1 uRPF Commands

Command	Function
clear ip urpf	Clear IPv4 Unicast Reverse Path Forwarding (uRPF) packet loss statistics.
ip verify unicast source reachable-via (Global configuration mode)	Enable IPv4 uRPF.
ip verify unicast source reachable-via (Interface configuration mode)	Enable uRPF on an interface.
ip verify urpf drop-rate compute interval	Configure the interval for calculating the uRPF IPv4/IPv6 packet loss rate.
ip verify urpf drop-rate notify	Enable uPRF packet loss information monitoring.
ip verify urpf drop-rate notify hold-down	Configure the alarm interval of the uRPF IPv4/IPv6 packet loss rate.
ip verify urpf notification threshold	Configure the threshold of the uRPF packet loss rate.
show ip urpf	Display the IPv4 uRPF configurations and statistics.

1.1 clear ip urpf

Function

Run the **clear ip urpf** command to clear IPv4 Unicast Reverse Path Forwarding (uRPF) packet loss statistics.

Syntax

clear ip urpf [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-name interface-number*: Specifies the interface whose statistics are cleared. If this parameter is not specified, statistics of all interfaces are cleared.

Command Modes

Privileged EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example clears IPv4 uRPF packet loss statistics on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear ip urpf interface gigabitethernet0/1
```
The following example clears IPv4 uRPF packet loss statistics on all interfaces.

```
Hostname> enable
Hostname# clear ip urpf
```

Notifications

When IPv4 uRPF is not enabled on the specified interface, the following notification will be displayed:

```
% Interface GigabitEthernet 0/1 does not enable URPF function.
```
When no interface is specified and IPv4 uRPF is not enabled on the device, the following notification will be displayed:

```
% Device does not enable URPF function.
```

Platform Description

N/A

1.2 ip verify unicast source reachable-via (Global configuration mode)

Function

Run the **ip verify unicast source reachable-via** command to enable IPv4 uRPF.

Run the **no** form of this command to disable this feature.

IPv4 uRPF is disabled by default.

Syntax

ip verify unicast source reachable-via rx

no ip verify unicast

Parameter Description

rx: Configures the strict mode to perform a uRPF check. The strict mode requires that the outbound interface of the forwarding entry found in the forwarding table based on the source address of a received IP packet must match the inbound interface of the packet.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Based on the source address of a received IP packet, uRPF checks whether any route to the source address exists in the forwarding table and accordingly determines whether the packet is valid. If no forwarding entry is matched, the packet is determined as invalid.

You can enable uRPF in global configuration mode to perform a uRPF check for packets received on all interfaces of a device.

Only the uRPF strict mode can be configured in global configuration mode. If a matched equal-cost route is found for a packet, the packet will be processed according to the uRPF loose mode.

If uRPF is configured in global configuration mode, the default route cannot be used for a uRPF check.

uRPF cannot be configured in global configuration mode and interface configuration mode simultaneously.

Examples

The following example enables IPv4 uRPF.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip verify unicast source reachable-via rx
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 ip verify unicast source reachable-via (Interface configuration mode)

Function

Run the **ip verify unicast source reachable-via** command to enable uRPF on an interface.

Run the **no** form of this command to disable this feature.

uRPF is disabled for an interface by default.

Syntax

ip verify unicast source reachable-via { any | rx } [allow-default]

no ip verify unicast

Parameter Description

any: Configures the loose mode to perform a uRPF check. The loose mode only requires that a forwarding entry can be found in the forwarding table based on the source address of a received IP packet.

rx: Configures the strict mode to perform a uRPF check. The strict mode requires that the outbound interface of the forwarding entry found in the forwarding table based on the source address of a received IP packet must match the inbound interface of the packet.

allow-default: Allows to use the default route for a uRPF check. If this parameter is not specified, the default route is not used for a uPRF check.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After this command is configured, a switch will perform a uRPF check on both IPv4 and IPv6 packets.

A switch supports configuration of uRPF on a routed port, a L3 aggregation port (AP) or a switch virtual interface (SVI).

Based on the source address of a received IP packet, uRPF checks whether any route to the source address exists in the forwarding table and accordingly determines whether the packet is valid. If no forwarding entry is matched, the packet is determined as invalid.

You can enable uRPF in interface configuration mode to perform a uRPF check for packets received on the interface.

The default route is not used for a uRPF check by default. You can use the **allow-default** keyword to use the default route for a URPF check if necessary.

● uRPF does not support association with the ACL option.

● uRPF does not support the use of IPv6 routes with a 65-bit to 127-bit prefix for a uRPF check.

● After uRPF is enabled on interfaces, a uRPF check is performed for all packets received on physical ports corresponding to these interfaces, which increases the scope of packets checked by uRPF. If a packet received on a tunnel port is also received on the preceding physical ports, the packet is also checked by uRPF. In such a scenario, be cautious in enabling uRPF.

- After uRPF is enabled, the route forwarding capacity of a device will be reduced by half.

- After the uRPF strict mode is enabled, if a packet received on an interface matches an equal-cost route during the uRPF check, the packet will be processed according to the URPF loose mode.

- If uRPF is configured in global configuration mode, the default route cannot be used for a uRPF check.

- uRPF cannot be configured in global configuration mode and interface configuration mode simultaneously.

- uRPF cannot be enabled on a range of interfaces.

Examples

The following example enables uRPF on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet0/1
Hostname(config-if-GigabitEthernet 0/1)# ip verify unicast source reachable-via
rx
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4   ip verify urpf drop-rate compute interval

Function

Run the **ip verify urpf drop-rate compute interval** command to configure the interval for calculating the uRPF IPv4/IPv6 packet loss rate.

Run the **no** form of this command to remove this configuration.

The default interval for calculating the uRPF IPv4/IPv6 packet loss rate is **30** seconds.

Syntax

ip verify urpf drop-rate compute interval *interval*

no ip verify urpf drop-rate compute interval

Parameter Description

interval *interval*: Specifies the interval for calculating the uRPF packet loss rate, in seconds. The value range is from 30 to 300.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The interval for calculating the uRPF packet loss rate is configured in global configuration mode, which applies to the calculation of the uRPF packet loss rate globally and on each interface with uRPF enabled and takes effect to IPv4 and IPv6 uRPF.

Examples

The following example sets the interval for calculating the uRPF IPv4/IPv6 packet loss rate to 60 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip verify urpf drop-rate compute interval 60
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip verify urpf drop-rate notify**
- **ip verify urpf drop-rate notify hold-down**

1.5   ip verify urpf drop-rate notify

Function

Run the **ip verify urpf drop-rate notify** command to enable uPRF packet loss information monitoring.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

uRPF packet loss information monitoring is disabled by default.

Syntax

ip verify urpf drop-rate notify

no ip verify urpf drop-rate notify

default ip verify urpf drop-rate notify

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After uRPF packet loss information monitoring is enabled, a device can proactively send syslogs or trap messages to notify users of the packet loss information detected in the uRPF check so that the users can monitor the network status conveniently.

Examples

The following example enables uRPF packet loss information monitoring on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet0/1
Hostname(config-if-GigabitEthernet 0/1)# ip verify urpf drop-rate notify
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

● **ip verify urpf drop-rate compute interval**

● **ip verify urpf drop-rate notify hold-down**

1.6 ip verify urpf drop-rate notify hold-down

Function

Run the **ip verify urpf drop-rate notify hold-down** command to configure the alarm interval of the uRPF IPv4/IPv6 packet loss rate.

Run the **no** form of this command to remove this configuration.

The default alarm interval for the uRPF IPv4/IPv6 packet loss rate is **300** seconds.

Syntax

ip verify urpf drop-rate notify hold-down *hold-down-time*

no ip verify urpf drop-rate notify hold-down

Parameter Description

hold-down *hold-down-time*: Specifies the alarm interval of the uRPF packet loss rate, in seconds. The value range is from 30 to 300.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The alarm interval of the uRPF packet loss rate is configured in global configuration mode, and applies to alarm reporting of the uRPF packet loss rate globally and on each interface with uRPF enabled and takes effect to IPv4 and IPv6 uRPF.

Examples

The following example sets the alarm interval of the uRPF IPv4/IPv6 packet loss rate to 60 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip verify urpf drop-rate notify hold-down 60
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip verify urpf drop-rate compute interval**
- **ip verify urpf drop-rate notify**

1.7   ip verify urpf notification threshold

Function

Run the **ip verify urpf notification threshold** command to configure the threshold of the uRPF packet loss rate.

Run the **no** form of this command to remove this configuration.

The default threshold of the uRPF packet loss rate is **1000** packets per second.

Syntax

ip verify urpf notification threshold *rate-value*

no ip verify urpf notification threshold

Parameter Description

threshold *rate-value*: Specifies the threshold of the uRPF packet loss rate, in packets per second. The value range is from 0 to 4294967295. If the threshold is **0**, a notification is sent for every packet that is discarded because it fails in the uRPF check.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the threshold of the uRPF packet loss rate to 10 packets per second on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet0/1
Hostname(config-if-GigabitEthernet 0/1)# ip verify urpf drop-rate notify
Hostname(config-if-GigabitEthernet 0/1)# ip verify urpf notification threshold 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8   show ip urpf

Function

Run the **show ip urpf** command to display the IPv4 uRPF configurations and statistics.

Syntax

show ip urpf [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-type interface-number*: Specifies the interface whose configurations and statistics are displayed. If this parameter is not specified, configurations and statistics of all interfaces are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the uRPF configurations and statistics on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show ip urpf interface gigabitethernet0/1
IP verify source reachable-via RX
IP verify URPF drop-rate notify is disabled
IP verify URPF notification threshold is 1000pps
Number of drop packets in this interface is 124
Number of drop-rate notification counts in this interface is 2
```

The following example displays IPv4 uRPF configurations and statistics on all interfaces.

```
Hostname> enable
Hostname# show ip urpf
IP verify URPF drop-rate compute interval is 30s
IP verify URPF drop-rate notify hold-down is 300s
Interface GigabitEthernet 0/1
IP verify source reachable-via RX
IP verify URPF drop-rate notify is disabled
IP verify URPF notification threshold is 1000pps
Number of drop packets in this interface is 124
Number of drop-rate notification counts in this interface is 2
```

Table 1-1Output Fields of the show ip urpf Command

Field	Description
IP verify URPF drop-rate compute interval is x	Interval for calculating the packet loss rate
IP verify URPF drop-rate notify hold-down is x	Alarm interval of the packet loss rate
Interface *interface-type interface-number*	Type and number of the interface whose uRPF configurations and statistics are displayed
IP verify source reachable-via *mode*	● When *mode* is set to **RX**, the uRPF strict mode is used. ● When *mode* is set to **ANY**, the uRPF loose mode is used.
IP verify URPF drop-rate notify *status*	Packet loss information monitoring status: ● When *status* is set to **enabled**, packet loss information monitoring is enabled. ● When *status* is set to **disabled**, packet loss information monitoring is disabled.
IP verify URPF notification threshold is *number*pps	Threshold of the uRPF packet loss rate
Number of drop packets in this interface is *number*	Number of lost packets
Number of drop-rate notification counts in this interface is *count*	Number of notifications for uRPF packet loss information monitoring

Notifications

N/A

Platform Description

N/A