Configuring Unicast RPF

This chapter describes how to configure unicast reverse path forwarding (uRPF) on Cisco NX-OS devices.

This chapter includes the following sections:

About Unicast RPF

The unicast RPF feature reduces problems that are caused by the introduction of malformed or forged (spoofed) IPv4 or IPv6 source addresses into a network by discarding IPv4 or IPv6 packets that lack a verifiable IP source address. For example, a number of common types of Denial-of-Service (DoS) attacks, including Smurf and Tribal Flood Network (TFN) attacks, can take advantage of forged or rapidly changing source IPv4 or IPv6 addresses to allow attackers to thwart efforts to locate or filter the attacks. Unicast RPF deflects attacks by forwarding only the packets that have source addresses that are valid and consistent with the IP routing table.

When you enable unicast RPF on an interface, the switch examines all ingress packets received on that interface to ensure that the source address and source interface appear in the routing table and match the interface on which the packet was received. This examination of source addresses relies on the Forwarding Information Base (FIB).

Note Unicast RPF is an ingress function and is applied only on the ingress interface of a switch at the upstream end of a connection.

Unicast RPF verifies that any packet received at a switch interface arrives on the best return path (return route) to the source of the packet by doing a reverse lookup in the FIB. If the packet was received from one of the best reverse path routes, the packet is forwarded as normal. If there is no reverse path route on the same

interface from which the packet was received, the source address might have been modified by the attacker. If unicast RPF does not find a reverse path for the packet, the packet is dropped.

Note With unicast RPF, all equal-cost "best" return paths are considered valid, which means that unicast RPF works where multiple return paths exist, if 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. Unicast RPF also functions where Enhanced Interior Gateway Routing Protocol (EIGRP) variants are being used and unequal candidate paths back to the source IP address exist.

Unicast RPF Process

Unicast RPF has several key implementation principles:

- The packet must be received at an interface that has the best return path (route) to the packet source (a process called *symmetric routing*). There must be a route in the FIB that matches the route to the receiving interface. Static routes, network statements, and dynamic routing add routes to the FIB.
- IP source addresses at the receiving interface must match the routing entry for the interface.
- Unicast RPF is an input function and is applied only on the input interface of a device at the upstream end of a connection.

You can use unicast RPF for downstream networks, even if the downstream network has other connections to the Internet.

Caution Be careful when using optional BGP attributes, such as weight and local preference, because an attacker can modify the best path back to the source address. Modification would affect the operation of unicast RPF.

When a packet is received at the interface where you have configured unicast RPF and ACLs, the Cisco NX-OS software performs the following actions:

1. Checks the input ACLs on the inbound interface.
2. Uses unicast RPF to verify that the packet has arrived on the best return path to the source, which it does by doing a reverse lookup in the FIB table.
3. Conducts a FIB lookup for packet forwarding.
4. Checks the output ACLs on the outbound interface.
5. Forwards the packet.

Guidelines and Limitations for Unicast RPF

Unicast RPF (uRPF) has the following configuration guidelines and limitations:

- uRPF is supported for the following platforms:
  - Cisco Nexus 9500 Series switches with N9K-X9636C-R and N9K-X9636Q-R line cards

  - Cisco Nexus 9500 Series switches with N9K-X9636C-RX line cards
  - Cisco Nexus 9300 platform switches (excluding the 9300-FXP switches)

- Beginning with Cisco NX-OS Release 10.1(2), uRPF is supported on:
  - Cisco Nexus 9300-GX/GX2 series switches and Cisco Nexus 9500 series switches with FX linecards (for IPv4 and IPv6)
  - Cisco Nexus 9500 series switches with EX linecards (for IPv4 only)
  - ToR and EoR switches that support vPC
- Beginning with Cisco NX-OS Release 9.2(1), uRPF is supported on:
  - Cisco Nexus 9300-EX Series switches (for IPv4 only)
  - Cisco Nexus 9300-FX/FX2 Series switches (for IPv4 and IPv6)
- Beginning with Cisco NX-OS Release 9.3(5), uRPF is supported on Cisco Nexus 9300-FX3 platform switches (for IPv4 and IPv6).
- Beginning with Cisco Nexus Release 9.3(1), uRPF is supported on Cisco Nexus 9500 Series switches with the family of modular EX/FX line cards (see Cisco Nexus 9500 Cloud-Scale Line Cards and Fabric Modules Data Sheet).

Note uRPF on the modular EX/FX line cards is supported only in DUAL STACK MCAST routing mode. Specify the following configuration before enabling uRPF: `system routing template-dual-stack-mcast`. Refer to the *Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide* on how to configure DUAL STACK MCAST routing mode.

From Cisco NX-OS Release 10.1(2), uRPF on the modular EX/FX line cards is supported in default routing mode, too.

- You must apply uRPF at the interface downstream from the larger portion of the network, preferably at the edges of your network.
- The further downstream that you apply uRPF, the finer the granularity you have in mitigating address spoofing and in identifying the sources of spoofed addresses. For example, applying uRPF on an aggregation device helps to mitigate attacks from many downstream networks or clients and is simple to administer, but it does not help identify the source of the attack. Applying uRPF at the network access server helps limit the scope of the attack and trace the source of the attack; however, deploying uRPF across many sites does add to the administration cost of operating the network.
- The more entities that deploy uRPF across Internet, intranet, and extranet resources mean the better the chances of mitigating large-scale network disruptions throughout the Internet community and of tracing the source of an attack.
- uRPF won’t inspect IP packets that are encapsulated in tunnels, such as generic routing encapsulation (GRE) tunnels. Configure uRPF at a home gateway so that uRPF processes network traffic only after the tunneling and encryption layers have been stripped off the packets.

- You can use uRPF in any “single-homed” environment where there is only one access point out of the network or one upstream connection. Networks that have one access point provide symmetric routing, which means that the interface where a packet enters the network is also the best return path to the source of the IP packet.
- Don’t use uRPF on interfaces that are internal to the network. Internal interfaces are likely to have routing asymmetry, which means that multiple routes to the source of a packet exist. You should configure uRPF only where there is natural or configured symmetry.
- uRPF allows packets with 0.0.0.0 source and 255.255.255.255 destination to pass so that the Bootstrap Protocol (BOOTP) and the Dynamic Host Configuration Protocol (DHCP) can operate correctly.
- When uRPF is enabled, the amount of static routes to null0 the switch can install is limited to the value of "Max V4 Ucast DA TCAM table entries" in "show hardware internal forwarding table utilization".
- Beginning with Cisco NX-OS Release 9.2(1), for N9K-X9636C-R and N9K-X96136YC-R switches, you can configure only one version of the available IPv4 and IPv6 Unicast RPF command on an interface. However, this enables Unicast RPF for both IPv4 and IPv6.
- The following guidelines and limitations apply only to Cisco Nexus 9500 Series switches with a N9K-X9636C-R, N9K-X9636C-RX, or N9K-X9636Q-R line card:
  - For strict uRPF to work, enable it on the ingress interface and the interface where the source IP address is learned.
  - The switch hardware does not implement strict uRPF per the configured routing interface.
  - Strict uRPF is implemented per learned route on strict uRPF-enabled interfaces.
  - If a route is resolved as ECMP, strict uRPF falls back to loose mode.
  - Because of the hardware limitation on the trap resolution, uRPF might not be applied on supervisor-bound packets via inband.
  - For IP traffic, enable IPv4 and IPv6 configurations simultaneously.
  - Due to hardware limitations, the N9K-X9636C-R, N9K-X9636C-RX, and N9K-X9636Q-R line cards support only the following combinations:

uRPF Configuration		**Applied Traffic Check on Source IP Address**			
IPv4	IPv6	IP Unipath	IP ECMP	MPLS Encap VPN ECMP	Unipath MPLS VPN for N9K-X9636C-RX Line Card
Disable	Disable	Allow	Allow	Allow	Allow
Loose	Loose	uRPF loose	uRPF loose	uRPF loose	uRPF strict
Strict	Strict	uRPF strict	uRPF loose	uRPF loose	uRPF strict

- Strict uRPF discards the ICMPv6 NA packets even if the destined interface receives them for the following Cisco NX-OS devices:
  - Line cards: N9K-X9564PX, N9K-X9564TX, N9K-X9536PQ, X9408PC-CFP2, X9464TX, X9464TX2

- Uplink modules: N9K-M12PQ
- Switches: 93128TX, 9396PX, 9396TX, 9372PX, 9372PX-E, 3164Q, 31128PQ

- Strict uRPF blocks the ICMP traffic destined to the interface through VxLAN for the following platforms:
  - Cisco Nexus 9200 platform switches
  - Cisco Nexus 9300-EX/FX/GX platform switches
  - Nexus 9500 switches with N9K-X9700-EX and N9K-X9700-FX line cards
- If Strict uRPF is configured, append the following commands for urpf strict mode to work for unresolved host behind a subnet:
  - **no system multicast dcs-check**
  - **hardware profile multicast max-limit lpm-entries 0**

Default Settings for Unicast RPF

This table lists the default settings for unicast RPF parameters.

Table 1: Default Unicast RPF Parameter Settings

Parameters	Default
Unicast RPF	Disabled

Configuring Unicast RPF for Cisco Nexus 9500 Switches with -R Line Cards

You can configure unicast RPF on an ingress interface for Cisco Nexus 9500 Series switches with an -R line card.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface ethernet** *slot*/*port*
	Example:
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		Enters interface configuration mode.

	Command or Action	Purpose
Step 3	{**ip** | **ipv6**} **address** *ip-address/length* **Example:** `switch(config-if)# ip address 172.23.231.240/23`	Specifies an IPv4 or IPv6 address for the interface.
Step 4	{**ip** | **ipv6**} **verify unicast source reachable-via any** **Example:** `switch(config-if)# ip verify unicast source reachable-via any`	Configures unicast RPF on the interface for both IPv4 and IPv6. **Note** When you enable uRPF for IPv4 or IPv6 (using the **ip** or **ipv6** keywords), uRPF is enabled for both IPv4 and IPv6.
Step 5	(Optional) **show ip interface ethernet** *slot*/*port* **Example:** `switch(config)# show ip interface ethernet 2/3`	Displays the IP information for an interface.
Step 6	(Optional) **show running-config interface ethernet** *slot*/*port* **Example:** `switch(config)# show running-config interface ethernet 2/3`	Displays the configuration for an interface in the running configuration.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Unicast RPF for Cisco Nexus 9300 Switches

You can configure one of the following Unicast RPF modes on an ingress interface for Cisco Nexus 9300 platform switches (excluding the 9300-FXP switches) running Cisco NX-OS Release 9.2(1) or a later release.

Strict Unicast RPF mode
A strict mode check is successful when Unicast RPF finds a match in the FIB for the packet source address and the ingress interface through which the packet is received matches one of the Unicast RPF interfaces in the FIB match. If this check fails, the packet is discarded. You can use this type of Unicast RPF check where packet flows are expected to be symmetrical.

Loose Unicast RPF mode
A loose mode check is successful when a lookup of a packet source address in the FIB returns a match and the FIB result indicates that the source is reachable through at least one real interface. The ingress interface through which the packet is received is not required to match any of the interfaces in the FIB result.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **system urpf disable** **Example:** `switch(config)# no system urpf disable`	Enables Unicast RPF on the switch. **Note** You must reload the Cisco NX-OS box to apply the Unicast RPF configuration.

Step 3	**interface ethernet** *slot*/*port*
	Example:
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		Specifies an Ethernet interface and enters interface configuration mode.

Step 4	{**ip** | **ipv6**} **address** *ip-address/length* **Example:** `switch(config-if)# ip address 172.23.231.240/23`	Specifies an IPv4 or IPv6 address for the interface.
Step 5	{**ip** | **ipv6**} **verify unicast source reachable-via** {**any** [**allow-default**] | **rx**} **Example:** `switch(config-if)# ip verify unicast source reachable-via any`	Configures Unicast RPF on the interface for both IPv4 and IPv6. You can enable IPv4 and IPv6 uRPF separately for the Cisco Nexus 9300-EX Series switches (for IPv4) and on Cisco Nexus 9300-FX/FX2 Series switches. **Note** When you enable Unicast RPF for IPv4 or IPv6 (using the **ip** or **ipv6** keyword), Unicast RPF is enabled for both IPv4 and IPv6. You can configure only one version of the available IPv4 and IPv6 Unicast RPF command on an interface. When you configure one version, all the mode changes must be done by this version and all other versions will be blocked by that interface. • The **any** keyword specifies loose Unicast RPF. • If you specify the **allow-default** keyword, the source address lookup can match the default route and use that for verification.

	Command or Action	Purpose
		Note The **allow-default** keyword is not applicable in the ALPM routing mode. **Note** The source address lookup (in case of a loose Unicast RPF check) does not match the default route if you do not specify the **allow-default** keyword. • The **rx** keyword specifies strict Unicast RPF.

Step 6	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 7	(Optional) **show ip interface ethernet** *slot/port*
	Example:
	`switch(config)# show ip interface ethernet 1/54 | grep -i "unicast reverse path forwarding"`
	`IP unicast reverse path forwarding: none`
		Displays the IP information for an interface and verifies if Unicast RPF is enabled.

Step 8	(Optional) **show running-config interface ethernet** *slot/port* **Example:** `switch(config)# show running-config interface ethernet 2/3`	Displays the configuration for an interface in the running configuration.
Step 9	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuration Examples for Unicast RPF

The following example shows how to configure loose unicast RPF for IPv4 packets on a Cisco Nexus 9500 Series switch with an -R line card:

```
interface Ethernet2/3
  ip address 172.23.231.240/23
  ip verify unicast source reachable-via any
```

The following example shows how to configure loose unicast RPF for IPv6 packets on a Cisco Nexus 9500 Series switch with an -R line card:

```
interface Ethernet2/1
  ipv6 address 2001:0DB8:c18:1::3/64
  ipv6 verify unicast source reachable-via any
```

The following example shows how to configure loose unicast RPF for IPv4 packets on a Cisco Nexus 9300 platform switch:

```
no system urpf disable
interface Ethernet2/3
  ip address 172.23.231.240/23
  ip verify unicast source reachable-via any
```

The following example shows how to configure loose unicast RPF for IPv6 packets on a Cisco Nexus 9300 platform switch:

```
no system urpf disable
interface Ethernet2/1
  ipv6 address 2001:0DB8:c18:1::3/64
  ipv6 verify unicast source reachable-via any
```

The following example shows how to configure strict unicast RPF for IPv4 packets on a Cisco Nexus 9300 platform switch:

```
no system urpf disable
interface Ethernet2/2
  ip address 172.23.231.240/23
  ip verify unicast source reachable-via rx
```

The following example shows how to configure strict unicast RPF for IPv6 packets on a Cisco Nexus 9300 platform switch:

```
no system urpf disable
interface Ethernet2/4
  ipv6 address 2001:0DB8:c18:1::3/64
  ipv6 verify unicast source reachable-via rx
```

Verifying the Unicast RPF Configuration

To display unicast RPF configuration information, perform one of the following tasks:

Command	Purpose
show running-config interface ethernet *slot*/*port*	Displays the interface configuration in the running configuration.
show running-config ip [**all**]	Displays the IPv4 configuration in the running configuration.
show running-config ipv6 [**all**]	Displays the IPv6 configuration in the running configuration.
show startup-config interface ethernet *slot*/*port*	Displays the interface configuration in the startup configuration.

Command	Purpose
show startup-config ip	Displays the IP configuration in the startup configuration.

Additional References for Unicast RPF

This section includes additional information related to implementing unicast RPF.

Related Documents

Related Topic	Document Title
Data Management Engine (DME)-ized commands	Cisco Nexus 3000 and 9000 Series NX-API REST SDK User Guide and API Reference
MPLS VPN	Cisco Nexus 9000 Series NX-OS Label Switching Configuration Guide