



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.

History for the Unicast Reverse Path Forwarding Loose Mode Feature

Release	Modification
12.0(15)S	This feature was introduced.
12.1(8a)E	This feature was integrated into Cisco IOS Release 12.1(8a)E.
12.2(13)T	This feature was integrated into Cisco IOS Release 12.2(13)T.

Finding Support Information for Platforms and Cisco IOS Software Images

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

Contents

- [Prerequisites for Unicast Reverse Path Forwarding Loose Mode, page 2](#)
- [Information About Unicast Reverse Path Forwarding Loose Mode, page 2](#)
- [How to Configure Unicast Reverse Path Forwarding Loose Mode, page 3](#)
- [Configuration Examples for Unicast Reverse Path Forwarding Loose Mode, page 5](#)
- [Additional References, page 6](#)
- [Command Reference, page 7](#)



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

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

Prerequisites for Unicast Reverse Path Forwarding 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 Reverse Path Forwarding Loose Mode

Before configuring Unicast Reverse Path Forwarding Loose Check, you should understand the following concepts:

- [Unicast Reverse Path Forwarding: Background, page 2](#)
- [Loose Mode, page 3](#)

Unicast Reverse Path Forwarding: 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 Reverse Path Forwarding Loose Mode

This section contains the following procedure:

- [Configuring Unicast Reverse Path Forwarding Loose Mode, page 3](#)

Configuring Unicast Reverse Path Forwarding 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	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: Router# configure terminal	Enters global configuration mode.
Step 3	<code>ip cef</code> Example: Router (config)# ip cef	Enables CEF on the route processor card.
Step 4	<code>interface type slot/port-adapter/port</code> Example: Router (config)# interface serial5/0/0	Configures an interface type and enters interface configuration mode.
Step 5	<code>ip verify unicast source reachable-via any</code> Router (config-if)# ip verify unicast source reachable-via any	Enables Unicast RPF using loose mode.

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 Reverse Path Forwarding Loose Mode

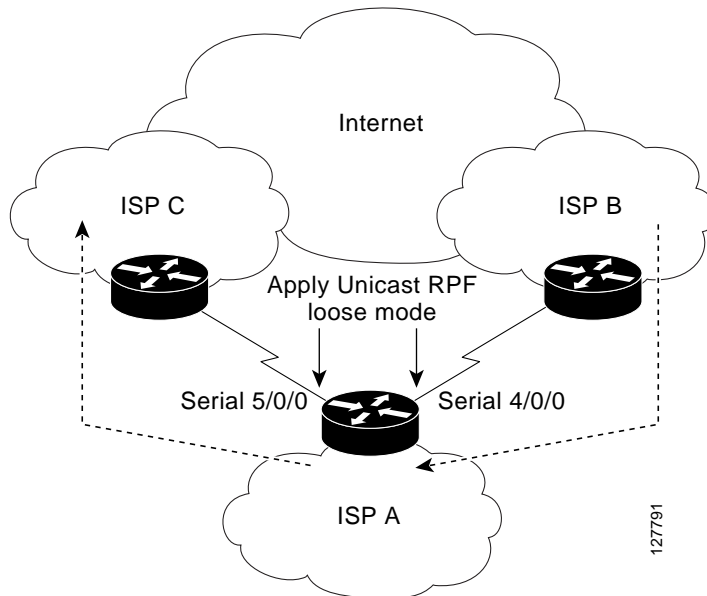
This section includes the following configuration example:

- [Configuring Unicast RPF Using Loose Mode: Example, page 5](#)

Configuring Unicast RPF Using Loose Mode: Example

The following example (see [Figure 1](#)) 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 1 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

The following sections provide references related to Unicast Reverse Path Forwarding Loose Check.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Command Reference , Release 12.3T
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 Technical Support website contains thousands of pages of searchable content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log on from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents new and replaced commands only.

New

- [ip verify unicast source reachable-via](#)

Replaced

- [ip verify unicast reverse-path](#)

ip verify unicast reverse-path



Note

This command was replaced by the **ip verify unicast source reachable-via** command effective with Cisco IOS Release 12.0(15)S. The **ip verify unicast source reachable-via** command allows for more flexibility and functionality, such as supporting asymmetric routing, and should be used for any Reverse Path Forwarding (RPF) implementation.

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 [*list*]

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

Syntax Description	<i>list</i>
	(Optional) Specifies a numbered access control list (ACL) in the following ranges: <ul style="list-style-type: none"> • 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

CommandHistory	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.
	12.0(15) S	The ip verify unicast source reachable-via command replaced this command, and the following keywords were added: allow-default , allow-self-ping , rx , and any .
	12.1(8a)E	The ip verify unicast source reachable-via command was integrated into Cisco IOS Release 12.1(8a)E.
	12.2(13)T	The ip verify unicast source reachable-via command was integrated into Cisco IOS Release 12.2(13)T.
	12.2(14)S	The ip verify unicast source reachable-via command was integrated into Cisco IOS Release 12.2(14)S.

Usage Guidelines

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

When Unicast RPF is enabled on an interface, the router examines all packets that are received on that interface. The router checks to ensure that the source address appears in the Forwarding Information Base (FIB) and that it 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 FIB. CEF generates the FIB as part of its operation.

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. If 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.



Note

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

The Unicast Reverse Path Forwarding feature checks to determine whether any packet that is received at a router interface arrives on one of the best return paths to the source of the packet. 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 determine whether the packet should be dropped (using a deny statement in the ACL) or forwarded (using a permit statement in the ACL). Whether a packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for Unicast RPF drops and in the interface statistics for Unicast RPF.

If no ACL is specified in the Unicast 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.

Where to Use RPF in Your Network

Unicast RPF may be used on interfaces in which only one path allows packets from valid source networks (networks contained in the FIB). Unicast RPF may also be used in cases for which a router has multiple paths to a given network, as long as the valid networks are switched via the incoming interfaces. Packets for invalid networks will be dropped. For example, routers at the edge of the network of an Internet Service Provider (ISP) are likely to have symmetrical reverse paths. Unicast RPF may still be applicable in certain multi-homed situations, provided that optional Border Gateway Protocol (BGP) attributes such as weight and local preference are used to achieve symmetric routing.

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.

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. In this scenario, you should use the new form of the command, **ip verify unicast source reachable-via**, if there is a chance of asymmetrical routing.

Examples

The following example shows that the Unicast Reverse Path Forwarding feature has been enabled 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 192.165.202.128/28 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 192.165.200.225 255.255.255.252
 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 192.165.202.128 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 172.0.0.0 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
```

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

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

```
ip cef distributed
!
int eth0/1/1
 ip address 192.168.200.1 255.255.255.0
```

```
ip verify unicast 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-input
access-list 197 deny ip 172.0.0.0 0.255.255.255 any log-input
access-list 197 deny ip 10.0.0.0 0.255.255.255 any log-input
access-list 197 deny ip 172.16.0.0 0.15.255.255 any log-input
access-list 197 deny ip 192.168.0.0 0.0.255.255 any log-input
```

Related Commands

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

ip verify unicast source reachable-via

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

ip verify unicast source reachable-via { *rx* | **any** } [**allow-default**] [**allow-self-ping**] [*list*]

no ip verify unicast source reachable-via

Syntax Description		
	<i>list</i>	(Optional) Specifies a numbered access control list (ACL) in the following ranges: <ul style="list-style-type: none"> • 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)
	rx	Examines incoming packets to determine whether the source address is in the Forwarding Information Base (FIB) and permits the packet only if the source is reachable through the interface on which the packet was received (sometimes referred to as strict mode).
	any	Examines incoming packets to determine whether the source address is in the FIB and permits the packet if the source is reachable through any interface (sometimes referred to as loose mode).
	allow-default	(Optional) Allows the use of the default route for RPF verification.
	allow-self-ping	(Optional) Allows a router to ping its own interface. Use with caution, because when implemented, this keyword enables a denial-of-service (DoS) hole.

Defaults Unicast RPF is disabled.

Command Modes Interface configuration

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.
	12.0(15) S	This command replaced the ip verify unicast reverse-path command, and the following keywords were added: allow-default , allow-self-ping , rx , and any .
	12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.

Release	Modification
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Usage Guidelines

Use the **ip verify unicast source reachable-via** interface command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through a router. Malformed or forged source addresses can indicate DoS attacks on the basis of source IP address spoofing.

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



Note

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

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.



Note

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

The Unicast Reverse Path Forwarding feature checks to determine whether any packet that is received at a router interface arrives on one of the best return paths to the source of the packet. The feature does this checking 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, when (and only when) a packet fails the Unicast RPF check, the ACL is checked to determine whether the packet should be dropped (using a deny statement in the ACL) or forwarded (using a permit statement in the ACL). Whether a packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for Unicast RPF drops and in the interface statistics for Unicast RPF.

If no ACL is specified in the **ip verify unicast source reachable-via** command, the router drops the forged or malformed packet immediately and no ACL logging occurs. The router and interface Unicast RPF counters are updated.

Unicast RPF events can be logged by specifying the logging option for the ACL entries that are used by the **ip verify unicast source reachable-via** command. Log information can be used to gather information about the attack, such as source address, time, and so on.

Strict Mode RPF

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

Exists-Only (or Loose Mode) RPF

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

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

allow-default

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

allow-self-ping

This Unicast RPF optional keyword setting allows the router to ping its own interface(s). Without this option, ping packets generated by the router fail the RPF verification check and, thus, self-pinging is not allowed. You must specify the **allow-self-ping** keyword in the command to enable self-pinging. Caution should be used when enabling this feature because this option opens a potential DoS hole.

Where to Use RPF in Your Network

Unicast RPF strict mode may be used on interfaces in which only one path allows packets from valid source networks (networks contained in the FIB). Unicast RPF strict mode may also be used in cases for which a router has multiple paths to a given network, as long as the valid networks are switched via the incoming interfaces. Packets for invalid networks will be dropped. For example, routers at the edge of the network of an ISP are likely to have symmetrical reverse paths. Unicast RPF strict mode may still be applicable in certain multihomed situations, provided that optional Border Gateway Protocol (BGP) attributes, such as weight and local preference, are used to achieve symmetric routing.

**Note**

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

Unicast RPF loose mode may be used on interfaces in which asymmetric paths allow packets from valid source networks (networks contained in the FIB). Routers that are in the core of the ISP network have no guarantee that the best forwarding path out of the router will be the path selected for packets returning to the router.

Examples

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

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

Related Commands

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

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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