Overview

HP devices support **unicast reverse path forwarding (unicast RPF)**. Unicast RPF can be used as a defense against Denial of Service (DoS) attacks in which an attacker attempts to flood a network with packets that have spoofed or falsified source IP addresses.

When unicast RPF is enabled on an interface, the HP device examines the source address of each incoming packet and verifies that this interface is the correct one to receive packets with that source address. If this is not the correct interface to receive the packet, then the packet is dropped.

For example, in one type of DoS attack an attacker may attempt to send a large amount of traffic into a network through an external interface, using spoofed addresses of the internal network as the source of the traffic. When the unicast RPF feature is enabled, the HP device recognizes that traffic coming in on an external interface should not have source addresses belonging to the internal network, and the HP device consequently drops the traffic with the spoofed source addresses.

When you configure unicast RPF on an interface, you specify which interfaces are **external**. External interfaces are those that can receive traffic from external networks, but not from the internal network. When an interface is specified as an external interface for unicast RPF, the HP device creates CAM entries that correspond to the internally learned routes in the device’s routing table. The unicast RPF CAM entries deny packets with source IP addresses that correspond to the internally learned routes. All other traffic is permitted.

To accommodate routing table changes, the internally learned routes are synchronized with the unicast RPF CAM entries every 1 minute.

Figure 9.1 shows an illustration of a network that uses unicast RPF.
In this configuration, interface e 1/1 is specified as an external interface for unicast RPF. CAM entries are created for that interface that deny incoming packets with source addresses from the 192.168.9.x network.

The HP device’s loopback interface/network is also considered an internally learned route. In the example, incoming packets on interface e 1/1 that have a source address corresponding to the HP device’s loopback interface/network are dropped.

For interfaces that can receive packets from the internal network as well as from external sources, you identify the interface as an external interface; this prevents the HP device from creating RPF CAM entries for routes learned on the interface. For example, in the configuration in Figure 9.2, interface 2/1 can receive packets from the Internet as well as from the internal network.
In this example, interface 2/1 as identified as an external interface. When the HP device compiles the list of internally learned routes for unicast RPF, it does not include the routes learned on interface 2/1. Note that identifying an external interface in this way (using the `ip verify unicast external-interface` command, rather than the `ip verify unicast reverse-path external` command) does not enable unicast RPF for incoming packets on the interface. In the example, unicast RPF CAM entries are not created for routes learned on interface 2/1, and incoming traffic on interface 2/1 is not permitted or denied using unicast RPF CAM entries.

**NOTE:** Unicast RPF is supported on HP devices running Enterprise software release 07.8.00 or higher. This feature is supported on EP devices only. It is not supported on 10 Gigabit Ethernet interfaces.

**Configuring Unicast RPF**

To configure unicast RPF, you enable it on an interface and specify the interface as external. Note that unicast RPF applies to incoming traffic on an interface where it is configured.

For example, the following commands enable unicast RPF on interface e 1/1, and identify it as an external interface:

```
ProCurveRS# interface e 1/1
ProCurveRS(config-if-e100-1/1)# ip verify unicast reverse-path external
```

When unicast RPF is enabled on an external interface, packets with source IP addresses that correspond to the internally learned routes are denied. All other traffic is permitted.

**Syntax:** `[no] ip verify unicast reverse-path external`

To identify an interface as an external interface, without enabling unicast RPF on the interface, enter commands such as the following:

```
ProCurveRS# interface e 2/1
```
proCurveRS(config-if-e100-2/1)# ip verify unicast external-interface

When an interface is identified as an external interface with this command, it prevents the HP device from creating RPF CAM entries for routes learned on the interface. Unicast RPF is not performed for incoming packets on the interface.

Syntax: [no] ip verify unicast external-interface

Specifying a Prefix List for Unicast RPF

When unicast RPF is enabled on an external interface, the HP device compiles a list of the internally learned routes in the device's routing table and creates unicast RPF CAM entries that deny packets with source IP addresses corresponding to these routes.

In addition, you can create an IP prefix list containing a list of routes and then specify the IP prefix list as part of the unicast RPF configuration. When you do this, the HP device creates unicast RPF CAM entries that deny packets with source IP addresses corresponding to the routes in the IP prefix list, in addition to the internally learned routes. Using an IP prefix list in this way allows you to configure the device to deny packets from networks other than internal ones.

For example, the following commands create an IP prefix list called “martians” consisting of three routes:

ProCurveRS(config)# ip prefix-list martians seq 5 deny 0.0.0.0/8 le 32
ProCurveRS(config)# ip prefix-list martians seq 10 deny 10.0.0.0/8 le 32
ProCurveRS(config)# ip prefix-list martians seq 15 deny 127.0.0.0/8 le 32

NOTE: For information on creating IP prefix lists, see the Advanced Configuration and Management Guide for ProCurve 9300/9400 Series Routing Switches.

The following commands specify the “martians” IP prefix list as part of the unicast RPF configuration for interface e 1/1:

ProCurveRS# interface e 1/1
ProCurveRS(config-if-1/1)# ip verify unicast reverse-path external prefix-list martians

Syntax: [no] ip verify unicast reverse-path external prefix-list <name>

This command causes the device to drop packets incoming on interface e 1/1 that have source addresses corresponding to the routes in the “martians” prefix list (as well as packets with source addresses corresponding to internally learned routes, as well as the device's loopback address/network).

Displaying Unicast RPF Information

To display information about the CAM entries created for unicast RPF, enter the following command:

ProCurveRS# show ip rpf
Total number of RPF route entries 4

<table>
<thead>
<tr>
<th>Destination</th>
<th>NetMask</th>
<th>Port</th>
<th>VLAN ID</th>
<th>Deny</th>
</tr>
</thead>
<tbody>
<tr>
<td>40.0.0.0</td>
<td>255.255.255.0</td>
<td>3/9</td>
<td>1</td>
<td>32778</td>
</tr>
<tr>
<td>30.0.0.0</td>
<td>255.255.255.0</td>
<td>3/9</td>
<td>1</td>
<td>32779</td>
</tr>
<tr>
<td>192.168.135.0</td>
<td>255.255.255.0</td>
<td>v2</td>
<td>2</td>
<td>32769</td>
</tr>
<tr>
<td>65.0.0.0</td>
<td>255.255.255.252</td>
<td>3/9</td>
<td>1</td>
<td>32770</td>
</tr>
</tbody>
</table>

Syntax: show ip rpf [ <ipaddr> | <ipaddr>/<mask-length> | <portnum> | <ve> ]
Table 9.1 lists the information displayed in the output of the `show ip rpf` command.

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of RPF route entries</td>
<td>The number of CAM entries that have been created for unicast RPF.</td>
</tr>
<tr>
<td>Destination</td>
<td>The address of the route.</td>
</tr>
<tr>
<td>NetMask</td>
<td>The subnet mask for the route.</td>
</tr>
<tr>
<td>Port</td>
<td>The port on which the route was learned.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The VLAN ID of the port.</td>
</tr>
<tr>
<td>Deny</td>
<td>The index number of the CAM entry used for denying packets matching this route.</td>
</tr>
</tbody>
</table>

**Clearing Unicast RPF CAM Entries**

To clear the CAM entries created for unicast RPF, enter the following command:

```
ProCurveRS# clear ip rpf
```

**Syntax:** clear ip rpf