



## 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](#)
- [Information About Unicast Reverse Path Forwarding for IPv6, on page 2](#)
- [How to Configure Unicast Reverse Path Forwarding for IPv6, on page 2](#)
- [Configuration Examples for Unicast Reverse Path Forwarding for IPv6, on page 4](#)
- [Additional References, on page 4](#)
- [Feature Information for Unicast Reverse Path Forwarding for IPv6, on page 5](#)

## 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  |
|---------------|---|--|
| <b>Step 1</b> | <b>enable</b><br><b>Example:</b><br><pre>Device&gt; enable</pre>  | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>            |
| <b>Step 2</b> | <b>configure terminal</b><br><b>Example:</b><br><pre>Device# configure terminal</pre>   | Enters global configuration mode.  |
| <b>Step 3</b> | <b>interface type number</b><br><b>Example:</b><br><pre>Device(config)# interface GigabitEthernet 0/0</pre>   | Specifies an interface type and number, and places the device in interface configuration mode.                                   |
| <b>Step 4</b> | <b>ipv6 verify unicast source reachable-via {rx   any} [allow-default]</b><br><b>Example:</b><br><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.<br>"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, <i>IPv6 Configuration Guide</i>              |
| Cisco IOS voice configuration              | Cisco IOS Voice Configuration Library   |
| Cisco IOS commands                         | <a href="#">Cisco IOS Master Commands List, All Releases</a>  |
| IPv6 commands, including voice commands    | Cisco IOS IPv6 Command Reference  |
| Cisco Unified Border Element configuration | Cisco Unified Border Element Configuration Guide  |
| SIP Configuration Guide                    | <a href="#">SIP Configuration Guide</a>   |
| Troubleshooting and debugging guides       | Cisco IOS Debug Command Reference<br><br><a href="#">Troubleshooting and Debugging VoIP Call Basics</a> |

### 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:<br><br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

**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. | <a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a> |

## 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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 1: Feature Information for Unicast Reverse Path Forwarding for IPv6**

| Feature Name                             | Releases | Feature Information  |
|--|----------|--|
| Unicast Reverse Path Forwarding for IPv6 |          | <p>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.</p> <p>The following commands were introduced or modified: <b>ipv6 verify unicast source reachable-via</b>, <b>show ipv6 traffic</b>.</p> |

