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, page 1
- Prerequisites for Unicast RPF Loose Mode, page 2
- 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, 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.

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.

	Command or Action	Purpose
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.
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

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.

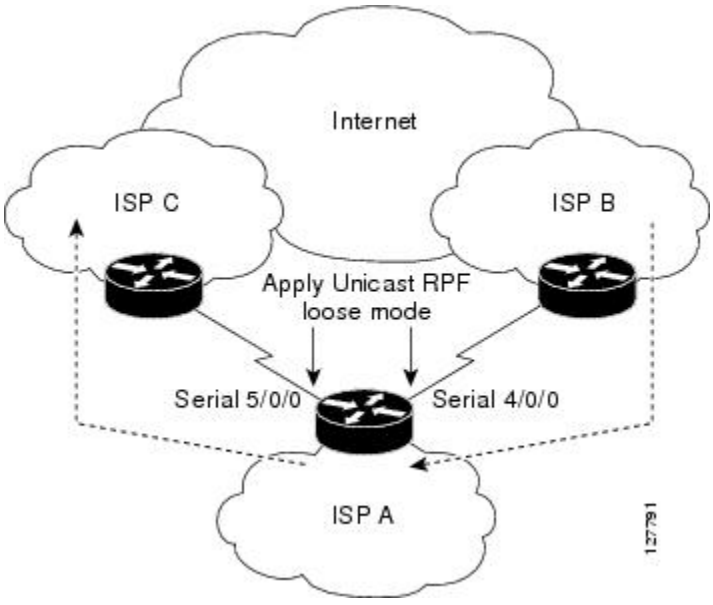
- Use the following command to apply the above configured access list to Unicast RPF on the interface in question:
  ```
  Device(config-if)# ip verify unicast source reachable-via any 199
  ```
- Use the following **show** command to periodically check the counters in the above access list:
  ```
  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 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 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

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	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**.