Contents

1 Configuring uRPF

1.1 Introduction

1.1.1 Overview

Unicast Reverse Path Forwarding (uRPF) is a function that protects the network against source address spoofing.

uRPF obtains the source address and inbound interface of a received packet and searches for a forwarding entry in the forwarding table based on the source address. If no entry is configured, the packet is discarded. In uRPF strict mode, if the outbound interface of the forwarding entry does not match the inbound interface of the packet, the packet is also discarded.

1.1.2 Principles

1. Basic Concepts

- uRPF strict mode

  uRPF obtains the source address and inbound interface of a received packet and searches for a forwarding entry in the forwarding table based on the source address. If the entry does not exist, the packet is discarded. If the outbound interface of the forwarding entry does not match the inbound interface of the packet, the packet is also discarded. The strict mode requires that the inbound interface of a received packet must be the outbound interface of the route entry to the source address of the packet.

  The uRPF strict mode is often deployed on a point-to-point (P2P) interface, and inbound and outbound data streams must go through the network of the P2P interface. uRPF blocks the packets with spoofed source addresses at the access layer or aggregation layer to prevent sending such packets from PCs to the core network.

- uRPF loose mode

  uRPF reversely searches for a route based on the source IP address of a received packet. The outbound interface of the next hop on the route does not need to be the inbound interface of the received packet. However, the route cannot be a route of a host on the local network.

  The loose mode is applicable to asymmetric routes or multi-homed networks with asymmetric traffic. On a multi-homed network, the user network is connected to multiple Internet service providers (ISPs), and the inbound and outbound traffic is not symmetric. To prevent invalid packets from attacking the user network, deploy the uRPF loose mode on the outbound interface connected to ISPs.

- uRPF packet loss rate

  The uRPF packet loss rate is the number of packets discarded due to the uRPF check per second. The unit is packets/second, that is, pps.

- Interval for calculating the uRPF packet loss rate

  It refers to the interval from the previous time the packet loss rate is calculated to the current time the packet loss rate is calculated.

- Sampling interval of the uRPF packet loss rate

  It refers to the interval at which the number of lost packets is collected for calculating the packet loss rate. This interval must be greater than or equal to the interval for calculating the packet loss rate.

- Threshold of the uRPF packet loss rate

  It refers to the maximum packet loss rate that is acceptable. When the packet loss rate exceeds the threshold, alarms can be sent to users through syslogs or trap messages. You can adjust the threshold of the packet loss rate based on the actual network conditions.

- Alarm interval of the uRPF packet loss rate

  It refers to the interval at which alarms are sent to users. You can adjust the alarm interval based on the actual network conditions to prevent frequent output of logs or trap messages.

2. Enabling uRPF

Enable uRPF to perform a uRPF check on IP packets, thus protecting the device against source address spoofing.

uRPF can be configured in global or interface configuration mode.

Notice

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

- Global configuration mode

  After uRPF is enabled in global configuration mode, a device will perform a uRPF check for packets received over all interfaces of the device.

- Interface configuration mode

  uRPF is performed for packets received on the configured interface.

3. Notifying the uRPF Packet Loss Rate

To conveniently monitor lost packets after uRPF is enabled, the device uses syslogs or trap messages to proactively notify users of the packet loss information detected in the uRPF check.

In the period from the time when uRPF is enabled to the time when the sampling interval arrives, the packet loss rate is the number of lost packets measured within the sampling interval divided by the uRPF enabling time. After that, the packet loss rate is calculated as follows:
Current packet loss rate = (Current number of lost packets measured at the calculation interval – Number of lost packets measured before the sampling interval)/Sampling interval

1.1.3 Protocols and Standards

- RFC 2827: Network Ingress Filtering: DDOS Attacks which employ IP Source Address Spoofing
- RFC 3704: Ingress Filtering for Multi-homed Networks

1.2 Restrictions and Guidelines

- uRPF is implemented with the help of existing unicast routes in the network. Therefore, unicast routes must be configured in the network.
- uRPF checks only source addresses of packets whose destination addresses are unicast addresses and

does not check packets whose destination addresses are multicast or IPv4 broadcast addresses.

- uRPF cannot be enabled on a range of interfaces.
- uRPF does not check DHCP/BOOTP packets whose source IP address is 0.0.0.0 and destination IP address is 255.255.255.255.
- uRPF does not check loopback packets sent by the local device to itself.

1.3 Configuration Task Summary

uRPF configuration includes the following tasks:

(1)Enabling uRPF. Please configure only one task.

- Enabling Global uRPF
- Enabling uRPF on an Interface

(2)(Optional) Configuring uRPF Packet Loss Rate Advertisement. Configure at least one of the tasks.

- Configuring Global Packet Loss Rate Parameters
- Configuring Packet Loss Rate Parameters on an Interface

1.4 Enabling Global uRPF

1.4.1 Overview

After global uRPF is enabled, a uRPF check is performed for packets received over all interfaces of a device to protect the device against source address spoofing.

1.4.2 Restrictions and Guidelines

- 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 global uRPF is enabled, the default route cannot be used for the uRPF check.
- uRPF cannot be configured in global configuration mode and interface configuration mode simultaneously.

1.4.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enable global uRPF. Configure at least one of the tasks.

- Enable global IPv4 uRPF.

  ip verify unicast source reachable-via rx

  IPv4 uRPF is disabled by default.

1.5 Enabling uRPF on an Interface

1.5.1 Overview

uRPF is performed for packets received on the configured interface to prevent source address spoofing.

1.5.2 Restrictions and Guidelines

- Both the uRPF strict mode and loose mode can be configured on an interface.
- uRPF cannot be configured in global configuration mode and interface configuration mode simultaneously.
- The default route is not used for a uRPF check by default. You can configure **allow-default** to use the default route for a uRPF check if necessary.
- The uRPF strict mode supports matching of equal-cost routes. 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.
- After uRPF is enabled, the route forwarding capacity of a device will be reduced by half.
- 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.

1.5.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the interface configuration mode.

interface *interface-type interface-number*

(4)Enable uRPF for an interface. Configure at least one of the tasks.

- Enable IPv4 uRPF for an interface.

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

  IPv4 uRPF is disabled for an interface by default.

  support configuration of IPv4 uRPF on a routed port or L3 AP port.

1.6 Configuring uRPF Packet Loss Rate Advertisement

1.6.1 Overview

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.

1.6.2 Restrictions and Guidelines

uRPF must be enabled.

1.6.3 Configuration Tasks

Configure at least one of the tasks.

- Configuring Global Packet Loss Rate Parameters
- Configuring Packet Loss Rate Parameters on an Interface

1.6.4 Configuring Global Packet Loss Rate Parameters

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure global packet loss rate parameters. Configure at least one of the tasks.

- Configure the interval of calculating the uRPF IPv4 packet loss rate.

  ip verify urpf drop-rate compute interval *interval*

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

- Configure the alarm interval for the uRPF IPv4 packet loss rate.

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

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

1.6.5 Configuring Packet Loss Rate Parameters on an Interface

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure packet loss rate parameters on an interface. Configure at least one of the tasks.

- Enable uRPF packet loss information monitoring.

  ip verify urpf drop-rate notify

  uRPF packet loss information monitoring is disabled by default.

- Configure the threshold of the uRPF packet loss rate.

  ip verify urpf notification threshold *rate-value*

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

  If the threshold is **0**, a notification is sent for every packet that is discarded because it fails in the uRPF check.

1.7 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

Run the **debug** commands to output debugging information.

Notice

- Running the **clear** command during operation of the device may lose vital information and interrupt services.
- The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-1Monitoring

Command	Purpose
show ip urpf [**interface** *interface-type interface-number*]	Displays the IPv4 uRPF configurations and statistics.
clear ip urpf [**interface** *interface-type interface-number*]	Clears IPv4 uRPF packet loss statistics.
debug urpf event	Debugs uRPF events.
debug urpf timer	Debugs uRPF timers.

1.8 Configuration Examples

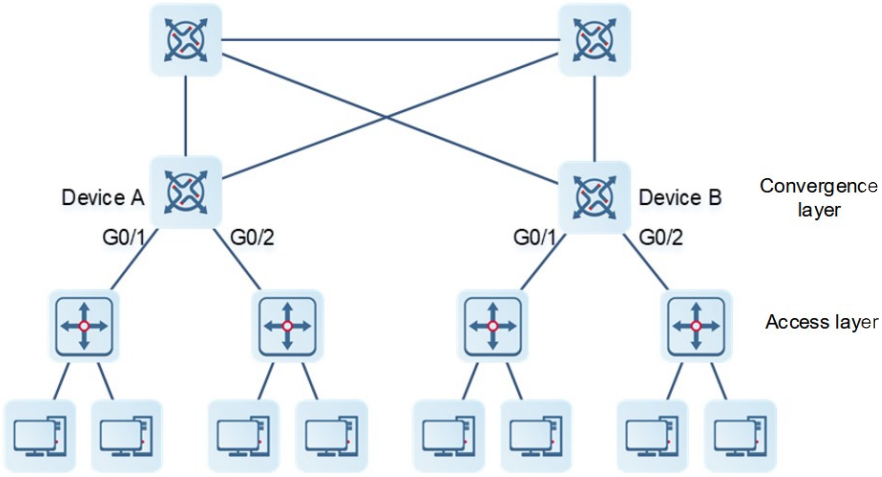
1.8.1 Configuring the uRPF Strict Mode

1. Requirements

In uRPF strict mode, packets with spoofed source addresses are blocked at the access layer or aggregation layer to prevent sending such packets from PCs to the core network.

2. Topology

Figure 1-1Configuring the uRPF Strict Mode



3. Notes

Enable the uRPF strict mode on the aggregation devices, including Devices A and B.

4. Procedure

(1)Configure Device A.

```
DeviceA> enable

DeviceA# configure terminal

DeviceA(config)# interface gigabitethernet0/1

DeviceA(config-if-GigabitEthernet 0/1)# ip address 195.52.1.1 255.255.255.0

DeviceA(config-if-GigabitEthernet 0/1)# ip verify unicast source reachable-via
rx

DeviceA(config-if-GigabitEthernet 0/1)# ip verify urpf drop-rate notify

DeviceA(config-if-GigabitEthernet 0/1)# exit

DeviceA(config)# interface gigabitethernet0/2

DeviceA(config-if-GigabitEthernet 0/2)# ip address 195.52.2.1 255.255.255.0

DeviceA(config-if-GigabitEthernet 0/2)# ip verify unicast source reachable-via
rx

DeviceA(config-if-GigabitEthernet 0/2)# ip verify urpf drop-rate notify

DeviceA(config-if-GigabitEthernet 0/2)# exit
```

(2)Configure Device B.

```
DeviceB> enable

DeviceB# configure terminal

DeviceB(config)# interface gigabitethernet0/1

DeviceB(config-if-GigabitEthernet 0/1)# ip address 195.52.3.1 255.255.255.0

DeviceB(config-if-GigabitEthernet 0/1)# ip verify unicast source reachable-via
rx

DeviceB(config-if-GigabitEthernet 0/1)# ip verify urpf drop-rate notify

DeviceB(config-if-GigabitEthernet 0/1)# exit

DeviceB(config)# interface gigabitethernet0/2

DeviceB(config-if-GigabitEthernet 0/2)# ip address 195.52.4.1 255.255.255.0

DeviceB(config-if-GigabitEthernet 0/2)# ip verify unicast source reachable-via
rx

DeviceB(config-if-GigabitEthernet 0/2)# ip verify urpf drop-rate notify

DeviceB(config-if-GigabitEthernet 0/2)# exit
```

5. Verification

If source address spoofing exists on the network, run the **show ip urpf** command to display the number of spoofing packets discarded by uRPF.

Display the number of spoofing packets discarded by uRPF on GigabitEthernet 0/1 of Device A.

```
DeviceA# show ip urpf interface gigabitethernet 0/1

IP verify source reachable-via RX

IP verify URPF drop-rate notify is enabled

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 0
```

Display the number of spoofing packets discarded by uRPF on GigabitEthernet 0/2 of Device A.

```
DeviceA# show ip urpf interface gigabitethernet 0/2

IP verify source reachable-via RX

IP verify URPF drop-rate notify is enabled

IP verify URPF notification threshold is 1000pps

Number of drop packets in this interface is 133
```

```
Number of drop-rate notification counts in this interface is 0
```

Display the number of spoofing packets discarded by uRPF on GigabitEthernet 0/1 of Device B.

```
DeviceB# show ip urpf interface gigabitethernet 0/1

IP verify source reachable-via RX

IP verify URPF drop-rate notify is enabled

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 0
```

Display the number of spoofing packets discarded by uRPF on GigabitEthernet 0/2 of Device B.

```
DeviceB# show ip urpf interface gigabitethernet 0/2

IP verify source reachable-via RX

IP verify URPF drop-rate notify is enabled

IP verify URPF notification threshold is 1000pps

Number of drop packets in this interface is 250

Number of drop-rate notification counts in this interface is 0
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA

!

interface GigabitEthernet 0/1

 ip address 195.52.1.1 255.255.255.0

 ip verify unicast source reachable-via rx

 ip verify urpf drop-rate notify

!

interface GigabitEthernet 0/2

 ip address 195.52.2.1 255.255.255.0

 ip verify unicast source reachable-via rx

 ip verify urpf drop-rate notify

!
```

```
end
```

- Device B configuration file

```
hostname DeviceB

!

interface GigabitEthernet 0/1

 ip address 195.52.3.1 255.255.255.0

 ip verify unicast source reachable-via rx

 ip verify urpf drop-rate notify

!

interface GigabitEthernet 0/2

 ip address 195.52.4.1 255.255.255.0

 ip verify unicast source reachable-via rx

 ip verify urpf drop-rate notify

!

end
```

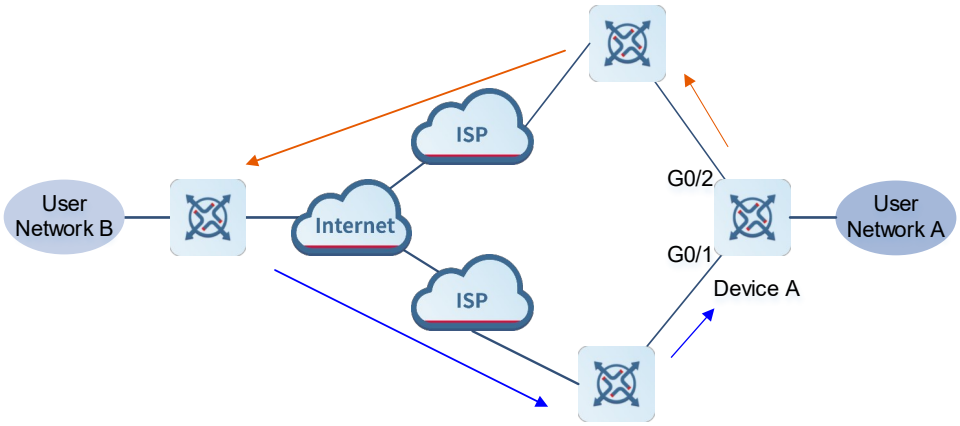
1.8.2 Configuring the uRPF Loose Mode

1. Requirements

To prevent invalid packets from attacking the user network, deploy the uRPF loose mode.

2. Topology

Figure 1-1Configuring the uRPF Loose Mode



3. Notes

Configure the uRPF loose mode on the outbound interfaces connected to ISPs.

4. Procedure

Enable the uRPF loose mode on GigabitEthernet 0/1 and GigabitEthernet 0/2.

```
DeviceA> enable

DeviceA# configure terminal

DeviceA(config)# interface gigabitethernet0/1

DeviceA(config-if-GigabitEthernet0/1)# ip address 195.52.1.2 255.255.255.252

DeviceA(config-if-GigabitEthernet0/1)# ip verify unicast source reachable-via any

DeviceA(config-if-GigabitEthernet0/1)# ip verify urpf drop-rate notify

DeviceA(config-if-GigabitEthernet0/1)# exit

DeviceA(config)# interface gigabitethernet0/2

DeviceA(config-if-GigabitEthernet0/2)# ip address 152.95.1.2 255.255.255.252

DeviceA(config-if-GigabitEthernet0/2)# ip verify unicast source reachable-via any

DeviceA(config-if-GigabitEthernet0/2)# ip verify urpf drop-rate notify

DeviceA(config-if-GigabitEthernet0/2)# end
```

5. Verification

If source address spoofing exists on the network, run the **show ip urpf** command to display the number of spoofing packets discarded by uRPF.

```
DeviceA# show ip urpf

IP verify URPF drop-rate compute interval is 300s

IP verify URPF drop-rate notify hold-down is 300s

Interface gigabitEthernet0/1

IP verify source reachable-via ANY

IP verify URPF drop-rate notify is enabled

IP verify URPF notification threshold is 1000pps

Number of drop packets in this interface is 4121

Number of drop-rate notification counts in this interface is 2

Interface gigabitEthernet0/2
```

```
IP verify source reachable-via ANY

IP verify URPF drop-rate notify is enabled

IP verify URPF notification threshold is 1000pps

Number of drop packets in this interface is 352

Number of drop-rate notification counts in this interface is 0
```

6. Configuration Files

Device A configuration file

```
hostname DeviceA

!

interface GigabitEthernet 0/1

 ip address 195.52.1.2 255.255.255.252

 ip verify unicast source reachable-via any

 ip verify urpf drop-rate notify

!

interface GigabitEthernet 0/2

 ip address 152.95.1.2 255.255.255.252

 ip verify unicast source reachable-via any

 ip verify urpf drop-rate notify

!

end
```