



Security Configuration Guide: Unicast Reverse Path Forwarding, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. 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. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Unicast Reverse Path Forwarding Strict Mode 1

- Prerequisites for Unicast Reverse Path Forwarding 1
- Restrictions for Unicast Reverse Path Forwarding 2
- Information About Unicast Reverse Path Forwarding 2
 - Overview of Unicast Reverse Path Forwarding 2
 - Unicast RPF Operation 2
 - Per-Interface Statistics 3
 - Rules for Implementing Unicast RPF 5
 - Security Policy and Unicast RPF 6
 - Ingress and Egress Filtering Policy for Unicast RPF 6
 - Where to Use Unicast RPF 6
 - Routing Table Requirements 9
 - Where Not to Use Unicast RPF 9
 - Unicast RPF with BOOTP and DHCP 10
 - How to Configure Unicast Reverse Path Forwarding 10
 - Configuring Unicast RPF 10
 - Troubleshooting Tips 12
 - Configuration Examples for Unicast Reverse Path Forwarding 12
 - Example: Configuring Unicast RPF 12
 - Additional References 13
 - Feature Information for Unicast Reverse Path Forwarding 13

CHAPTER 2

Unicast Reverse Path Forwarding for IPv6 15

- Prerequisites for Unicast Reverse Path Forwarding for IPv6 15
- Information About Unicast Reverse Path Forwarding for IPv6 16
 - Unicast Reverse Path Forwarding 16

How to Configure Unicast Reverse Path Forwarding for IPv6	16
Configuring Unicast RPF	16
Configuration Examples for Unicast Reverse Path Forwarding for IPv6	18
Example: Configuring Unicast Reverse Path Forwarding for IPv6	18
Additional References	18
Feature Information for Unicast Reverse Path Forwarding for IPv6	19



CHAPTER 1

Unicast Reverse Path Forwarding Strict Mode

The Unicast Reverse Path Forwarding feature limits the malicious traffic on a network. This feature enables devices to verify the reachability of the source address in packets that are being forwarded and limit the appearance of spoofed or malformed addresses on a network. If the source IP address is not valid, Unicast Reverse Path Forwarding (RPF) discards the packet.

This module describes the Unicast Reverse Path Forwarding feature.

- [Prerequisites for Unicast Reverse Path Forwarding, on page 1](#)
- [Restrictions for Unicast Reverse Path Forwarding, on page 2](#)
- [Information About Unicast Reverse Path Forwarding, on page 2](#)
- [How to Configure Unicast Reverse Path Forwarding, on page 10](#)
- [Configuration Examples for Unicast Reverse Path Forwarding, on page 12](#)
- [Additional References, on page 13](#)
- [Feature Information for Unicast Reverse Path Forwarding, on page 13](#)

Prerequisites for Unicast Reverse Path Forwarding

- Unicast Reverse Path Forwarding (RPF) requires Cisco Express Forwarding to function properly on a device.
- Prior to configuring Unicast RPF, you must configure the following access control lists (ACLs):
 - Configure standard or extended ACL to mitigate the transmission of invalid IP addresses (by performing egress filtering). Configuring standard or extended ACLs permit only valid source addresses to leave your network and enter the Internet.
 - Configure standard or extended ACL entries to drop (deny) packets that have invalid source IP addresses (by performing ingress filtering). Invalid source IP addresses include the following types:
 - Broadcast addresses (including multicast addresses)
 - Loopback addresses
 - Private addresses (RFC 1918, *Address Allocation for Private Internets*)
 - Reserved addresses
 - Source addresses that fall outside the range of valid addresses that are associated with the protected network

Restrictions for Unicast Reverse Path Forwarding

- Unicast RPF does not support access control list (ACL) templates.

The following basic restrictions apply to multihomed clients:

- Clients should not be multihomed on the same device because multihoming defeats the purpose of creating a redundant service for a client.
- Ensure that packets that flow up the link (out to the Internet) match the route advertised out of the link. Otherwise, Unicast RPF filters these packets as malformed packets.

Information About Unicast Reverse Path Forwarding

Overview of Unicast Reverse Path Forwarding

The Unicast Reverse Path Forwarding 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 verifiable IP source addresses. 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 these attacks. For 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, thereby protecting the network of the ISP, ISP customers, and the Internet.

Unicast RPF Operation

When Unicast RPF is enabled on an interface of a device, the device examines all packets received as input on that interface to ensure that the source address and source interface information appears in the routing table and matches the interface on which packets are received. This ability to “look backwards” is available only when Cisco Express Forwarding is enabled on a device because the lookup relies on the presence of a Forwarding Information Base (FIB). Cisco Express Forwarding generates a FIB as part of its operation.

**Note**

Unicast RPF is an input function and is applied only on the input interface of a device at the upstream end of a connection.

Unicast RPF does a reverse lookup in the Cisco Express Forwarding table to check if any packet received at the interface of a device arrives on the best return path (or return route) to the source of the packet. If the packet was received from one of the best reverse path routes, the packet is forwarded as normal. No reverse path route on the interface from which the packet was received can mean that the source address was modified.



Note With Unicast RPF, all equal-cost “best” return paths are considered valid. Unicast RPF supports multiple return paths, provided that each path is equal to the others in terms of the routing cost (such as number of hops, weights, and so on) and the route is available in the FIB. Unicast RPF also functions where Enhanced Interior Gateway Routing Protocol (EIGRP) variants are used.

Before forwarding a packet that is received at the interface on which Unicast RPF and ACLs have been configured, Unicast RPF does the following checks:

1. If input ACLs are configured on the inbound interface.
2. If the packet has arrived on the best return path to the source by doing a reverse lookup in the FIB table.
3. Does a lookup of the Cisco Express Forwarding table for packet forwarding.
4. Checks output ACLs on the outbound interface.
5. Forwards the packet.

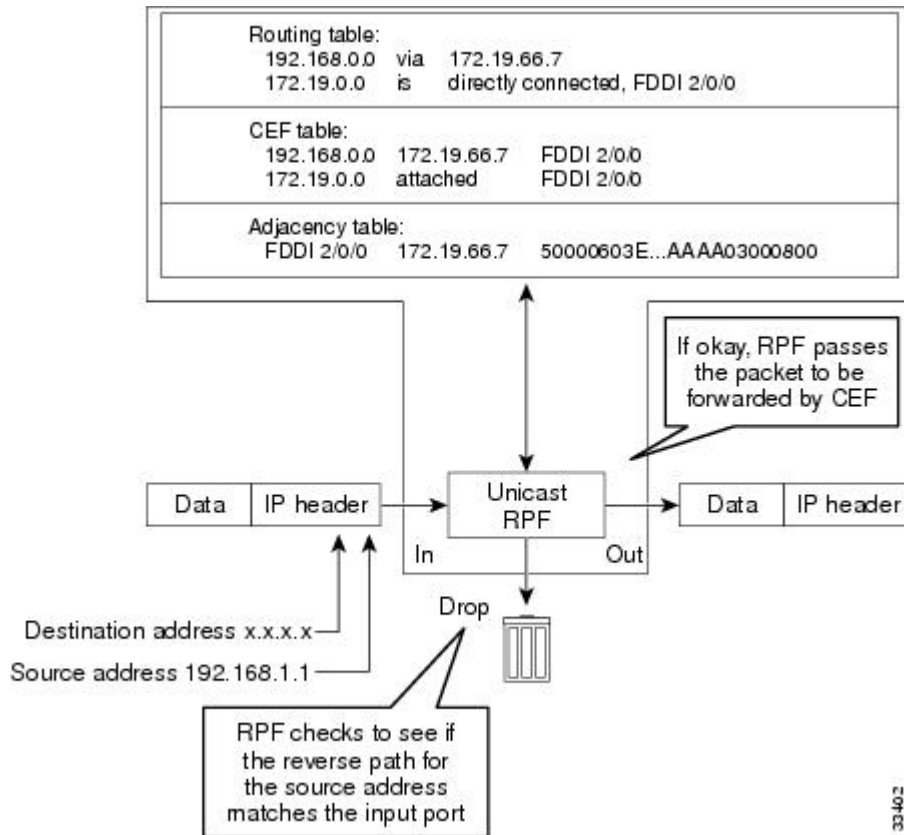
Per-Interface Statistics

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 take steps to isolate the attack at a specific interface.

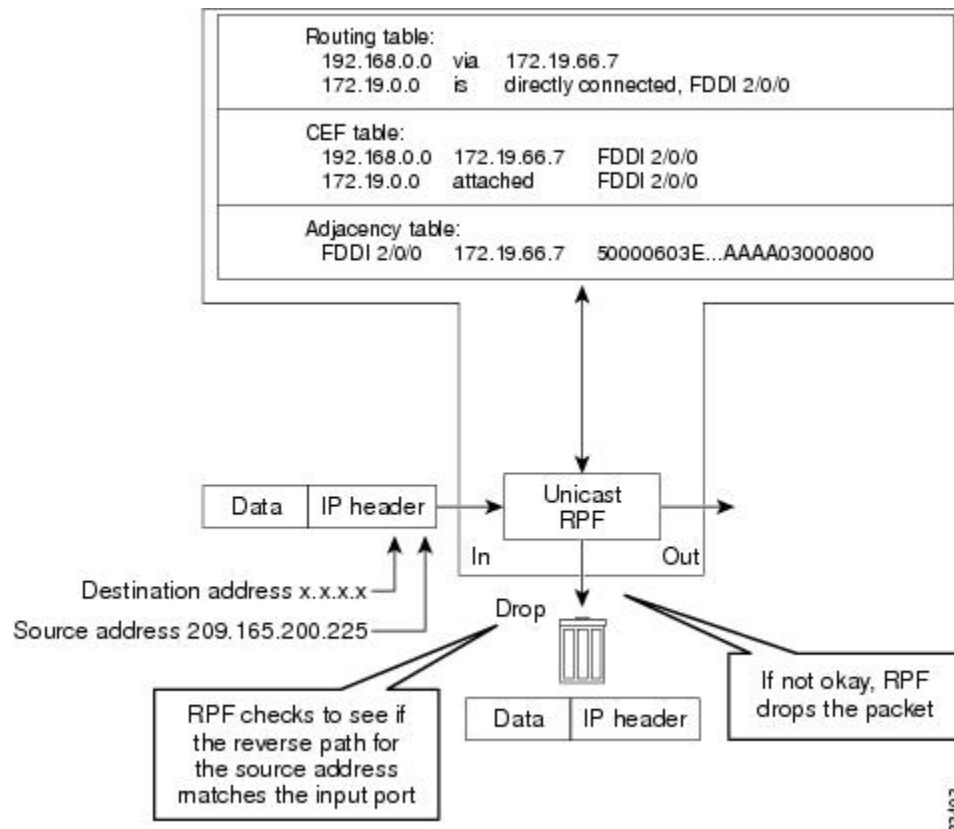
The figure below illustrates how Unicast RPF and CEF work together to validate IP source addresses by verifying packet return paths. In this example, a customer has sent a packet having a source address of 192.168.1.1 from interface FDDI 2/0/0. Unicast RPF checks the FIB to see if 192.168.1.1 has a path 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



Rules for Implementing Unicast RPF

The following rules apply when implementing Unicast Reverse Path Forwarding (RPF):

- Packets must be received at an interface that has the best return path (route) to the packets' source. This process is called symmetric routing. A route in the Forwarding Information Base (FIB) must match the route to the receiving interface. Add a route in the FIB through dynamic or static routing or by using a network statement.
- IP source addresses at the receiving interface must match the routing entry for the interface.
- Unicast RPF is an input function and can be applied at the input interface of a device at the upstream end of a connection.

Network administrators can use Unicast RPF for their customers and also for their downstream network or ISP, even if the downstream network or ISP has other connections to the Internet.



Caution

Using optional Border Gateway Protocol (BGP) attributes, such as weight and local preference, the best path back to source addresses can be modified. The best path modification will affect the operation of Unicast RPF.

The following sections provides information about the implementation of Unicast RPF:

Security Policy and Unicast RPF

When determining how to deploy Unicast Reverse Path Forwarding (RPF), consider the following points:

- Apply Unicast RPF at the downstream interface, away from the larger portion of the network, preferably at the edges of your network. The further you apply Unicast RPF, the finer the granularity you have in mitigating address spoofing and in identifying sources of spoofed addresses. For example, applying Unicast RPF on an aggregation device helps to mitigate attacks from many downstream networks or clients and is simple to administer, but Unicast RPF does not help in identifying the source of the attack. Applying Unicast RPF at the network access server helps to limit the scope of the attack and trace the source of the attack. However, deploying Unicast RPF across many sites adds to the administration cost of operating a network.
- When you deploy Unicast RPF on many entities on a network (for example, across the Internet, intranet, and extranet resources), you have better chances of mitigating large-scale network disruptions throughout the Internet community, and of tracing the source of an attack.
- Unicast RPF does not inspect IP packets that are encapsulated in tunnels, such as the generic routing encapsulation (GRE), Layer 2 Tunneling Protocol (L2TP), or Point-to-Point Tunneling Protocol (PPTP). Configure Unicast RPF on a home gateway so that Unicast RPF processes network traffic only after tunneling and encryption layers are stripped off from the packets.

Ingress and Egress Filtering Policy for Unicast RPF

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

Ingress filtering applies filters to traffic that is 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 or private or broadcast addresses are dropped. For example, in ISP environments, ingress filtering can be applied to traffic that is received at a device from either a client (customer) or the Internet.

Egress filtering applies filters to the traffic that exits a network interface (the sending interface). By filtering packets on devices 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, *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*.

Where to Use Unicast RPF

Unicast Reverse Path Forwarding (RPF) can be used in any “single-homed” environment where there is essentially only one access point out of the network, which means that there is only one upstream connection to the network. 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 describe two sample network environments in which Unicast RPF is implemented:

Enterprise Networks with a Single Connection to an ISP

In enterprise networks, you can use Unicast Reverse Path Forwarding (RPF) to filter traffic at the input interface (a process called ingress filtering) to protect from malformed packets that arrive from the Internet.

Traditionally, local networks that have one connection to the Internet use access control lists (ACLs) at the receiving interface to prevent spoofed packets from entering their local network.

ACLs work well for single-homed customers. However, when ACLs are used as ingress filters, the following two commonly referenced limitations apply:

- Packet-per-second (PPS) performance at very high packet rates
- ACL maintenance (whenever there are new addresses added to the network)

Unicast RPF addresses both the limitations described above. With Unicast RPF, ingress filtering is done at Cisco Express Forwarding PPS rates. Because Unicast RPF uses the Forwarding Information Base (FIB), ACL maintenance is not required, 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 GigabitEthernet interface 1/0/2 on the enterprise device for protection from malformed packets arriving from the Internet. Unicast RPF is also applied at GigabitEthernet interface 1/0/2 on the ISP device for protection from malformed packets arriving from the enterprise network.

Figure 3: Enterprise Network Using Unicast RPF for Ingress Filtering



A typical configuration on an ISP device that uses the topography in the figure above would be as follows:

```
ip cef
interface loopback 0
  description Loopback interface on Gateway Device 2
  ip address 192.168.3.1 255.255.255.255
  no ip redirects
  no ip directed-broadcast
  no ip proxy-arp
!
interface GigabitEthernet 1/0/2
  description 128K HDLC link to ExampleCorp WT50314E R5-0
  bandwidth 128
  ip unnumbered loopback 0

  no ip redirects
  no ip directed-broadcast
  no ip proxy-arp
!
ip route 192.168.10.0 255.255.252.0 GigabitEthernet 1/0/2
```

The gateway device configuration of the enterprise network will be similar to the following:

```
ip cef
interface FastEthernet 0/0/0
  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 GigabitEthernet 1/0/2
```

```
description 128K HDLC link to ExampleCorp Internet Inc WT50314E C0
bandwidth 128
ip unnumbered FastEthernet 0/0/0

no ip redirects
no ip directed-broadcast
no ip proxy-arp
!
ip route 0.0.0.0 0.0.0.0 GigabitEthernet 1/0/2
```

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 network 192.168.10.0/22 will be dropped by Unicast RPF.

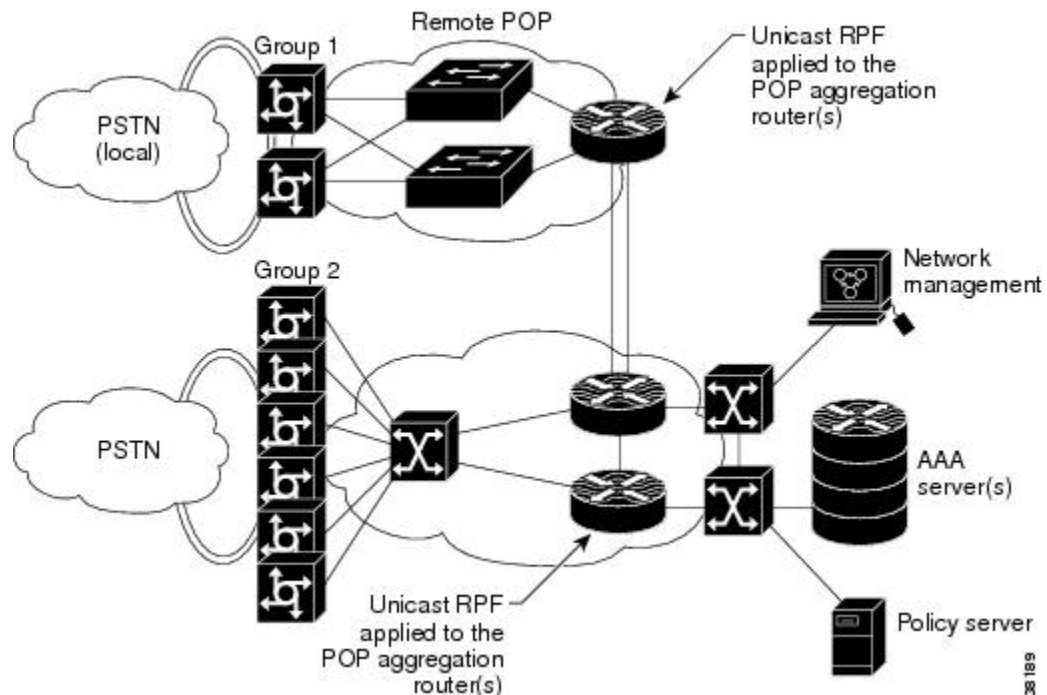
Applying Unicast RPF to Network Access Servers

If a network access server supports Cisco Express Forwarding, Unicast RPF will work on that network. A network access server (NAS) allows users to access a network by checking the credentials of the users accessing the network. Aggregation devices support Unicast RPF with single-homed clients. Unicast RPF works well on leased lines or on a digital subscriber line (DSL), ISDN, or public switched telephone network (PSTN) customer connections that are connected to the Internet. Dialup connections are a big source of denial of service (Dos) attacks that use forged IP addresses.

Aggregation devices need routing prefixes information (IP address block) for routing traffic. In the topology described below, aggregation devices do not have a full Internet routing table, and as a result, Unicast RPF uses the information configured or redistributed by the Interior Gateway Protocol (IGP) or Internal Border Gateway Protocol (IBGP) (based on how customer routes are added to the network) to route traffic. Unicast RPF is applied upstream on the customer dialup connection device that is on the receiving (input) interfaces of ISP aggregation devices.

The figure below illustrates how Unicast RPF is applied to aggregation and access devices for an ISP or point of presence (PoP) with ISP devices providing dialup connections.

Figure 4: Unicast RPF Applied to PSTN/ISDN Customer Connections



Routing Table Requirements

Unicast Reverse Path Forwarding (RPF) uses the routing information in Cisco Express Forwarding tables for routing traffic. The amount of routing information that must be available in Cisco Express Forwarding tables depends on the device where Unicast RPF is configured and the functions the device performs in the network. For example, in an ISP environment where a device is a leased-line aggregation device for customers, the information about static routes that are redistributed into the Interior Gateway Protocol (IGP) or Internal Border Gateway Protocol (IBGP) (depending on which technique is used in the network) is required in the routing table. Because Unicast RPF is configured on customer interfaces, only minimal routing information is required. If a single-homed ISP configures Unicast RPF on the gateway to the Internet, the full Internet routing table information is required by Unicast RPF to help protect the ISP from external denial of service (DoS) attacks that use addresses that are not in the Internet routing table.

Where Not to Use Unicast RPF

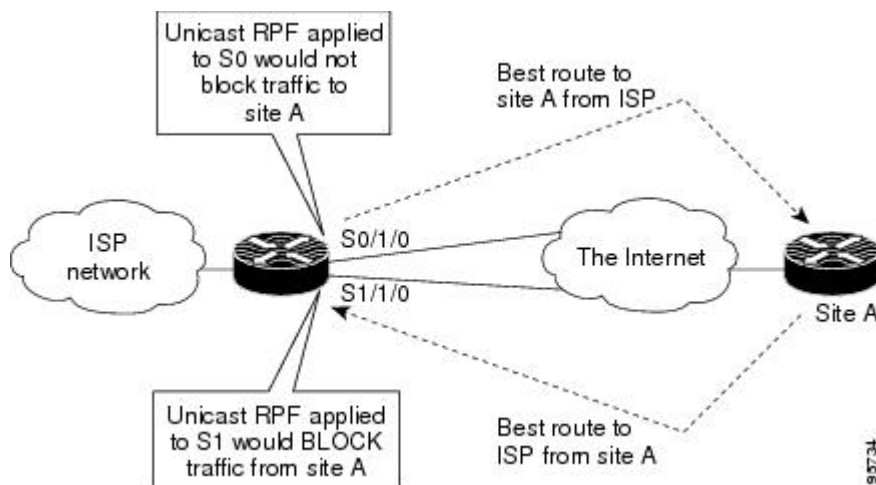
Do not use Unicast Reverse Path Forwarding (RPF) on interfaces that are internal to a network. Internal interfaces are likely to have routing asymmetry (see the figure below), which means that there can be multiple routes to the source of a packet. Unicast RPF is applied only where there is a natural or configured symmetry.

For example, devices at the edge of an ISP network are more likely to have symmetrical reverse paths than devices that are in the core of an ISP network. The best forwarding path to forward packets from devices that are at the core of an ISP network may not be the best forwarding path that is selected for packets that are returned to the device.

We recommend that you do not apply Unicast RPF where there is a chance of asymmetric routing, unless you configure access control lists (ACLs) to allow the device to accept incoming packets. ACLs permit the use of Unicast RPF when packets arrive through specific, less-optimal asymmetric input paths.

The figure below illustrates how Unicast RPF can block legitimate traffic in an asymmetric routing environment.

Figure 5: Unicast RPF Blocking Legitimate Traffic in an Asymmetric Routing Environment



Unicast RPF with BOOTP and DHCP

Unicast RPF allows packets with 0.0.0.0 as the source IP address and 255.255.255.255 as the destination IP address to pass through a network to enable Bootstrap Protocol (BOOTP) and DHCP functions to work properly when Unicast RPF is configured.

How to Configure Unicast Reverse Path Forwarding

Configuring Unicast RPF

Before you begin

To use Unicast Reverse Path Forwarding, you must configure a device for Cisco Express Forwarding switching or distributed Cisco Express Forwarding switching. If Cisco Express Forwarding is not enabled globally on a device, Unicast RPF will not work on that device. If Cisco Express Forwarding is running on a device, individual interfaces on the device 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 Unicast RPF operates on IP packets that are received by the device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef distributed**
4. **interface slot/subslot/port**
5. **exit**
6. **end**
7. **show cef interface [type number]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip cef distributed Example: Device(config)# ip cef distributed	Enables Cisco Express Forwarding or distributed Cisco Express Forwarding on a device.
Step 4	interface slot/subslot/port Example: Device(config)# interface GigabitEthernet 0/0	Selects the input interface on which you want to apply Unicast Reverse Path Forwarding and enters interface configuration mode. • The interface that is configured is the receiving interface, which allows Unicast RPF to verify the best return path before forwarding a packet to the next destination.
Step 5	exit Example: Device(config-if)# exit	Exits interface configuration mode.
Step 6	end Example: Device(config-if)# end	Exits interface configuration mode and enters privileged EXEC mode.
Step 7	show cef interface [type number] Example: Device# show cef interface	Displays detailed Cisco Express Forwarding information for a specified interface or for all interfaces.

Example:

The following sample output from the **show cef interface** command shows that Unicast RPF is enabled on GigabitEthernet interface 1/0/2:

```
Device# show cef interface GigabitEthernet 1/0/2

GigabitEthernet 1/0/2 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 GigabitEthernet 1/0/2
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

HSRP Failure

The failure to disable Unicast RPF before disabling Cisco Express Forwarding can cause a Hot Standby Router Protocol (HSRP) failure. If you want to disable Cisco Express Forwarding on a device, you must first disable Unicast RPF.

Configuration Examples for Unicast Reverse Path Forwarding

Example: Configuring Unicast RPF

```

Device# configure terminal
Device(config)# ip cef distributed
Device(config)# interface GigabitEthernet 1/0/2
Device(config-if)# description Connection to Upstream ISP
Device(config-if)# ip address 209.165.200.225 255.255.255.252
Device(config-if)# no ip redirects
Device(config-if)# no ip directed-broadcast
Device(config-if)# no ip proxy-arp
Device(config-if)# ip verify unicast reverse-path

Device# configure terminal
Device(config)# ip cef distributed
Device(config)# interface GigabitEthernet 1/0/2
Device(config-if)# description Connection to Upstream ISP
Device(config-if)# ip address 209.165.200.225 255.255.255.252
Device(config-if)# no ip redirects
Device(config-if)# no ip directed-broadcast
Device(config-if)# no ip proxy-arp
Device(config-if)# ip verify unicast source reachable-via rx

```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Unicast RPF command descriptions	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z
Cisco Express Forwarding commands	Cisco IOS IP Switching Command Reference

Standards & RFCs

Standard/RFC	Title
RFC 1918	<i>Address Allocation for Private Internets</i>
RFC 2267	<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 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 Unicast Reverse Path Forwarding

Feature Name	Releases	Feature Information
Unicast Reverse Path Forwarding	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.3SE	The Unicast Reverse Path Forwarding feature limits the malicious traffic on a network. This feature enables devices to verify the reachability of the source address in packets that are being forwarded and limit the appearance of spoofed or malformed addresses on a network. If the source IP address is not valid, Unicast Reverse Path Forwarding (RPF) discards the packet. In Cisco IOS XE Release 3.3SE, this feature is supported on Cisco Catalyst 3850 Series Switches.



CHAPTER 2

Unicast Reverse Path Forwarding for IPv6

The Unicast Reverse Path Forwarding (uRPF) for IPv6 feature mitigates problems caused by malformed or forged (spoofed) IPv6 source addresses that pass through an IPv6 device.

- [Prerequisites for Unicast Reverse Path Forwarding for IPv6, on page 15](#)
- [Information About Unicast Reverse Path Forwarding for IPv6, on page 16](#)
- [How to Configure Unicast Reverse Path Forwarding for IPv6, on page 16](#)
- [Configuration Examples for Unicast Reverse Path Forwarding for IPv6, on page 18](#)
- [Additional References, on page 18](#)
- [Feature Information for Unicast Reverse Path Forwarding for IPv6, on page 19](#)

Prerequisites for Unicast Reverse Path Forwarding for IPv6

- Enable Cisco Express Forwarding switching or distributed Cisco Express Forwarding switching in 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 with other switching modes.
- Cisco Express Forwarding must be configured globally in the device. uRPF will not work without Cisco Express Forwarding.
- uRPF should not be used on interfaces that are internal to the network. Internal interfaces are likely to have routing asymmetry; this means that there are multiple routes to the source of a packet. uRPF should be applied only where there is natural or configured symmetry.

For example, devices at the edge of the network of an ISP are more likely to have symmetrical reverse paths than devices that are in the core of the ISP network. Devices that are in the core of the ISP network have no guarantee that the best forwarding path out of the device will be the path selected for packets returning to the device. Therefore, we do not recommend that you apply uRPF where there is a chance of asymmetric routing. Place uRPF only at the edge of a network or, for an ISP, at the customer edge of the network.

Information About Unicast Reverse Path Forwarding for IPv6

Unicast Reverse Path Forwarding

Use the Unicast Reverse Path Forwarding for IPv6 feature to mitigate problems caused by malformed or spoofed IPv6 source addresses that pass through an IPv6 device. Malformed or forged source addresses can indicate denial-of-service (DoS) attacks based on source IPv6 address spoofing.

When uRPF is enabled on an interface, the device examines all packets received on that interface. The device verifies that the source address appears in the routing table and matches the interface on which the packet was received. This "look backward" ability is available only when Cisco Express Forwarding is enabled on the device; this is because the lookup relies on the presence of the Forwarding Information Bases (FIBs). Cisco Express Forwarding generates the FIB as part of its operation.



Note uRPF is an input function and is applied only on the input interface of a device at the upstream end of a connection.



Note With uRPF, all equal-cost "best" return paths are considered valid. uRPF 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.

How to Configure Unicast Reverse Path Forwarding for IPv6

Configuring Unicast RPF

Before you begin

To use uRPF, enable Cisco Express Forwarding switching or distributed Cisco Express Forwarding switching in 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 with other switching modes.



Note Cisco Express Forwarding must be configured globally in the device. uRPF does not work without Cisco Express Forwarding.



Note uRPF 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. uRPF should be applied only where there is natural or configured symmetry.

For example, devices at the edge of the network of an ISP are more likely to have symmetrical reverse paths than devices that are in the core of the ISP network. Devices that are in the core of the ISP network have no guarantee that the best forwarding path out of the device will be the path selected for packets returning to the device. Therefore, we do not recommend that you apply uRPF where there is a chance of asymmetric routing. It is simplest to place uRPF only at the edge of a network or, for an ISP, at the customer edge of the network.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface type number**
4. **ipv6 verify unicast source reachable-via {rx | any} [allow-default]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	interface type number Example: <pre>Device(config)# interface GigabitEthernet 0/0</pre>	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	ipv6 verify unicast source reachable-via {rx any} [allow-default] Example: <pre>Device(config-if)# ipv6 verify unicast source reachable-via any</pre>	Verifies that a source address exists in the FIB table and enables uRPF. "rx" is for strict mode and "any" is for loose mode.

Configuration Examples for Unicast Reverse Path Forwarding for IPv6

Example: Configuring Unicast Reverse Path Forwarding for IPv6

```
Device# enable
Device# configure terminal
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# ipv6 verify unicast source reachable-via rx
```

Additional References

Related Documents

Related Topic	Document Title
Cisco Express Forwarding for IPv6	Implementing IPv6 Addressing and Basic Connectivity Guide, <i>IPv6 Configuration Guide</i>
Cisco IOS voice configuration	Cisco IOS Voice Configuration Library
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands, including voice commands	Cisco IOS IPv6 Command Reference
Cisco Unified Border Element configuration	Cisco Unified Border Element Configuration Guide
SIP Configuration Guide	SIP Configuration Guide
Troubleshooting and debugging guides	Cisco IOS Debug Command Reference Troubleshooting and Debugging VoIP Call Basics

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified 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

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 Reverse Path Forwarding for IPv6

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 Reverse Path Forwarding for IPv6

Feature Name	Releases	Feature Information
Unicast Reverse Path Forwarding for IPv6	Cisco IOS XE Release 3.3SE	Use the uRPF feature to mitigate problems caused by malformed or spoofed IPv6 source addresses that pass through an IPv6 device. Malformed or forged source addresses can indicate DoS attacks based on source IPv6 address spoofing. The following commands were introduced or modified: ipv6 verify unicast source reachable-via, show ipv6 traffic. In Cisco IOS XE Release 3.3SE, this feature is supported on Cisco Catalyst 3850 Series Switches.