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 1
- Restrictions for Unicast Reverse Path Forwarding for IPv6, on page 1
- Information About Unicast Reverse Path Forwarding for IPv6, on page 2
- How to Configure Unicast Reverse Path Forwarding for IPv6, on page 3
- Configuration Examples for Unicast Reverse Path Forwarding for IPv6, on page 4
- Additional References, on page 4

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.

Restrictions for Unicast Reverse Path Forwarding for IPv6

- If both IPv4 and IPv6 uRPF need to be enabled under a single VRF, then IPv4 uRPF enabled interfaces and IPv6 uRPF enabled interfaces in single VRF must be same. For example, within the same VRF, you

cannot enable IPv4 uRPF on one interface and IPv6 uRPF on other interface, but you can enable either IPv4 or IPv6 uRPF configuration in a VRF without any restrictions.

On each uRPF enabled interface in the VRF, there has to be either IPv4/ IPv6 uRPF or both IPv4 and IPv6 uRPF enabled or disabled. IPv4 / IPv6 uRPF mode on the interface can be same or different but a single uRPF mode for each interface type (IPv4/IPv6) for each VRF should be applied. So, we can have one IPv4 uRPF mode and another IPv6 uRPF mode for a single VRF.

- Only a single IPv6 uRPF mode is allowed on all the IPv6 interfaces in this VRF.
- IPv6 uRPF with the allow-self-ping option is *not* supported.
- If allow-default is configured on any IPv6 interface, it should be applied to all the IPv6 uRPF enabled interfaces on that VRF.
- IPv6 uRPF does not drop packets with the link-local address as the source.
- IPv6 uRPF drops packets with the source IP having Null0 route. This is applicable to all the modes.

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:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0`	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:** `Device(config-if)# ipv6 verify unicast source reachable-via any`	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

Additional References

Related Documents

Related Topic	Document Title
Cisco Express Forwarding for IPv6	Implementing IPv6 Addressing and Basic Connectivity Guide, *IPv6 Configuration Guide*
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*

Related Topic	Document Title
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