

Implementing URPF

This section describes the implementation of URPF.

- Understanding URPF, on page 1
- Command compatibility and prerequisites for uRPF loose mode , on page 2
- Configuring uRPF Loose Mode, on page 2
- uRPF strict mode with external TCAM, on page 3
- Configure uRPF strict mode , on page 5

Understanding URPF

It has become a commonplace practice for hackers planning a DoS attack to use forged IP addresses (the practice is known as IP address spoofing) and constantly change the source IP address to avoid detection by service providers.

Unicast Reverse Path Forwarding (URPF) is a mechanism for validating the source IP address of packets received on a router. A router configured with URPF performs a reverse path lookup in the FIB table to validate the presence of the source IP address. If the source IP address is listed in the table, then it indicates that the source is reachable and valid. If source IP address cannot be located in the FIB table, the packet is treated as malicious by the router and discarded.

The router supports the use of URPF in both strict and loose modes. URPF loose mode is enabled when the router is configured to validate only the prefix of the source IP address in the FIB and not the interface used by the packet to reach the router. By configuring loose mode, legitimate traffic that uses an alternate interface to reach the router is not mistaken to be malicious. URPF loose mode is very useful in multi-homed provider edge networks.

When URPF strict mode is enabled, the source address of the packet is checked in the FIB. If the packet is received on the same interface that would be used to forward the traffic to the source of the packet, the packet passes the check and is further processed; otherwise, it is dropped. Strict uRPF should only be applied where there is natural or configured symmetry. Because internal interfaces are likely to have routing asymmetry, that is, multiple routes to the source of a packet, URPF strict mode should not be implemented on interfaces that are internal to the network.

Note The behavior of URPF strict mode varies slightly by platform, number of recursion levels, and number of paths in Equal-Cost Multipath (ECMP) scenarios. A platform may switch to loose RPF check for some or all prefixes, even though strict RPF is configured.

The URPF loose and strict modes support both **allow self-ping** and **self-ping** options. The **self-ping** option allows the source of the packet to ping itself.

Command compatibility and prerequisites for uRPF loose mode

- Both **hw-module fib ipv6 scale internet-optimized-disable** and **hw-module fib ipv4 scale host-optimized-disable** commands cannot coexist with **hw-module profile segment-routing srv6 mode**.
- If **hw-module fib ipv4 scale host-optimized-disable** is configured, do not enable SRv6 micro-segment format (these profiles are mutually exclusive).
- Cisco NCS 5500 line cards require reload after disabling scale for immediate effect; reload not required for NCS 5700 line cards.
- On NCS55Ax systems with external TCAM (eTCAM), dual capacity mode does not need to be disabled to enable URPF.
- No hw-module configuration needed for NCS 5700 series line cards.
- NL TCAM requires: **hw-module tcam fib ipv4 scale disable** and **hw-module profile tcam fib ipv6 unicast** *percent*
- For OP external TCAM, no configuration is required.

Table 1: Command Compatability

Command	Coexistence restriction	Card models	Note
hw-module fib ipv6 scale internet-optimized-disable	Mutually exclusive with SRv6 profile	All	Must reload NCS 5500
hw-module fib ipv4 scale host-optimized-disable	Mutually exclusive with SRv6 micro-segment	All	Must reload NCS 5500
hw-module tcam fib ipv4 scale disable	Only for NL TCAM cards	NCS 5500 (NL) TCAM	NA
hw-module profile tcam fib ipv6 unicast Percent	Only for NL TCAM cards	NCS 5500 (NL) TCAM	NA

Configuring uRPF Loose Mode

This section explains how you can configure uRPF loose mode on the router for both IPv4 and IPv6 networks.

Before You Begin

Before you can configure uRPF loose mode on a router, you must disable the default scale on the Cisco NCS 5500 series line card, as described in this section.

For all types of line cards with TCAM:

```
RP/0/RP0/CPU0:router(config)# hw-module tcam fib ipv4 scaledisable

RP/0/RP0/CPU0:router(config)# commit
RP/0/RP0/CPU0:router(config)# end
RP/0/RP0/CPU0:router# reload location all
Proceed with reload? [confirm]
```

For all types of line cards without TCAM:

```
RP/0/RP0/CPU0:router(config)# hw-module fib ipv4 scale host-optimized-disable

RP/0/RP0/CPU0:router(config)# commit
RP/0/RP0/CPU0:router(config)# end
RP/0/RP0/CPU0:router# reload location all
Proceed with reload? [confirm]
```

Configuration

Use the following configuration to configure uRPF loose mode on the router.

Note You must configure both IPv4 and IPv6 commands (as described in this section) for uRPF to work.

```
RP/0/RP0/CPU0:router(config)# interface Bundle-Ether1
RP/0/RP0/CPU0:router(config-if)# ipv4 address 10.0.0.1 255.255.255.0
RP/0/RP0/CPU0:router(config-if)# ipv4 verify unicast source reachable-via any
RP/0/RP0/CPU0:router(config-if)# ipv6 address 2001::1/64
RP/0/RP0/CPU0:router(config-if)# ipv6 verify unicast source reachable-via any
RP/0/RP0/CPU0:router(config-if)# commit
```

Running Configuration

Confirm your configuration as shown:

```
RP/0/RP0/CPU0:router(config-if)# show running-config
Thu Jul 27 14:40:38.167 IST
...
!
interface Bundle-Ether1
 ipv4 address 10.0.0.1 255.255.255.0
 ipv4 verify unicast source reachable-via any
ipv6 address 2001::1/64
 ipv6 verify unicast source reachable-via any
!
```

You have successfully configured uRPF loose mode on the router.

uRPF strict mode with external TCAM

A uRPF strict mode is a network security mechanism that

- verifies that incoming packets are received on the interface used to reach the source address,

- drops packets when the source does not match the expected return-path interface, and
- prevents IP spoofing and enforces routing symmetry.

Table 2: Feature History Table

Feature Name	Release Information	Feature Description
uRPF strict mode	Release 26.2.1	Introduced in this release on: NCS 5500 fixed port routersNCS 5500 modular routers uRPF strict mode increases network security by blocking IP spoofing and dropping packets whose source IP does not match the expected return path interface. It checks that incoming traffic uses the same interface that the router would use to reach the source IP address. uRPF strict modes supports up to 16 Equal-Cost Multipath (ECMP) paths. This release extends uRPF strict mode to devices with external TCAM.

Restrictions for uRPF strict mode with external TCAM

- You cannot enable uRPF strict mode if either **hw-module profile segment-routing srv6** or **hw-module profile qos ipv6 short** is enabled.
- Strict uRPF mode is not supported on NCS 5500 line cards without external TCAM.
- S-RTBH (Source-based Remotely Triggered Black Hole) feature is not supported with strict mode uRPF mode on NCS5500 Series routers with external TCAM.
- Strict uRPF is supported only for IPv4 and IPv6 address family routes. If MPLS LDP is configured, you must also configure LDP label filtering to prevent the allocation of local labels for access IPv4 or IPv6 prefixes.
- On NCS 5700 line cards, strict uRPF is only supported with external TCAM.

Guidelines for uRPF strict mode with external TCAM

These guidelines are only applicable to NCS 5500 fixed port routers and NCS 5500 modular port routers.

- For routers with NL (Network Logic) TCAM you need to configure these commands.
  - **hw-module tcam fib ipv4 scaledisable**
  - **hw-module profile tcam fib ipv6 unicast percent** <*percentage*>
- You don't need to configure these commands for OP (Operations) TCAM.
  - **hw-module tcam fib ipv4 scaledisable**
  - **hw-module profile tcam fib ipv6 unicast percent** <*percentage*>

- uRPF strict mode is supported by default on line cards having external TCAM, if these hw-module commands are not configured:
  - **hw-module profile qos ipv6 short**
  - **hw-module profile segment-routing srv6**
- If a route has more than 16 strict uRPF-enabled paths, you get these syslog messages mentioning the invalid configuration, its impact, and recovery steps.

```
LC/0/0/CPU0:Oct 8 18:10:42.867 IST: fib_mgr[305]:
%PLATFORM-PLAT_FIB-3-SuRPF_MAX_ECMP_REACH_ERR : ECMP paths with suRPF enabled are 18
for some prefixes. Supported suRPF enabled ECMP paths for a given prefix are 16 on this
platform. This will lead to complete traffic drop for affected prefixes. Please reduce
suRPF config to supported ECMP paths scale to recover
```

Configure uRPF strict mode

Use this procedure to configure uRPF strict mode on a router.

uRPF strict mode discards packets if the device cannot verify that the source address of each packet is reachable through the receiving interface. uRPF helps prevent attacks that rely on spoofing source addresses.

Before you begin

- Configure both IPv4 and IPv6 commands as described in Configuring uRPF Loose Mode, on page 2.

Procedure

Step 1 Enter interface configuration mode for the required interface.

Example:

```
Router(config)#interface GigabitEthernet 0/1/0/0
```

Step 2 Assign the IPv4 address to the interface.

Example:

```
Router(config-if)#ipv4 address 10.0.0.1 255.255.255.0
```

Step 3 Enable uRPF strict mode for IPv4.

Example:

```
Router(config-if)#ipv4 verify unicast source reachable-via rx
```

Step 4 Assign the IPv6 address to the interface.

Example:

```
Router(config-if)#ipv6 address  2001:DB8::1/64
```

Step 5 Enable uRPF strict mode for IPv6.

Example:

```
Router(config-if)#ipv6 verify unicast source reachable-via rx
Router(config-if)#commit
```

Step 6 Verify your configuration.

Example:

```
Router#show running-config
...
!
interface GigabitEthernet 0/1/0/0
 ipv4 address 10.0.0.1 255.255.255.0
 ipv4 verify unicast source reachable-via rx
ipv6 address  2001:DB8::1/64
 ipv6 verify unicast source reachable-via rx
!
```