

Configuring Unicast RPF (CLI Procedure)

Unicast reverse-path forwarding (RPF) can help protect your LAN from denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks on untrusted interfaces. Enabling unicast RPF on the switch interfaces filters traffic with source addresses that do not use the incoming interface as the best return path back to the source. When a packet comes into an interface, if that interface is not the best return path to the source, the switch discards the packet. If the incoming interface is the best return path to the source, the switch forwards the packet.



NOTE: On EX-series switches, you can only enable unicast RPF globally, on all switch interfaces. You cannot enable unicast RPF on a per-interface basis.

Before you begin:

- Ensure that all switch interfaces are symmetrically routed before you enable unicast RPF on an interface. A symmetrically routed interface is an interface that uses the same route in both directions between the source and the destination. When you enable unicast RPF on any interface, it is enabled globally on all switch interfaces. Do not enable unicast RPF on asymmetrically routed interfaces. An asymmetrically routed interface uses different paths to send and receive packets between the source and the destination.

To enable unicast RPF globally on all switch interfaces, you only need to configure it explicitly on one interface. However, you can configure it explicitly on every interface or only on some interfaces. Regardless of how many interfaces on which you explicitly enable unicast RPF, unicast RPF is implicitly enabled globally after you explicitly configure it on one interface.

We recommend that you enable unicast RPF explicitly on either all interfaces or only one interface, but that you do not enable it on only some interfaces:

- Enabling unicast RPF explicitly on only one interface makes it easier if you choose to disable it in the future because you must explicitly disable unicast RPF on every interface on which you explicitly enabled it. If you explicitly enable unicast RPF on two interfaces and you disable it on only one interface, unicast RPF is still implicitly enabled globally on the switch. The drawback to this approach is that the switch displays unicast RPF status as enabled only on interfaces on which unicast RPF is explicitly enabled, so even though unicast RPF is enabled on all interfaces, its status does not display as enabled on all interfaces.
- Enabling unicast RPF explicitly on all interfaces makes it easier to know if unicast RPF is enabled on the switch because every interface shows the correct status. (Only interfaces on which you explicitly enable unicast RPF display unicast RPF as enabled.) The drawback to this approach is that if you want to disable unicast RPF, you must explicitly disable it on every interface. If unicast RPF is enabled on any interface, it is implicitly enabled on all interfaces.

To enable unicast RPF to filter incoming traffic on all switch interfaces by enabling it on one interface:

[edit interfaces]

```
user@switch# set ge-1/0/10 unit 0 family inet rpf-check
```

- Related Topics**
- Example: Configuring Unicast RPF on an EX-series Switch
 - Verifying Unicast RPF Status
 - Disabling Unicast RPF (CLI Procedure)
 - Troubleshooting Unicast RPF
 - Understanding Unicast RPF for EX-series Switches