



Unicast Reverse Path Forwarding Loose Mode

Last Updated: November 25, 2012

The Unicast Reverse Path Forwarding Loose Mode feature creates a new option for Unicast Reverse Path Forwarding (Unicast RPF), providing a scalable antispoofing mechanism suitable for use in multihome network scenarios. This mechanism is especially relevant for ISPs, specifically on devices that have multiple links to multiple ISPs.

This module describes the Unicast Reverse Path Forwarding Loose Mode feature.

- [Finding Feature Information, page 1](#)
- [Prerequisites for Unicast RPF Loose Mode, page 1](#)
- [Information About Unicast RPF Loose Mode, page 2](#)
- [How to Configure Unicast RPF Loose Mode, page 3](#)
- [Configuration Examples for Unicast RPF Loose Mode, page 5](#)
- [Additional References for Unicast RPF Loose Mode, page 6](#)
- [Feature Information for Unicast RPF Loose Mode, page 6](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 module.

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 Reverse Path Forwarding (Unicast RPF), you must enable Cisco Express Forwarding switching or distributed Cisco Express Forwarding switching on the device. There is no need to configure the input interface for Cisco Express Forwarding switching. As long as Cisco Express Forwarding is running on the device, individual interfaces can be configured for other switching modes.



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

Information About Unicast RPF Loose Mode

- [Unicast RPF Overview, page 2](#)
- [Unicast RPF Loose Mode, page 2](#)

Unicast RPF Overview

Unicast Reverse Path Forwarding (Unicast RPF) helps mitigate denial of service (DoS) attacks by providing an automated, scalable mechanism that implements the IETF Best Common Practices 38/RFC 2827 (BCP 38/RFC 2827) antispoofing filtering on the customer-to-ISP network edge.

Unicast RPF loose mode is especially relevant for ISPs, specifically on devices 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 DoS and distributed DoS attacks.

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 takes advantage of the information stored in the Forwarding Information Base (FIB) that is created by the Cisco Express Forwarding switching process to determine whether IP packets are spoofed or malformed by matching the IP source address and the 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 out of the same interface are forwarded as normal. If no reverse path route is on the same interface from which the packet was received, it might indicate that the source address was modified, and the packet is dropped by default.

With Unicast RPF, all equal-cost “best” return paths are considered valid, indicating that Unicast RPF 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 used and unequal candidate paths back to the source IP address exist. This original implementation of Unicast RPF, known as “strict mode,” required a match between the ingress interface and the reverse path FIB entry. 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 (an ISP device “peered” with another ISP device) network edges use multihomed configurations in which routing asymmetry is typical. When traffic flows are asymmetrical, 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, Unicast RPF’s strict mode was not used by ISPs on their core devices and ISP-to-ISP links. In asymmetric routing, a packet traverses from a source to a destination in one path and takes a different path when it returns to the source.

With an increase in distributed DoS attacks on the Internet, the Unicast RPF functionality was reviewed as a tool that ISPs can use on the ISP-to-ISP network edge to enable dynamic BGP and 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 device so that asymmetrical routing is not a problem.

Unicast RPF Loose Mode

To provide ISPs with a distributed denial of service (DoS) resistance tool on the ISP-to-ISP edge of a network, Unicast Reverse Path Forwarding (Unicast RPF) was modified from strict mode implementation

to check 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:

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

Loose mode removes the match requirement on the specific ingress interface, allowing Unicast RPF to loose-check packets. This packet checking allows the “peering” device of an ISP that has multiple links to multiple ISPs to check the source IP address of ingress packets to determine whether packets exist in the Forwarding Information Base (FIB). If packets exist in the FIB, packets are forwarded. If they do not exist in the FIB, the packets are dropped. This packet checking increases the resistance against DoS and distributed DoS attacks that use spoofed source addresses and unallocated IP addresses.

How to Configure Unicast RPF Loose Mode

- [Configuring Unicast RPF Loose Mode, page 3](#)

Configuring Unicast RPF Loose Mode

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip verify unicast source reachable-via any**
5. **end**

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 configure terminal Example: Device# configure terminal	Enters global configuration mode.

Command or Action	Purpose
Step 3 <code>interface type number</code> Example: <pre>Device(config)# interface serial 5/0/0</pre>	Configures an interface and enters interface configuration mode.
Step 4 <code>ip verify unicast source reachable-via any</code> Example: <pre>Device(config-if)# ip verify unicast source reachable- via any</pre>	Enables Unicast RPF using loose mode.
Step 5 <code>end</code> Example: <pre>Device(config-if)# end</pre>	Exits interface configuration mode and enters privileged EXEC mode.

- [Troubleshooting Tips, page 4](#)

Troubleshooting Tips

Dropped Packets

If the network administrator believes that Unicast Reverse Path Forwarding (Unicast RPF) is dropping packets that are deemed valid, you must 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:

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

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

```
Device# show ip interface serial 5/0/0 | include verif
```

The **show ip interface** 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 that is used to identify traffic types and add it to the Unicast RPF configuration on the interface or interfaces that are in question.

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

- Use the following command to apply the above configured access list to Unicast RPF on the interface in question:

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

- Use the following **show** command to periodically check the counters in the above access list:

```
Device# 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.

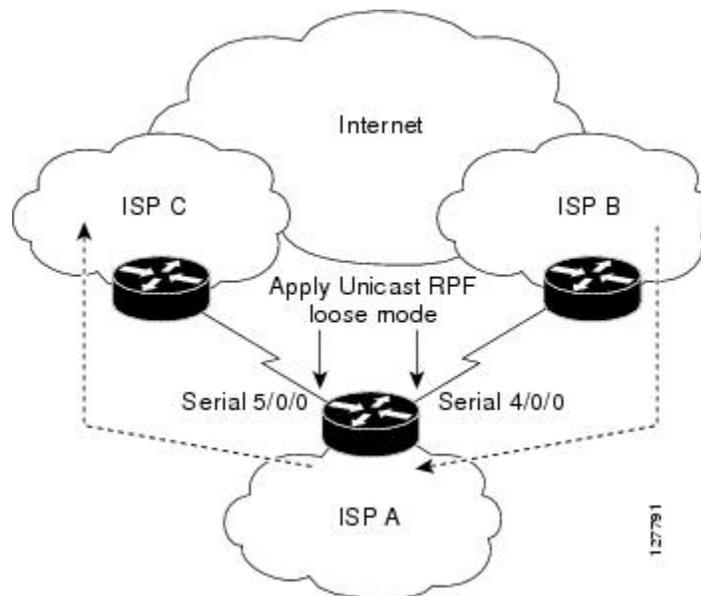
Configuration Examples for Unicast RPF Loose Mode

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

Example: Configuring Unicast RPF 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 device that is connected to two different upstream ISPs (B and C) and shows that traffic that flows into and out of ISP A can be asymmetric given this dual-homed configuration. Hence, provisions for asymmetric 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 Serial 4/0/0
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 Serial 5/0/0
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 for Unicast RPF Loose Mode

Related Documents

Related Topic	Document Title
Cisco IOS commands	<i>Cisco IOS Master Command List, All Releases</i>
Security commands	<ul style="list-style-type: none"> • <i>Cisco IOS Security Command Reference: Commands A to C</i> • <i>Cisco IOS Security Command Reference: Commands D to L</i> • <i>Cisco IOS Security Command Reference: Commands M to R</i> • <i>Cisco IOS Security Command Reference: Commands S to Z</i>
Best practices using Unicast RPF	<i>ISP Security Bootcamp/Best Practices—CPN-Summit-2004/Paris-Sept-04</i>

Standards and RFCs

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

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 1 **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	<p>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.</p> <p>The following commands were introduced or modified: ip verify unicast reverse-path, ip verify unicast source reachable-via.</p>

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental. © 2009 Cisco Systems, Inc. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned 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. (1110R)

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

© 2012 Cisco Systems, Inc. All rights reserved.