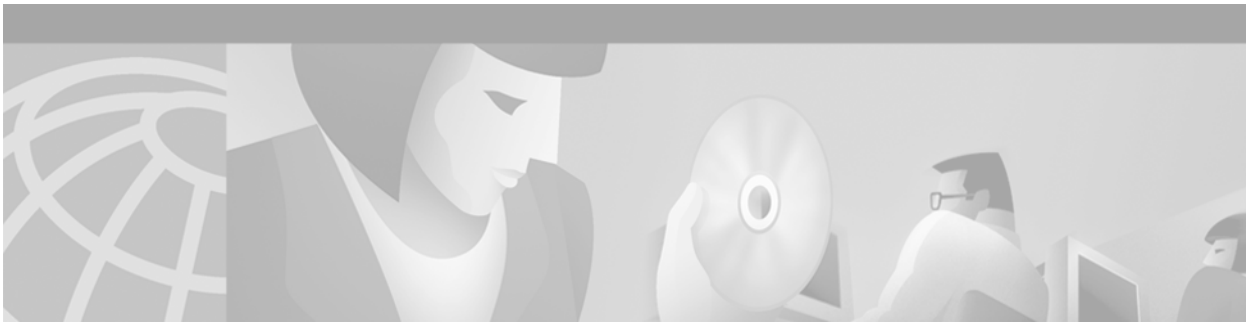

URPF MIB

This feature module describes the addition of URPF MIB support using Simple Network Management Protocol (SNMP) in Cisco IOS Release 12.0(32)S. It includes information on the benefits of the new feature, supported platforms, supported standards, and the new and modified Cisco IOS commands used to enable URPF monitoring.

This document includes the following sections:

Feature Overview

This release introduces support for the new CISCO-IP-URPF-MIB. The IP Unicast Reverse Path Forwarding MIB provides objects for notification whenever drop rates exceed a customer-determined threshold. The cipUrpfIfDropRateNotifyEnable object enables notifications when set to true using an SNMP SET command. The default is false.

The cipUrpfIfDropRateNotifyEnable object determines whether any check is made to see whether drop-rate exceeds the configured threshold. If this object is FALSE, no NOTIFY will be generated for that interface and packet flow.

The thresholds are configured using the SNMP SET command on the following global MIB objects:

- cipUrpfDropRateWindow

The cipUrpfDropRateWindow object specifies the window of time over which the computation of the drop rate takes place.

- cipUrpfComputeInterval

The cipUrpfComputeInterval object specifies how often the drop rate computation occurs. This should be set as large as possible.

- cipUrpfDropNotifyHoldDownTime

The cipUrpfDropNotifyHoldDownTime object specifies the minimum time between notifications for a particular packet flow on an interface. This should also be set as large as possible.

The cipUrpfIfNotifyDropRateThreshold object specifies the drop rate threshold value above which a NOTIFY is sent to the SNMP manager.

The Unicast Reverse Path Forwarding feature verifies if the source IP is reachable in order to prevent malformed or forged source IP addresses from entering a network. When a packet is received, this feature determines if its source IP can be reached via the same (or any other) real interface. When enabled on an interface, any packets that have source addresses that are not found in the routing table are dropped.

There is a new IOS command introduced with this feature which is used to specify a URPF drop-rate threshold on interfaces of a managed device, which when exceeded causes a NOTIFY to be sent to a management station.

New and Changed IOS Commands

Changed Interface Command

An addition is made to the output of the **show ip interface** command when URPF is enabled on the interface. The line:

```
xxxxxx verification drop-rate
```

is added when URPF is enabled.

Command Modes Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.0(32)S	Output updated to display the URPF drop rate

Examples The following is sample output from the show ip interface command:

Router# show ip interface

```
Ethernet0 is up, line protocol is up
  Hardware is MCI Ethernet, address is 0000.0c00.750c (bia 0000.0c00.750c)
  Internet address is 1.0.46.10, subnet mask is 255.0.0.0
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is enabled
  Multicast groups joined: 224.0.0.1 224.0.0.2
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  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 fast switching on the same interface is disabled
  IP SSE switching is disabled
  Router Discovery is disabled
  IP accounting is disabled
  TCP/IP header compression is disabled
  Probe proxy name replies are disabled
  Gateway Discovery is disabled
Serial0 is up, line protocol is up
  Internet address is 198.135.2.49, subnet mask is 255.255.255.0
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is enabled
  Multicast groups joined: 224.0.0.1 224.0.0.2
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  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 fast switching on the same interface is disabled
  IP SSE switching is disabled
  Router Discovery is disabled
  IP accounting is disabled
  TCP/IP header compression is disabled
  Probe proxy name replies are disabled
  Gateway Discovery is disabled
  55000 verification drop-rate
```

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router or access server.

New Global CLI Commands

The following three global CLI commands are added to this release to support the configuration of URPF on the interface.

[no] ip verify drop-rate compute window <window-val>

30 <= window-val <= 300; unit is seconds

Command Modes Privileged EXEC

Command History

Release	Modification
12.0(32)S	This command was introduced.

Defaults This command is disabled by default (no drop notifications are being tallied to get a drop rate).

If you enter this command with no keywords or the **compute window** keyword is present with no **<window-val>** specified, the default window size is 300 seconds.

The window-val parameter defines the window of time in the recent past over which the drop count used in the drop rate computation is collected. This global value applies for the computation of all URPF rates, global and per-interface. The “compute window” value must be greater than or equal to the “compute interval” value. The range is between 30 to 300 seconds.

[no] ip verify drop-rate compute interval <interval-val>

30 <= interval-val <= 300; unit is seconds

Command Modes Privileged EXEC

Command History

Release	Modification
12.0(32)S	This command was introduced.

Defaults This command is disabled by default (no notifications are sent, so no need to define the time between drop rate computations).

If you enter this command with no keywords or the **compute interval** keyword is present with no **<interval-val>** specified, the default time between drop rate computations value is 30 seconds.

The interval-val parameter defines the time between drop rate computations. This global value applies for the computation of all URPF rates, global and per-interface. The “compute interval” value must be less than or equal to the “compute window” value. The range is between 30 to 300 seconds.

[no] ip verify drop-rate notify hold-down <hold-val>

30 <= hold-val <= 300; unit is seconds

Command Modes Privileged EXEC

Command History

Release	Modification
12.0(32)S	This command was introduced.

Defaults This command is disabled by default (no notifications are sent, so no need to define the minimum time between issuance of drop rate notifications for a particular interface and packet forwarding type).

If you enter this command with no keywords or the **hold-down** keyword is present with no **<hold-val>** specified, the default minimum time between issuance of drop rate notifications value is 300 seconds.

The hold-val parameter defines the minimum time between issuance of drop rate notifications for a particular interface and packet forwarding type. The default interval is 300 seconds. The range is between 30 to 300 seconds

New Interface Configuration CLI Command

New Interface CLI commands are:

[no] snmp trap ip verify drop-rate

Command Modes Privileged EXEC

Command History

Release	Modification
12.0(32)S	This command was introduced.

Defaults This command enables the sending of SNMP Notify messages (traps) when the URPF drop rate for IPv4 packets on the interface exceeds the drop-rate threshold. The default behavior is disabled (no SNMP Notify messages are sent).

This command specifies the threshold value used to determine whether or not to send a Notify for URPF rate. If the recent rate meets or exceeds this value, and "notify enable" is configured, a Notify is sent to the management station. If the threshold value is set to 0, a SNMP Notify message is sent whenever any packet drops occur.

Benefits

Allows the monitoring of UPRF activity through network management applications.

Restrictions

The CISCO-IP-URPF-MIB supports IPv4 and IPv6, however URPF packet flow instrumentation is not supported on IPv6.

Related Features and Technologies

- Unicast Reverse Path Forwarding (URPF)
- Simple Network Management Protocol (SNMP)

Related Documents

For information about UPRF, see the chapter "Configuring Unicast Reverse Path Forwarding" in the *Cisco IOS Security Configuration Guide* document.

For information about SNMP, see the chapter "Monitoring the Router and Network" in the *Configuration Fundamentals Configuration Guide*, Release 12.0.

Supported Platforms

The UPRF MIB is supported on Cisco IOS Release 12.0(32)S on the following platforms:

- Cisco 12000 series routers

Supported Standards, MIBs, and RFCs

Standards

No standards are supported for this feature.

MIBs

UPRF MIB support consists of the following MIBs and related files:

- CISCO-IP-URPF-MIB.my

For MIB implementation details, refer to the CISCO-IP-URPF-MIB.my file, available through the Cisco MIB FTP site at the following URL:

ftp://ftp.cisco.com/pub/mibs/v2/.

RFCs

RFC 2267, *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*

Glossary

Management Information Base—See MIB.

MIB—Management Information Base. A database of network management information that is used and maintained by a network management protocol such as SNMP. The value of a MIB object can be changed or retrieved using SNMP commands, usually through a network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

Simple Network Management Protocol—See SNMP.

SNMP—Simple Network Management Protocol. Management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

trap—A message sent by an SNMP agent to a network management station, console, or terminal to indicate the occurrence of a significant event, such as a specifically defined condition or a threshold that was reached.

Unicast Reverse Path Forwarding—See URPF.

URPF—Unicast Reverse Path Forwarding. A feature that verifies if the source IP is reachable in order to prevent malformed or forged source IP addresses from entering a network. When a packet is received, this feature determines if its source IP can be reached via the same (or any other) real interface. When enabled on an interface, any packets that have source addresses that are not found in the routing table are dropped.