

Example: Configuring Unicast RPF on an EX-series Switch

Unicast reverse-path forwarding (RPF) helps protect the switch against denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks by verifying the unicast source address of each packet that arrives on an ingress interface where unicast RPF is enabled.

This example shows how to help defend the switch ingress interfaces against denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks by configuring global unicast reverse-path forwarding (RPF) on all switch interfaces to filter incoming traffic:

- Requirements on page 1
- Overview and Topology on page 1
- Configuration on page 2
- Verification on page 2

Requirements

This example uses the following software and hardware components:

- JUNOS Release 9.3 or later for EX-series switches
- Two EX 3200 switches

Before you configure unicast RPF, make sure that all of the switch interfaces are symmetrically routed (the switch uses the same path in both directions between the source and the destination).

Overview and Topology

Large amounts of unauthorized traffic such as attempts to flood a network with fake (bogus) service requests in a denial-of-service (DoS) attack can consume network resources and deny service to legitimate users. One way to help prevent DoS and distributed denial-of-service (DDoS) attacks is to verify that incoming traffic originates from legitimate network sources.

Unicast RPF helps ensure that a traffic source is legitimate (authorized) by comparing the source address of each packet that arrives on an interface to the forwarding-table entry for its source address. If the switch uses the same interface that the packet arrived on to reply to the packet's source, this verifies that the packet originated from an authorized source, and the switch forwards the packet. If the switch does not use the same interface that the packet arrived on to reply to the packet's source, the packet might have originated from an unauthorized source, and the switch discards the packet.

In this example, an enterprise network's system administrator wants to protect Switch A against potential DoS and DDoS attacks from the Internet. The administrator configures unicast RPF on interface `ge-1/0/10` on Switch A. Packets arriving on interface `ge-1/0/10` on Switch A from the Switch B source also use incoming interface `ge-1/0/10` as the best return path to send packets back to the source. All other

interfaces on Switch A are also symmetrically routed, because when you enable unicast RPF on any interface, it is thereby enabled globally on all switch interfaces.

The topology of this configuration example uses two EX-series 3200 switches, Switch A and Switch B, connected by symmetrically routed interfaces:

- Switch A is on the edge of an enterprise network. The interface `ge-1/0/10` on Switch A connects to the interface `ge-1/0/5` on Switch B.
- Switch B is on the edge of the service provider network that connects the enterprise network to the Internet.

Configuration

To enable unicast RPF globally on all Switch A interfaces:

CLI Quick Configuration To quickly configure unicast RPF on a switch to help prevent DoS/DDoS attacks, copy the following command and paste it into the switch terminal window:

```
[edit interfaces]
set ge-1/0/10 unit 0 family inet rpf-check
```

Step-by-Step Procedure To configure Switch A interfaces to perform unicast RPF filtering:

1. Enable unicast RPF on interface `ge-1/0/10`:

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

Results Check the results:

```
[edit interfaces]
user@switch# show
ge-1/0/10 {
  unit 0 {
    family inet {
      rpf-check;
    }
  }
}
```

Verification

To confirm that the configuration is correct, perform these tasks:

- Verifying That Unicast RPF Is Enabled on the Switch on page 2

Verifying That Unicast RPF Is Enabled on the Switch

Purpose Verify that unicast RPF is enabled.

Action Verify that unicast RPF is enabled on interface ge-1/0/10 by using the show interfaces ge-1/0/10 extensive or show interfaces ge-1/0/10 detail command.

```
user@switch> show interfaces ge-1/0/10 extensive
Physical interface: ge-1/0/10, Enabled, Physical link is Down
Interface index: 139, SNMP ifIndex: 58, Generation: 140
Link-level type: Ethernet, MTU: 1514, Speed: Auto, MAC-REWRITE Error: None,
Loopback: Disabled, Source filtering: Disabled, Flow control: Enabled,
Auto-negotiation: Enabled, Remote fault: Online
Device flags   : Present Running
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Link flags     : None
CoS queues     : 8 supported, 8 maximum usable queues
Hold-times    : Up 0 ms, Down 0 ms
Current address: 00:19:e2:50:95:ab, Hardware address: 00:19:e2:50:95:ab
Last flapped   : Never
Statistics last cleared: Never
Traffic statistics:
Input bytes   :                0                0 bps
Output bytes  :                0                0 bps
Input packets :                0                0 pps
Output packets:                0                0 pps
IPv6 transit statistics:
Input bytes   :                0
Output bytes  :                0
Input packets :                0
Output packets:                0
Input errors:
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0,
L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0,
FIFO errors: 0, Resource errors: 0
Output errors:
Carrier transitions: 0, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0,

FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
Egress queues: 8 supported, 4 in use
Queue counters:      Queued packets  Transmitted packets      Dropped packets

0 best-effort                0                0                0
1 assured-forw              0                0                0
5 expedited-fo              0                0                0
7 network-cont              0                0                0

Active alarms  : LINK
Active defects : LINK
MAC statistics:
Total octets      Receive      Transmit
Total packets    0            0
Unicast packets  0            0
Broadcast packets 0            0
Multicast packets 0            0
CRC/Align errors 0            0
FIFO errors       0            0
MAC control frames 0            0
MAC pause frames  0            0
Oversized frames  0
Jabber frames     0
```

```

Fragment frames                                0
VLAN tagged frames                            0
Code violations                                0
Filter statistics:
Input packet count                            0
Input packet rejects                          0
Input DA rejects                              0
Input SA rejects                              0
Output packet count                            0
Output packet pad count                       0
Output packet error count                     0
CAM destination filters: 0, CAM source filters: 0
Autonegotiation information:
Negotiation status: Incomplete
Packet Forwarding Engine configuration:
Destination slot: 1

Logical interface ge-1/0/10.0 (Index 69) (SNMP ifIndex 59) (Generation 135)
Flags: Device-Down SNMP-Traps 0x0 Encapsulation: ENET2
Traffic statistics:
Input bytes :                                0
Output bytes :                               0
Input packets:                              0
Output packets:                              0
IPv6 transit statistics:
Input bytes :                                0
Output bytes :                               0
Input packets:                              0
Output packets:                              0
Local statistics:
Input bytes :                                0
Output bytes :                               0
Input packets:                              0
Output packets:                              0
Transit statistics:
Input bytes :                                0                0 bps
Output bytes :                               0                0 bps
Input packets:                              0                0 pps
Output packets:                              0                0 pps
IPv6 transit statistics:
Input bytes :                                0
Output bytes :                               0
Input packets:                              0
Output packets:                              0
Protocol inet, MTU: 1500, Generation: 144, Route table: 0
Flags: uRPF
Addresses, Flags: Is-Preferred Is-Primary

```

Meaning The second-to-last line of the display shows the unicast RPF flag enabled. This confirms that unicast RPF is enabled on interface **ge-1/0/10** and thereby on all switch interfaces. Only the interface on which you configured unicast RPF shows the correct unicast RPF configuration status. If you check the unicast RPF status on an interface on which you did not explicitly configure it, the unicast RPF flag is not displayed, even though unicast RPF is implicitly enabled.

- Related Topics**
- Configuring Unicast RPF (CLI Procedure)
 - Disabling Unicast RPF (CLI Procedure)