, which determines whether to send a Unicast RPF drop-rate notification. • The range is from 0 to 2147483647. The default is 1000. **Note** If you configure the threshold as 0, every packet drop triggers a notification.
Step 8	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 9	**show ip interface** *type number* **Example:** `Router# show ip interface ethernet 2/3`	(Optional) Displays the verification drop rate and the number of verification drops when Unicast RPF is configured for an interface.
Step 10	**debug ip verify mib** **Example:** `Router# debug ip verify mib`	(Optional) Displays output that is useful for troubleshooting Unicast RPF notification.

Configuring Unicast RPF Drop-Rate Notification via SNMP

Perform this task to configure the Unicast RPF drop-rate threshold and computation parameters for notification via SNMP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip verify drop-rate compute window** *seconds*
4. **ip verify drop-rate compute interval** *seconds*
5. **ip verify drop-rate notify hold-down** *seconds*
6. **interface** *type number*
7. **ip verify unicast notification threshold** *packets-per-second*
8. **snmp trap ip verify drop-rate**
9. **end**
10. **show ip interface** *type number*
11. **debug ip verify mib**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip verify drop-rate compute window** *seconds* **Example:** `Router(config)# ip verify drop-rate compute window 60`	Configures the period of time, in seconds, over which the Unicast RPF drop count used in the drop-rate computation is collected. • The range is from 30 to 300. The default is 300. **Note** The value for the compute window must be greater than or equal to that entered using the **ip verify drop-rate compute interval** command.

	Command or Action	Purpose
Step 4	**ip verify drop-rate compute interval** *seconds* **Example:** `Router(config)# ip verify drop-rate compute interval 60`	Configures the interval of time, in seconds, between Unicast RPF drop-rate computations. • The range is from 30 to 300. The default is 30. **Note** The value for the compute interval must be less than or equal to that entered using the **ip verify drop-rate compute window**command.
Step 5	**ip verify drop-rate notify hold-down** *seconds* **Example:** `Router(config)# ip verify drop-rate notify hold-down 60`	Configures the minimum time, in seconds, between Unicast RPF drop-rate notifications. • The range is from 30 to 300. The default is 300.
Step 6	**interface** *type number* **Example:** `Router(config)# interface ethernet 3/0`	Configures an interface and enters interface configuration mode.
Step 7	**ip verify unicast notification threshold** *packets-per-second* **Example:** `Router(config-if)# ip verify unicast notification threshold 750`	Configures the threshold value, in packets per second, which determines whether to send a Unicast RPF drop-rate notification. • The range is from 0 to 2147483647. The default is 1000. **Note** If you configure the threshold to be 0, every packet drop triggers a notification.
Step 8	**snmp trap ip verify drop-rate** **Example:** `Router(config-if)# snmp trap ip verify drop-rate`	Configures the router to send an SNMP notification when the Unicast RPF drop rate exceeds the configured threshold.
Step 9	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 10	**show ip interface** *type number* **Example:** `Router# show ip interface ethernet 2/3`	(Optional) Displays the verification drop rate and the number of verification drops when Unicast RPF is configured for an interface.

	Command or Action	Purpose
Step 11	**debug ip verify mib** **Example:** `Router# debug ip verify mib`	(Optional) Displays output that is useful for troubleshooting Unicast RPF notification.

Configuration Examples for CISCO-IP-URPF-MIB Support

Example Configuring Unicast RPF Drop-Rate Notification via Syslog

The following example shows how to configure Unicast RPF drop-rate notification via syslog:

```
Router> enable
Router# configure terminal
Router(config)# ip verify drop-rate compute window 60
Router(config)# ip verify drop-rate compute interval 60
Router(config)# ip verify drop-rate notify hold-down 60
Router(config)# i
nterface ethernet 3/0
Router(config-if)# ip verify unicast notification threshold 750
Router(config-if)# end
```

Example Configuring Unicast RPF Drop-Rate Notification via SNMP

The following example shows how to configure Unicast RPF drop-rate notification via SNMP:

```
Router> enable
Router# configure terminal
Router(config)# ip verify drop-rate compute window 60
Router(config)# ip verify drop-rate compute interval 60
Router(config)# ip verify drop-rate notify hold-down 60
Router(config)# interface ethernet 3/0
Router(config-if)# ip verify unicast notification threshold 750
Router(config-if)# snmp trap ip verify drop-rate
Router(config-if)# end
```

Example Verifying and Troubleshooting the Unicast RPF Configuration

The following is sample output from the **show ip interface** command. The output displays the verification drop rate and the number of verification drops when Unicast RPF is configured for an interface. The last five lines in the following example show the output of the **show ip interface**command when Unicast RPF is configured:

```
Router# show ip interface ethernet 2/3
Ethernet2/3 is up, line protocol is up
  Internet address is 10.10.5.4/16
```

```
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP Flow switching is disabled
  IP CEF switching is disabled
  IP Null turbo vector
  IP Null turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are No CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
  Input features: uRPF
  IP verify source reachable-via RX, allow default
   0 verification drops
   0 suppressed verification drops
   0 verification drop-rate
Router#
```

The following is sample output from the **debug ip verify mib** command. The command displays output that is useful for troubleshooting Unicast RPF notification:

```
Router# debug ip verify mib
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: ipurpfmib_get_scalars
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: ipurpfmib_get_scalars
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: ipurpfmib_get_scalars
01:29:45: cipUrpfScalar_get, searchType
161ipurpfmib_get_urpf_entryipurpfmib_get_urpf_entryipurpfmib_get_urpf_entryipurpfmib_get_
urpf_entry
01:29:45: cipUrpfIfMonEntry_get, searchType 161
01:29:45: ipurpfmib_get_urpf_ifmon_entry entry: ST 161, if 1, ip 1
01:29:45: cipUrpfIfMonEntry_get, searchType 161
01:29:45: ipurpfmib_get_urpf_ifmon_entry entry: ST 161, if 1, ip 1
01:29:45: cipUrpfIfMonEntry_get, searchType 161
01:29:45: ipurpfmib_get_urpf_ifmon_entry entry: ST 161, if 1, ip 1
01:29:45: cipUrpfIfMonEntry_get, searchType 161
01:29:45: ipurpfmib_get_urpf_ifmon_entry entry: ST 161, if 1, ip 1
01:29:45: cipUrpfIfMonEntry_get, searchType 161
01:29:45: ipurpfmib_get_urpf_ifmon_entry entry: ST 161, if 1, ip 1
01:29:45: cipUrpfIfMonEntry_get, searchType 161
01:29:45: ipurpfmib_get_urpf_ifmon_entry entry: ST 161, if 1, ip 1
01:29:45: cipUrpfIfMonEntry_get, searchType 161
01:29:45: ipurpfmib_get_urpf_ifmon_entry entry: ST 161, if 1, ip 1
01:29:45: cipUrpfIfMonEntry_get, searchType 161
01:29:45: ipurpfmib_get_urpf_ifmon_entry entry: ST 161, if 1, ip 1
01:29:45: cipUrpfIfMonEntry_get, searchType 161
```

```
01:29:45: ipurpfmib_get_urpf_ifmon_entry entry: ST 161, if 1, ip 1
01:29:45: cipUrpfIfMonEntry_get, searchType 161
01:29:45: ipurpfmib_get_urpf_ifmon_entry entry: ST 161, if 1, ip 1
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Security commands	*Cisco IOS Security Command Reference*
Configuring Unicast RPF	"Configuring Unicast Reverse Path Forwarding" module in the *Cisco IOS Security Configuration Guide: Securing the Data Plane*
Configuring SNMP	"Configuring SNMP Support" module in the *Network Management Configuration Guide*

MIBs

MIB	MIBs Link
CISCO-IP-URPF-MIB	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

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for CISCO-IP-URPF-MIB Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 3 Feature Information for CISCO-IP-URPF-MIB Support

Feature Name	Releases	Feature Information
CISCO-IP-URPF-MIB Support	12.2(31)SB2 12.2(33)SRC 12.4(20)T 12.2(33)SXI2 12.2(50)SY	The CISCO-IP-URPF-MIB provides SNMP notification when a specified drop-rate threshold on a managed device is exceeded. You can use the IP Unicast RPF feature to avert DoS attacks by verifying the validity of the source IP of an incoming packet. You can configure the Unicast RPF drop-rate threshold globally for a device or per interface. The following commands were introduced or modified: **debug ip verify mib**, **ip verify drop-rate compute interval**, **ip verify drop-rate compute window**, **ip verify drop-rate notify hold-down**, **ip verify unicast notification threshold**, **show ip interface**, **snmp trap ip verify drop-rate**