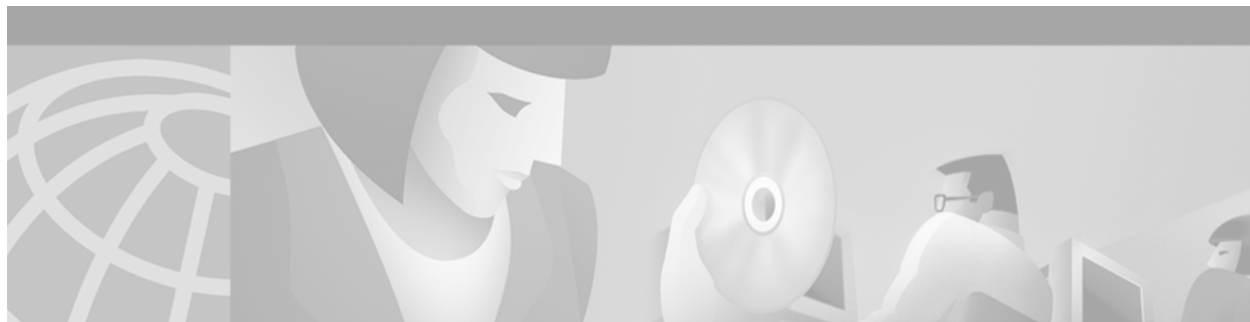




Unicast Reverse Path Forwarding Commands

This chapter describes Unicast Reverse Path Forwarding (Unicast RPF) commands. The Unicast RPF feature helps mitigate problems 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.

To find complete descriptions of other commands used when configuring Unicast RPF, refer to the *Cisco IOS Command Reference Master Index* or search online.

For Unicast RPF configuration information, refer to the “Configuring Unicast Reverse Path Forwarding” chapter in the *Cisco IOS Security Configuration Guide*.

ip verify unicast reverse-path

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

```
ip verify unicast reverse-path [list]

no ip verify unicast reverse-path [list]
```

Syntax Description	list (Optional) Specifies a numbered access control list (ACL) in the following ranges: 1 to 99 (IP standard access list) 100 to 199 (IP extended access list) 1300 to 1999 (IP standard access list, expanded range) 2000 to 2699 (IP extended access list, expanded range)
--------------------	--

Defaults	Unicast RPF is disabled.
----------	--------------------------

Command Modes	Interface configuration mode
---------------	------------------------------

Command History	Release	Modification
	11.1(CC), 12.0	This command was introduced. This command was not included in Cisco IOS Release 11.2 or 11.3
	12.1(2)T	Added ACL support using the <i>list</i> argument. Added per-interface statistics on dropped or suppressed packets.

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

When Unicast RPF is enabled on an interface, the router examines all packets received on that interface. The router checks to make sure that the source address appears in the routing table and matches 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.

The Unicast Reverse Path Forwarding feature 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. The feature does this by doing a reverse lookup in the CEF table. If Unicast RPF does not find a reverse path for the packet, Unicast RPF can

drop or forward the packet, depending on whether an ACL is specified in the Unicast Reverse Path Forwarding command. If an ACL is specified in the command, then when (and only when) a packet fails the Unicast RPF check, the ACL is checked to 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 Reverse Path Forwarding 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 Reverse Path Forwarding command. Log information can be used to gather information about the attack, such as source address, time, and so on.

**Note**

With Unicast RPF, all equal-cost “best” return paths are considered valid. This means that Unicast RPF works in cases where multiple return paths exist, provided that each path is equal to the others in terms of the routing cost (number of hops, weights, and so on) and as long as the route is in the FIB. Unicast RPF also functions where Enhanced Internet Gateway Routing Protocol (EIGRP) variants are being used and unequal candidate paths back to the source IP address exist.

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

Examples

The following example shows enabling the Unicast Reverse Path Forwarding feature 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 209.165.202.129/28 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 209.165.200.225 255.255.255.224
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 209.165.202.129 10.0.0.31 any
access-list 110 deny ip any any log
access-list 111 deny ip host 10.0.0.10 any log
access-list 111 deny ip 172.31.0.0 255.255.255.255 any log
access-list 111 deny ip 10.0.0.0 255.255.255.255 any log
access-list 111 deny ip 172.16.0.0 255.255.255.255 any log
access-list 111 deny ip 192.168.0.0 255.255.255.255 any log
access-list 111 deny ip 209.165.202.129 10.0.0.31 any log
access-list 111 permit ip any any
```

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 Ethernet0/1/1 are forwarded because of the permit statement in ACL 197. ACL information about dropped or suppressed packets is logged (the logging option is turned on for the ACL entry) to the log server.

```
ip cef distributed
!
int eth0/1/1
ip address 192.168.200.225 255.255.255.255
ip verify unicast reverse-path 197
!
int eth0/1/2
ip address 192.168.201.1 255.255.255.255
!
access-list 197 deny ip 192.168.201.0 10.0.0.63 any log-input
access-list 197 permit ip 192.168.201.64 10.0.0.63 any log-input
access-list 197 deny ip 192.168.201.128 10.0.0.63 any log-input
access-list 197 permit ip 192.168.201.192 10.0.0.63 any log-input
access-list 197 deny ip host 10.0.0.10 any log-input
access-list 197 deny ip 172.31.0.0 255.255.255.255 any log-input
access-list 197 deny ip 10.0.0.0 255.255.255.255 any log-input
access-list 197 deny ip 172.16.0.0 255.255.255.255 any log-input
access-list 197 deny ip 192.168.0.0 255.255.255.255 any log-input
```

Related Commands

Command	Description
ip cef	Enables CEF on the route processor card.

■ ip verify unicast reverse-path