CHAPTER 13

Unicast Reverse Path Forwarding

Cisco integrated security systems incorporate a comprehensive selection of feature-rich security services, offering commercial, enterprise and service provider customers the ability to deploy trusted and protected business applications and services.

Threat defense is a critical aspect of an integrated security approach and involves the implementation of proactive measures. One valuable threat defense tool is unicast Reverse Path Forwarding (uRPF).

The key function of uRPF is to verify that the path of an incoming packet is consistent with the local packet forwarding information. This is achieved by performing a reverse path look-up (hence the feature's name) using the source IP address of an incoming packet to determine the current path (adjacency) to that IP address. The validity of this path determines whether uRPF passes or drops the packet.

The specific uRPF path validation criteria that is used to determine path consistency is dependent upon the particular uRPF mode enabled on an interface. Table 13-1 shows two uRPF modes which are supported by Cisco 10000 series routers.

Table 13-1 Three uRPF Modes

uRPF Mode	Path Resolution Table	uRPF Path Selection Criteria
Strict	CEF FIB	Path to the source IP address must be through the SAME interface as that on which the packet arrived
Loose	CEF FIB	Path to the source IP address is through *any* interface on the device

If the path is:

- Valid—the packet will be passed.
- Invalid—the packet is silently discarded.

uRPF uses the Cisco Express Forwarding (CEF) Forwarding Information Base (FIB) to perform reverse path look-up on the source IP address of an incoming packet. The CEF FIB is a database of network layer routing information and associated forwarding/adjacency information used in the CEF switching of packets. The CEF FIB is populated with the path for all known IP prefixes and their associated adjacencies. It is thus a key element of uRPF reverse path validation. After enabled on an interface, uRPF checks all IP packets on the input path of that interface.

Note Cisco 10000 series routers support both strict and loose mode uRPF for IPv4. However, for IPv6, the router supports only strict uRPF.

The uRPF feature is described in the following topics:

- Feature History for uRPF, page 13-12
- Prerequisites for uRPF, page 13-12
- Restrictions for uRPF, page 13-12
- Configuring Unicast RPF, page 13-13
- Monitoring and Maintaining uRPF, page 13-14
- Configuration Examples of uRPF, page 13-16

Feature History for uRPF

Cisco IOS Release	Description	Required PRE
12.2(27)SBB	This feature was introduced on the Cisco 10000 series router with strict mode only.	PRE2
12.2(33) SB	This feature was integrated on Cisco 10000 with both strict and loose modes for IPv4 traffic.	PRE2, PRE3, and PRE4

Prerequisites for uRPF

Before you configure uRPF on a router, ensure that the interface supports IP addressing. For a broadband interface, uRPF configurations must be added in the virtual template with all of the other IP configurations.

Restrictions for uRPF

The uRPF feature in Cisco 10000 has the following restrictions:

- Clients should not be multihomed to the same router because multihoming defeats the purpose of building a redundant service for the client.
- Customers must ensure that the packets flowing up the link (out to the Internet) match the route advertised out the link. Otherwise, Unicast RPF filters those packets as malformed packets.
- Unicast RPF is available only for platform images that support CEF. Unicast RPF is supported in Cisco IOS Releases 11.1(17)CC, 12.0, and later. It is not available in Cisco IOS Release 11.2 or 11.3.
- Unicast RPF is not supported by MPLS. It is supported only by IP traffic—IPv4 and IPv6. However, IPv6 supports uRPF in strict mode only, with the allow-default option on.
- Unicast RPF does not support access control lists (ACLs).
- Unicast RPF requires Cisco express forwarding (CEF) to function properly on the router. For more information about CEF, see the Cisco IOS Switching Services Configuration Guide.

- By default, without uRPF provision urpf drops can be seen in pxf when:
  - the interface is not up
  - there is no ip address on the interface

Configuring Unicast RPF

To use Unicast RPF, you must configure the router for CEF switching or CEF distributed switching. There is no need to configure the input interface for CEF switching because Unicast RPF has been implemented as a search through the FIB using the source IP address. As long as CEF is running on the router, individual interfaces can be configured with other switching modes. Unicast RPF is an input-side function that is enabled on an interface or subinterface that supports any type of encapsulation and operates on IP packets received by the router. It is very important that CEF be turned on globally in the router—Unicast RPF will not work without CEF.

To configure Unicast RPF, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# ip cef`	Enables CEF on the router. You might want to disable CEF on a particular interface if that interface is configured with a feature that CEF does not support. You can enable CEF globally, but disable CEF on a specific interface by using the **no ip route-cache cef** interface command that enables all but that specific interface to use express forwarding. If you have disabled CEF operation on an interface and want to reenable it, you can use the **ip route-cache cef** command in interface configuration mode.
Step 2	`Router(config-if)# interface` *type*	Selects the input interface on which you want to apply Unicast RPF. This is the receiving interface, which allows Unicast RPF to verify the best return path before forwarding the packet on to the next destination. The interface type is specific to your router and the types of interface cards installed on the router. To display a list of available interface types, enter the **interface ?** command.

Step 3	`Router(config-if)# ip verify unicast source reachable-via any`
	or
	`Router(config-if)# ip verify unicast source reachable-via rx`
		Enables Unicast RPF on the interface.
		The **any** option enables a Loose Mode uRPF on the router. This mode allows the router to reach the source address via any interface.
		The **rx** option enables a Strict Mode uRPF on the router. This mode ensures that the router reaches the source address only via the interface on which the packet was received.
		You can also use the **allow-default** option, so that the default route can match when checking source address. The **allow-self-ping option** allows the router to ping itself.

Step 4	`Router(config-if)# exit`	Exits interface configuration mode. Repeat Steps 2 and 3 for each interface on which you want to apply Unicast RPF.

Note You can use default route to configure a default path for all addresses that are not in the regular routing table. When configuring uRPF, you can use the allow-default option to allow ip packets with the source address resolved to a valid default path, depending on the uRPF modes. In strict mode uRPF, the packets are allowed from the same interface that has been pointed by the default route. In loose mode uRPF, packets with the source address resolved to the default route are allowed. However, if there is no default route provisioned in the router, the allow-default option on or off would not make any difference regardless of the uRPF mode as there is no valid default path.

Monitoring and Maintaining uRPF

Unicast RPF counts the number of packets dropped or suppressed because of malformed or forged source addresses. Unicast RPF counts dropped or forwarded packets that include the following global and per-interface information:

- Global Unicast RPF drops
- Per-interface Unicast RPF drops

After you enable uRPF on a router, you can monitor the number of packets getting dropped by the router using the following commands.

Command	Description
Router# **show ip traffic**	Displays global router statistics about Unicast RPF drops and suppressed drops.
Router# **show ip interface** *type*	Displays per-interface statistics about Unicast RPF drops and suppressed drops.
Router# **show pxf cpu statistics drop** *interface*	Displays drop counters by pxf for a given interface, even without uRPF provision and if the interface is not up or does not have an IP address.

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco Systems technical support personnel. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.

Example 13-1 shows the total number (global count) of dropped packets for all interfaces on the router using the show ip traffic command. The Unicast RPF drop count is included in the IP statistics section.

Example 13-1 show ip traffic Command

```
Router# show ip traffic

IP statistics:
  Rcvd:  1753234 total, 1163482 local destination
         0 format errors, 0 checksum errors, 0 bad hop count
         1162010 unknown protocol, 523362 not a gateway
         0 security failures, 0 bad options, 0 with options
  Opts:  0 end, 0 nop, 0 basic security, 0 loose source route
         0 timestamp, 0 extended security, 0 record route
         0 stream ID, 0 strict source route, 0 alert, 0 cipso, 0 ump
         0 other
  Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
         0 fragmented, 0 couldn't fragment
  Bcast: 331512 received, 0 sent
  Mcast: 0 received, 0 sent
  Sent:  15 generated, 0 forwarded
  Drop:  0 encapsulation failed, 0 unresolved, 0 no adjacency
         0 no route, 5 unicast RPF, 0 forced drop, 0 unsupported-addr
         0 options denied, 0 source IP address zero
```

A nonzero value for the count of dropped or suppressed packets can mean one of two things:

- Packets have a bad source address (normal operation).
- Router is misconfigured to use Unicast RPF in environments where asymmetric routing exists; that is, where multiple paths can exist as the best return path for a source address.

Note The RPF counter increases when the source address resolves to a NULL 0 because the address is then considered as spoof.

Example 13-2 shows the total of dropped or suppressed packets at a specific interface using the show ip interface command.

Example 13-2 show ip interface Command

```
Router> show ip interface gigabitEthernet 8/1/0

GigabitEthernet8/1/0 is up, line protocol is up
  Internet address is 80.1.1.1/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF switching turbo vector
  IP CEF turbo switching turbo vector
  Associated unicast routing topologies:
        Topology "base", operation state is UP
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  Input features: uRPF
  IP verify source reachable-via ANY
   5 verification drops
   5 suppressed verification drops
   0 verification drop-rate
```

Example 13-3 shows how uRPF drops can also be seen at the PXF using the show pxf cpu statistics drop interface command.

Example 13-3 show pxf cpu statistics drop interface Command

```
router# sh pxf cpu statistics drop g8/1/0
FP drop statistics for GigabitEthernet8/1/0
                            packets            bytes
    vcci undefined          0                  0
    bad vlan id             0                  0
  vcci 9E6
    in l2 max mtu           0                  0
    in l2 min mtu           0                  0
    encap not supported     0                  0
    mlfr fragament          0                  0
    mpls not enabled        0                  0
    ip version              0                  0
    ip header length        0                  0
    ip length max           0                  0
    ip length min           0                  0
    ip checksum             0                  0
    fib rpf fail            0                  0
    acl denied              0                  0
    ttl                     0                  0
    unreachable             0                  0
    df multicast            0                  0
    police input drop       0                  0
    police output drop      0                  0
    out l2 max mtu          0                  0
    out l2 min mtu          0                  0
    tunnel no match         0                  0
    iedge input drop(s)     0                  0
    iedge output drop(s)    0                  0
```

Configuration Examples of uRPF

This section provides the following configuration examples:

- Configuring Loose Mode uRPF
- Configuring Loose Mode uRPF with the allow-self-ping Option
- Configuring Loose Mode uRPF with the allow-default Option

Configuring Loose Mode uRPF

Example 13-4 shows how to enable Loose Mode uRPF on a router over the Gigabit Ethernet Interface:

Example 13-4 Loose Mode uRPF configuration on 8/1/0 interface

```
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router (config)# int g8/1/0
Router (config-if)# ip verify unicast source reachable-via?
  any Source is reachable via any interface
  rx   Source is reachable via interface on which packet was received

Router (config-if)# ip verify unicast source reachable-via any?
  <1-199>          IP access list (standard or extended)
  <1300-2699>      IP expanded access list (standard or extended)
  allow-default    Allow default route to match when checking source address
  allow-self-ping  Allow router to ping itself (opens vulnerability in
                   verification)
  <cr>

Router (config-if)# ip verify unicast source reachable-via any
Router (config-if)# end
```

Example 13-5 shows how you can use the show router interface command for verifying that Loose Mode uRPF has been configured on a router

Example 13-5 Verifying Loose Mode uRPF on 8/1/0 interface

```
Router# sh ru interface gig8/1/0
!
interface GigabitEthernet8/1/0
 ip address 80.1.1.1 255.255.255.0
 ip verify unicast source reachable-via any
 negotiation auto
end
```

Configuring Loose Mode uRPF with the allow-self-ping Option

Example 13-6 shows how you can configure Loose Mode uRPF with the allow-self-ping option.

Example 13-6 Loose Mode uRPF with the allow-self-ping option

```
Router(config)# int g8/1/0
Router(config-if)# ip verify unicast source reachable-via any allow-self-ping
Router(config-if)# end
Router# sh ru int g8/1/0
!
interface GigabitEthernet8/1/0
 ip address 80.1.1.1 255.255.255.0
 ip verify unicast source reachable-via any allow-self-ping
 negotiation auto
end
```

Note After you enable the interface with uRPF using the allow-self ping option, initiate a self-ping to see whether the self-ping option is successful.

Configuring Loose Mode uRPF with the allow-default Option

Example 13-7 shows how you can configure Loose Mode uRPF with the allow-default option.

Example 13-7 Loose Mode uRPF with the allow-default option

```
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# int g8/1/0
Router(config-if)# ip verify unicast source reachable-via any allow-default
Router(config-if)# end
Router# sh ru int gig8/1/0
!
interface GigabitEthernet8/1/0
 ip address 80.1.1.1 255.255.255.0
 ip verify unicast source reachable-via any allow-default
 negotiation auto
end
```

Note For configuring Strict mode uRPF, replace the any keyword with rx in the ip verify unicast source reachable-via command.