CISCO-IP-URPF-MIB Support

First Published: November 20, 2006
Last Updated: November 20, 2006

Customers use the IP Unicast Reverse Path Forwarding (URPF) feature to avert denial of service (DoS) attacks by verifying the validity of the source IP of an incoming packet. The CISCO-IP-URPF-MIB has been defined to provide Simple Network Management Protocol (SNMP) notification when a specified URPF drop-rate threshold on a managed device is exceeded. The URPF drop-rate threshold can be configured globally for a device, or per interface.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for CISCO-IP-URPF-MIB Support" section on page 28.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Contents

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for CISCO-IP-URPF-MIB Support

Cisco IOS support for the CISCO-IP-URPF-MIB requires the following to be configured on the device:

- U RPF
- Cisco Express Forwarding (CEF)
- IP Routing
- SNMP

Restrictions for CISCO-IP-URPF-MIB Support

- Because Cisco IOS does not support Virtual Private Network (VPN) routing and forwarding- (VRF)-specific URPF counters, the following MIB objects related to VRF are not supported:
  - cipUrpfIfVrfName
  - cipUrpfVrfName
  - cipUrpfVrfIfDrops
  - cipUrpfVrfIfDiscontinuityTime
- This implementation of the CISCO-IP-URPF MIB supports IPv4 only.

Information About CISCO-IP-URPF-MIB Support

To configure a notification threshold for URPF dropped packets, you should understand the following concepts:

- Implementing URPF Notification, page 2
- Software Basis for URPF Notification, page 3

Implementing URPF Notification

URPF is a security feature that verifies the validity of the source IP of an incoming packet. When a packet arrives at an interface and its source IP is unknown in the routing table or is a known bad source address, URPF drops the packet. Source IP verification is done to prevent denial of service (DoS) attacks by detecting problems with the incoming packets on an interface. However, URPF is challenging to deploy without some automated monitoring capability.

The CISCO-IP-URPF-MIB allows users to specify a URPF drop-rate threshold on interfaces of a managed device, which when exceeded causes an SNMP notification to be sent. This MIB includes objects for specifying global and per-interface drop counts and drop rates, as well as a means of generating SNMP traps when the drop rate exceeds a configurable per-interface threshold.

Although some parameters can be configured globally, this feature must be configured on individual interfaces.

Software Basis for URPF Notification

The following elements make URPF drop-rate notification work:

- Global Scalars
- Global Tables
- Per-interface Statistics
- Per-interface Configuration
- Drop-Rate Computation

Global Scalars

The following global scalars affect the behavior of the MIB agent in computing all drop rates and controlling notification generation:

- cipUrpfDropRateWindow

  This object specifies the window of time in the recent past over which the computation takes place. If there were no window (that is, the window is the epoch since booting up), an identical drop count burst at a later time would produce a smaller drop rate than one occurring earlier.

- cipUrpfComputeInterval

  This object specifies how often the drop-rate computation occurs.

- cipUrpfDropNotifyHoldDownTime

  This object specifies the minimum time between notifications for a particular packet flow on an interface.

Global Tables

The CISCO-IP-URPF-MIB includes the following global tables:

- cipUrpfTable

  This table contains global drop count and drop-rate objects per packet flow (for both IPv4 and IPv6). These global rates are useful for determining quickly whether there is URPF activity on the managed device at a specific time.

- cipUrpfVrfTable

  This table allows users to index drop counters by VRF, if a VRF routing table is used to determine URPF checking. The table provides a means to index all the URPF-enabled interfaces by VRF.

Per-interface Statistics

The following MIB objects track per-interface statistics:

- cipUrpfIfMonTable

  This table contains the statistics for a particular packet flow on an interface.

- cipUrpfIfDrops

  This object accumulates URPF drops on an interface. Snapshots of this value are used in the drop-rate computation. Computed drop rate is specified in the **cipUrpfIfDropRate** object. IfURPF is configured on a subinterface, drop rates are computed.

Per-interface Configuration

The following MIB objects enable per-interface configuration.

- cipUrpfIfDropRateNotifyEnable

  This object specifies whether the system produces the **cipUrpfIfDropRateNotify** notification because URPF has dropped of version **cipUrpfIfIpVersion** IP packets on the specified interface.

- cipUrpfIfNotifyDropRateThreshold

  This object specifies the drop-rate threshold value above which a notification is generated.

Drop-Rate Computation

Whenever URPF is configured on an interface, the drop-rate calculation is performed periodically (at intervals specified by the **cipUrpfComputeInterval** object). Drop rates are computed over a constantly sliding window, covering the period ending with the performance of the calculation and starting the configured number of seconds before the calculation.

How to Configure URPF Drop-Rate Notification

This section contains the following tasks:

- Configuring URPF Drop-Rate Notification via Syslog, page 4
- Configuring URPF Drop-Rate Notification via SNMP, page 6
- Verifying the URPF Configuration, page 7

Configuring URPF Drop-Rate Notification via Syslog

This task describes how to configure the URPF drop-rate threshold and computation parameters for notification via syslog.

Prerequisites

You must have URPF configured on the router before configuring this feature. For information about configuring URPF, see *Configuring Unicast Reverse Path Forwarding*.

Restrictions

This feature can be configured only with IPv4.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip verify drop-rate compute window** *seconds*
4. **ip verify drop-rate compute interval** *seconds*
5. **ip verify drop-rate notify hold-down** *seconds*

6. **configure interface** *type number*
7. **ip verify unicast notification threshold** *rate-val*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enters the privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip verify drop-rate compute window** *seconds* **Example:** `Router config# ip verify drop-rate compute window 60`	Configures the period of time, in seconds, over which the URPF drop count used in the drop-rate computation is collected. The range of the seconds argument is from 30 to 300. The default is 300. **Note** The value for the compute window must be greater than or equal to that entered for the **ip verify drop-rate compute interval** command.
Step 4	**ip verify drop-rate compute interval** *seconds* **Example:** `Router config# ip verify drop-rate compute interval 60`	Configures the interval of time, in seconds, between URPF drop-rate computations. The range of the seconds argument is from 30 to 300. The default is 30. **Note** The value for the compute interval must be less than or equal to that entered for the **ip verify drop-rate compute window** command.
Step 5	**ip verify drop-rate notify hold-down** *seconds* **Example:** `Router config# ip verify drop-rate notify hold-down 60`	Configures the minimum time, in seconds, between URPF drop-rate notifications. The range of the seconds argument is from 30 to 300. The default is 300.
Step 6	**configure interface** *type number* **Example:** `Router# configure interface ethernet 3/0`	Enters interface configuration mode.
Step 7	**ip verify unicast notification threshold** *rate-val* **Example:** `Router (config-if)# ip verify unicast notification threshold 750`	Configures the threshold value, in packets per second, used to determine whether to send a URPF drop-rate notification. The range is from 0 to the maximum number of packets the interface can process in 1 second. The default is 1000. **Note** If you configure the threshold to be 0, every packet drop will trigger a notification.

Configuring URPF Drop-Rate Notification via SNMP

This task describes how to configure the URPF drop-rate threshold and computation parameters for notification via SNMP.

Prerequisites

You must have URPF configured on the router before configuring this feature. For information about configuring URPF, see *Configuring Unicast Reverse Path Forwarding*.

You must enable SNMP on the router to use this feature. For information about enabling SNMP, see *Configuring SNMP Support*.

Restrictions

This feature can be configured only with IPv4.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip verify drop-rate compute window** *seconds*
4. **ip verify drop-rate compute interval** *seconds*
5. **ip verify drop-rate notify hold-down** *seconds*
6. **configure interface** *type number*
7. **ip verify unicast notification threshold** *rate-val*
8. **snmp trap ip verify drop-rate**

DETAILED STEPS

	Command or Action	Purpose
Step 1	`enable`	Enters the privileged EXEC mode.

Step 2	`configure terminal`
	
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`ip verify drop-rate compute window` *seconds* **Example:** `Router config# ip verify drop-rate compute window 60`	Configures the period of time, in seconds, over which the URPF drop count used in the drop-rate computation is collected. The range is from 30 to 300. The default is 300. **Note** The value for the compute window must be greater than or equal to that entered for the **ip verify drop-rate compute interval** command.

	Command or Action	Purpose
Step 4	**ip verify drop-rate compute interval** *seconds* **Example:** `Router config# ip verify drop-rate compute interval 60`	Configures the interval of time, in seconds, between URPF drop-rate computations. The range is from 30 to 300. The default is 30. **Note** The value for the compute interval must be less than or equal to that entered for the **ip verify drop-rate compute window** command
Step 5	**ip verify drop-rate notify hold-down** *seconds* **Example:** `Router config# ip verify drop-rate notify hold-down 60`	Configures the minimum time, in seconds, between URPF drop-rate notifications. The range is from 30 to 300. The default is 300.
Step 6	**configure interface** *type number* **Example:** `Router# configure interface ethernet 3/0`	Enters interface configuration mode.
Step 7	**ip verify unicast notification threshold** *rate-val* **Example:** `Router (config-if)# ip verify unicast notification threshold 750`	Configures the threshold value, in packets per second, used to determine whether to send a URPF drop-rate notification. The range is from 0 to the maximum number of packets the interface can process in 1 second. The default is 1000. **Note** If you configure the threshold to be 0, every packet drop will trigger a notification.
Step 8	**snmp trap ip verify drop-rate** **Example:** `Router (config-if)# snmp trap ip verify drop-rate`	Configures the router to send an SNMP notification when the URPF drop rate exceeds the configured threshold.

Verifying the URPF Configuration

You can use the following two commands to verify the URPF configuration and troubleshoot the operation of URPF drop-rate notification.

SUMMARY STEPS

1. **enable**
2. **show ip interface** *type number*
3. **debug ip verify mib**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode.
Step 2	**show ip interface** *type number* **Example:** `Router# show ip interface ethernet 3/0`	Displays the verification drop rate and the number of verification drops when URPF is configured for the specified interface.
Step 3	**debug ip verify mib** **Example:** `Router# debug ip verify mib`	Displays output useful for troubleshooting URPF notification.

Examples

The last five lines in following example shows the output of the **show ip interface** command when URPF is configured:

```
Router# show ip interface ethernet 2/3

Ethernet2/3 is up, line protocol is up
  Internet address is 9.9.5.4/16
  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 disabled
  IP Flow switching is disabled
  IP CEF switching is disabled
  IP Null turbo vector
  IP Null turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are No 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
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
```

```
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
  Input features: uRPF
  IP verify source reachable-via RX, allow default
   0 verification drops
   0 suppressed verification drops
   0 verification drop-rate
router#
```

The following example shows the output of the **debug ip verify mib** command:

```
Router# debug ip verify mib

01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: ipurpfmib_get_scalars
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: ipurpfmib_get_scalars
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: ipurpfmib_get_scalars
01:29:45: cipUrpfScalar_get, searchType
161ipurpfmib_get_urpf_entryipurpfmib_get_urpf_entryipurpfmib_get_urpf_entryipurpfmib_get_
urpf_entry
01:29:45: cipUrpfIfMonEntry_get, searchType 161
01:29:45: ipurpfmib_get_urpf_ifmon_entry entry: ST 161, if 1, ip 1
01:29:45: cipUrpfIfMonEntry_get, searchType 161
01:29:45: ipurpfmib_get_urpf_ifmon_entry entry: ST 161, if 1, ip 1
01:29:45: cipUrpfIfMonEntry_get, searchType 161
01:29:45: ipurpfmib_get_urpf_ifmon_entry entry: ST 161, if 1, ip 1
01:29:45: cipUrpfIfMonEntry_get, searchType 161
01:29:45: ipurpfmib_get_urpf_ifmon_entry entry: ST 161, if 1, ip 1
01:29:45: cipUrpfIfMonEntry_get, searchType 161
01:29:45: ipurpfmib_get_urpf_ifmon_entry entry: ST 161, if 1, ip 1
01:29:45: cipUrpfIfMonEntry_get, searchType 161
01:29:45: ipurpfmib_get_urpf_ifmon_entry entry: ST 161, if 1, ip 1
01:29:45: cipUrpfIfMonEntry_get, searchType 161
01:29:45: ipurpfmib_get_urpf_ifmon_entry entry: ST 161, if 1, ip 1
01:29:45: cipUrpfIfMonEntry_get, searchType 161
01:29:45: ipurpfmib_get_urpf_ifmon_entry entry: ST 161, if 1, ip 1
01:29:45: cipUrpfIfMonEntry_get, searchType 161
01:29:45: ipurpfmib_get_urpf_ifmon_entry entry: ST 161, if 1, ip 1
01:29:45: cipUrpfIfMonEntry_get, searchType 161
01:29:45: ipurpfmib_get_urpf_ifmon_entry entry: ST 161, if 1, ip 1
```

Configuration Examples for CISCO-IP-URPF-MIB Support

This section includes the following examples:

- Configuring URPF Drop-Rate Notification via Syslog: Example, page 10
- Configuring URPF Drop-Rate Notification via SNMP: Example, page 10

Configuring URPF Drop-Rate Notification via Syslog: Example

The following example shows how to configure URPF drop-rate notification via syslog:

```
configure terminal
ip verify drop-rate compute window 60
ip verify drop-rate compute interval 60
ip verify drop-rate hold-down 60
configure interface ethernet 3/0
interface ethernet 3/0
ip verify unicast notification threshold 750
```

Configuring URPF Drop-Rate Notification via SNMP: Example

The following example shows how to configure URPF drop-rate notification via SNMP:

```
configure terminal
ip verify drop-rate compute window 60
ip verify drop-rate compute interval 60
ip verify drop-rate hold-down 60
configure interface ethernet 3/0
interface ethernet 3/0
ip verify unicast notification threshold 750
snmp trap ip verify drop-rate
```

Additional References

The following sections provide references related to theCISCO-IP-URPF-MIB Support feature.

Related Documents

Related Topic	Document Title
Configuring Unicast Reverse Path Forwarding	*Configuring Unicast Reverse Path Forwarding*
Configuring SNMP	*Configuring SNMP Support*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
• CISCO-IP-URPF-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and technical documentation. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents new and modified commands only.

- **debug ip verify mib**
- **ip verify drop-rate compute interval**
- **ip verify drop-rate compute window**
- **ip verify drop-rate notify hold-down**
- **ip verify unicast notification threshold**
- **show ip interface**
- **snmp trap ip verify drop-rate**

debug ip verify mib

To view debug output that displays the operation of unicast reverse path forwarding (URPF) MIB objects and the helper software, use the **debug ip verify mib** command in privileged EXEC mode. To disable debugging for URPF, use the **no** form of this command.

debug ip verify mib

no debug ip verify mib

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(31)SB2	This command was introduced.

Usage Guidelines

Debug information for the URPF MIB is collected only when logging is enabled. URPF messages are stored in the logging buffer, and they are not displayed on the console unless you use the **debug ip verify mib** command.

Examples

The following example shows sample output of the **debug ip verify mib** command:

```
router# debug ip verify mib

01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: ipurpfmib_get_scalars
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: ipurpfmib_get_scalars
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: ipurpfmib_get_scalars
01:29:45: cipUrpfScalar_get, searchType 
161ipurpfmib_get_urpf_entryipurpfmib_get_urpf_entryipurpfmib_get_urpf_entryipurpfmib_get_
urpf_entry
01:29:45: cipUrpfIfMonEntry_get, searchType 161
01:29:45: ipurpfmib_get_urpf_ifmon_entry entry: ST 161, if 1, ip 1
01:29:45: cipUrpfIfMonEntry_get, searchType 161
01:29:45: ipurpfmib_get_urpf_ifmon_entry entry: ST 161, if 1, ip 1
01:29:45: cipUrpfIfMonEntry_get, searchType 161
01:29:45: ipurpfmib_get_urpf_ifmon_entry entry: ST 161, if 1, ip 1
01:29:45: cipUrpfIfMonEntry_get, searchType 161
01:29:45: ipurpfmib_get_urpf_ifmon_entry entry: ST 161, if 1, ip 1
01:29:45: cipUrpfIfMonEntry_get, searchType 161
01:29:45: ipurpfmib_get_urpf_ifmon_entry entry: ST 161, if 1, ip 1
01:29:45: cipUrpfIfMonEntry_get, searchType 161
01:29:45: ipurpfmib_get_urpf_ifmon_entry entry: ST 161, if 1, ip 1
01:29:45: cipUrpfIfMonEntry_get, searchType 161
01:29:45: ipurpfmib_get_urpf_ifmon_entry entry: ST 161, if 1, ip 1
```

```
01:29:45: cipUrpfIfMonEntry_get, searchType 161
01:29:45: ipurpfmib_get_urpf_ifmon_entry entry: ST 161, if 1, ip 1
01:29:45: cipUrpfIfMonEntry_get, searchType 161
01:29:45: ipurpfmib_get_urpf_ifmon_entry entry: ST 161, if 1, ip 1
01:29:45: cipUrpfIfMonEntry_get, searchType 161
01:29:45: ipurpfmib_get_urpf_ifmon_entry entry: ST 161, if 1, ip 1
```

The command output is self-explanatory.

Related Commands

Command	Description
show ip interface	Displays the usability status of interfaces configured for IP.

ip verify drop-rate compute interval

To configure the interval of time between unicast reverse path forwarding (URPF) drop rate computations, use the **ip verify drop-rate compute interval** command in global configuration mode. To reset the interval to the default value, use the **no** form of this command.

ip verify drop-rate compute interval *seconds*

no ip verify drop-rate compute interval

Syntax Description

seconds	Interval, in seconds, between URPF drop rate computations. The range is from 30 to 300. The default is 30.

Command Default

The drop rate is not computed.

Command Modes

Global configuration

Command History

Release	Modification
12.2(31)SB2	This command was introduced.

Usage Guidelines

This command configures the interval between URPF drop rate computations. The configured value applies for the computation of all URPF drop rates, global and per-interface. The value for the compute interval must be less than or equal to the value configured using the **ip verify drop-rate compute window** command.

If you configure the **no** form of the command while the **cipUrpfDropRateWindow** value is configured to be less than the default compute interval value, the following message appears on the console:

"urpf drop rate window < interval"

This error message means the command was not executed. The compute interval remains at the configured value rather than changing to the default value.

Examples

The following example shows how to configure a compute interval of 45 seconds:

```
ip verify drop-rate compute interval 45
```

Related Commands

Command	Description
ip verify drop-rate compute window	Configures the the interval of time over which the URPF drop count used in the drop rate computation is collected.

ip verify drop-rate compute window

To configure the interval of time over which the unicast reverse path forwarding (URPF) drop count used in the drop rate computation is collected, use the **ip verify drop-rate compute window** command in global configuration mode. To reset the window to the default value, use the **no** form of this command.

ip verify drop-rate compute window *seconds*

no ip verify drop-rate compute window

Syntax Description

seconds	Interval, in seconds, during which the URPF drop count is accumulated for the drop rate computation. The range is from 30 to 300. The default is 300.

Command Default

The drop rate is not calculated.

Command Modes

Global configuration

Command History

Release	Modification
12.2(31)SB2	This command was introduced.

Usage Guidelines

This command configures the sliding window that ends with the URPF drop rate computation and begins the configured number of seconds prior to the computation. The configured value applies for the computation of all URPF drop rates, global and per-interface. The value configured for the "compute window" must be greater than or equal to the value configured using the **ip verify drop-rate compute interval** command.

If you configure the **no** form of the command while the **cipUrpfDropRateInterval** value is configured to be greater than the default compute window value, the following message appears on the console:

"urpf drop rate window < interval"

This error message means the command was not executed. The compute window remains at the configured value rather than changing to the default value.

Examples

The following example shows how to configure a compute window of 60 seconds:

```
ip verify drop-rate compute window 60
```

Related Commands

Command	Description
ip verify drop-rate compute interval	Configures the interval between URPF drop rate computations.

ip verify drop-rate notify hold-down

To configure the minimum time between unicast reverse path forwarding (URPF) drop rate notifications, use the **ip verify drop-rate notify hold-down** command in global configuration mode. To reset the hold-down time to the default value, use the **no** form of this command.

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

no ip verify drop-rate notify hold-down

Syntax Description

seconds	Minimum time, in seconds, between URPF drop rate notifications. The range is from 30 to 300. The default is 300.

Command Default

No notifications are sent.

Command Modes

Global configuration

Command History

Release	Modification
12.2(31)SB2	This command was introduced.

Usage Guidelines

This command configures the interval between URPF drop rate computations. The configured value applies for the computation of all URPF drop rates, global and per-interface.

Examples

The following example shows how to configure a notify hold-down time of 40 seconds:

```
ip verify drop-rate notify hold-down 40
```

Related Commands

Command	Description
ip verify drop-rate compute interval	Configures the interval of time between URPF drop rate computations.
ip verify drop-rate compute window	Configures the interval of time over which the URPF drop count used in the drop rate computation is collected.

ip verify unicast notification threshold

To configure the threshold value used to determine whether to send a unicast reverse path forwarding (URPF) drop rate notification, use the **ip verify unicast notification threshold** command in interface configuration mode. To set the notification threshold back to the default value, use the **no** form of this command.

ip verify unicast notification threshold *rate-val*

no ip verify unicast notification threshold

Syntax Description

rate-val	Threshold value, in packets per second, used to determine whether to send a URPF drop rate notification. The range is from 0 to 4294967295. The default is 1000.

Command Default

No notifications are sent.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(31)SB2	This command was introduced.

Usage Guidelines

This command configures the threshold URPF drop rate which, when exceeded triggers a notification. Configuring a value of 0 means any URPF packet drop will trigger a notification.

Examples

The following example shows how to configure a notification threshold value of 900:

```
ip verify unicast notification threshold 900
```

Related Commands

Command	Description
ip verify drop-rate compute interval	Configures the interval of time between URPF drop rate computations.
ip verify drop-rate compute window	Configures the interval of time over which the URPF drop count used in the drop rate computation is collected.

show ip interface

To display the usability status of interfaces configured for IP, use the **show ip interface** command in privileged EXEC mode.

show ip interface [*type number*] [**brief**]

Syntax Description

type	(Optional) Interface type.
number	(Optional) Interface number.
brief	(Optional) Displays a summary of the usability status information for each interface.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(3)T	This command was expanded to include the status of the **ip wccp redirect out** and **ip wccp redirect exclude add in** commands.
12.2(14)S	This command was expanded to display the status of NetFlow on a subinterface.
12.2(15)T	The command output enhancements introduced in Cisco IOS Release 12.2(14)S were integrated into Cisco IOS Release 12.2(15)T.
12.3(6)	The command output was modified to identify the downstream VRF in the output.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.
12.3(14)YM2	This command was modified to show the usability status of interfaces configured for Multi-Processor Forwarding (MPF) and implemented on the Cisco 7301 and Cisco 7206VXR routers.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was integrated into Cisco IOS 12.2(17d)SXB.
12.2(17d)SXB	The output was changed to include NDE for hardware flow status.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	The command output was modified to display information related to the Unicast Reverse Path Forwarding (URPF) notification feature.

Usage Guidelines

The Cisco IOS software automatically enters a directly connected route in the routing table if the interface is usable. A usable interface can send and receive packets. If an interface is not usable, the directly connected routing entry is removed from the routing table. Removing the entry allows the software to use dynamic routing protocols to determine backup routes to the network, if any.

If the interface can provide two-way communication, the line protocol is marked "up." If the interface hardware is usable, the interface is marked "up."

If you specify an optional interface type, you see information for that specific interface.

If you specify no optional arguments, you see information on all the interfaces.

When an asynchronous interface is encapsulated with PPP or Serial Line Internet Protocol (SLIP), IP fast switching is enabled. A **show ip interface** command on an asynchronous interface encapsulated with PPP or SLIP displays a message indicating that IP fast switching is enabled.

The **show ip interface brief** command can be used to view a summary of the router interfaces. This command displays the IP address, interface status, and additional information.

The **show ip interface brief** command does not display any information related to URPF.

Examples

The following examples from Cisco IOS Release 12.3(14)YM2 show:

- Configuration information on interface Gigabit Ethernet0/3, where the IP flow egress feature is configured on the output side (where packets go out of the interface) and the policy route-map named PBR_NAME is configured on the input side (where packets come into the interface).
- Interface information on Gigabit Ethernet interface 0/3 showing that MPF is enabled and that both features are not supported by MPF and are ignored.

The highlighted arrows (for documentation purposes only) show the configured output and input features and the additional MPF interface information.

```
Router# show running-config interface gigabitethernet 0/3

interface GigabitEthernet0/3
 ip address 10.1.1.1 255.255.0.0
 ip flow egress                  <== output
 ip policy route-map PBR_NAME    <== input
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
end

Router# show ip interface gigabitethernet 0/3

GigabitEthernet0/3 is up, line protocol is up
  Internet address is 10.1.1.1/16
  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 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 fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Feature Fast switching turbo vector
```

```
  IP VPN Flow CEF switching turbo vector
  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
  Policy routing is enabled, using route map PBR
  Network address translation is disabled
  BGP Policy Mapping is disabled
  IP Multi-Processor Forwarding is enabled   <======== MPF information
     IP Input features, "PBR",
         are not supported by MPF and are IGNORED
     IP Output features, "NetFlow",
         are not supported by MPF and are IGNORED
```

The following example identifies a downstream VRF. The highlighted line (for documentation purposes only) identifies the downstream VRF.

```
Router# show ip interface vi 3

Virtual-Access3 is up, line protocol is up
  Interface is unnumbered. Using address of Loopback2 (10.0.0.8)
  Broadcast address is 255.255.255.255
  Peer address is 10.8.1.1
  MTU is 1492 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 fast switching on the same interface is enabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Feature Fast switching turbo vector
  IP VPN CEF switching turbo vector
  VPN Routing/Forwarding "U"
  Downstream VPN Routing/Forwarding "D"
  IP multicast fast switching is disabled
  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
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

The following example shows the information displayed when URPF drop-rate notification is configured:

```
Router# show ip interface ethernet 2/3

Ethernet2/3 is up, line protocol is up
  Internet address is 10.0.0.4/16
  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 disabled
  IP Flow switching is disabled
  IP CEF switching is disabled
  IP Null turbo vector
  IP Null turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are No 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
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

URPF Information

```
  Input features: uRPF
  IP verify source reachable-via RX, allow default
   0 verification drops
   0 suppressed verification drops
   0 verification drop-rate
router#
```

This example shows how to display the usability status for a specific VLAN:

```
Router# show ip interface vlan 1

Vlan1 is up, line protocol is up
  Internet address is 10.0.0.4/24
  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 fast switching on the same interface is disabled
IP Flow switching is disabled
IP CEF switching is enabled
IP Fast switching turbo vector
IP Normal CEF switching turbo vector
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
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
BGP Policy Mapping is disabled
Sampled Netflow is disabled
IP multicast multilayer switching is disabled
Netflow Data Export (hardware) is enabled
```

Table 1 describes the significant fields shown in the display.

Table 1 show ip interface Field Descriptions

Field	Description
Virtual-Access3 is up	If the interface hardware is usable, the interface is marked "up." For an interface to be usable, both the interface hardware and line protocol must be up.
Broadcast address is	Displays the broadcast address.
Peer address is	Displays the peer address.
MTU is	Displays the MTU value set on the interface.
Helper address	Displays a helper address, if one has been set.
Directed broadcast forwarding	Indicates whether directed broadcast forwarding is enabled.
Outgoing access list	Indicates whether the interface has an outgoing access list set.
Inbound access list	Indicates whether the interface has an incoming access list set.
Proxy ARP	Indicates whether Proxy Address Resolution Protocol (ARP) is enabled for the interface.
Security level	Specifies the IP Security Option (IPSO) security level set for this interface.
Split horizon	Indicates that split horizon is enabled.

Table 1 show ip interface Field Descriptions (continued)

Field	Description
ICMP redirects	Specifies whether redirect messages will be sent on this interface.
ICMP unreachables	Specifies whether unreachable messages will be sent on this interface.
ICMP mask replies	Specifies whether mask replies will be sent on this interface.
IP fast switching	Specifies whether fast switching has been enabled for this interface. It is generally enabled on serial interfaces, such as this one.
IP Flow switching	Specifies whether Flow switching is enabled for this interface.
IP CEF switching	Specifies whether Cisco Express Forwarding is enabled for the interface.
Downstream VPN Routing/Forwarding "D"	Specifies the VRF where the PPP peer routes and AAA per-user routes are being installed.
IP multicast fast switching	Specifies whether multicast fast switching is enabled for the interface.
IP route-cache flags are Fast, Flow init, CEF, Ingress Flow	Specifies whether NetFlow has been enabled on an interface. Displays "Flow init" to specify that NetFlow is enabled on the interface. Displays "Ingress Flow" to specify that NetFlow is enabled on a subinterface using the **ip flow ingress** command. Specifies "Flow" to specify that NetFlow is enabled on a main interface using the **ip route-cache flow** command.
Router Discovery	Specifies whether the discovery process has been enabled for this interface. It is generally disabled on serial interfaces.
IP output packet accounting	Specifies whether IP accounting is enabled for this interface and what the threshold (maximum number of entries) is.
TCP/IP header compression	Indicates whether compression is enabled or disabled.
WCCP Redirect outbound is disabled	Indicates the status of whether packets received on an interface are redirected to a cache engine. Displays "enabled" or "disabled."
WCCP Redirect exclude is disabled	Indicates the status of whether packets targeted for an interface will be excluded from being redirected to a cache engine. Displays "enabled" or "disabled."
Netflow Data Export (hardware) is enabled	NDE hardware flow status on the interface.

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

```
Router# show ip interface brief

Interface      IP-Address      OK?  Method  Status                  Protocol
Ethernet0      10.108.00.5     YES  NVRAM   up                      up
Ethernet1      unassigned      YES  unset   administratively down   down
Loopback0      10.108.200.5    YES  NVRAM   up                      up
Serial0        10.108.100.5    YES  NVRAM   up                      up
Serial1        10.108.40.5     YES  NVRAM   up                      up
Serial2        10.108.100.5    YES  manual  up                      up
Serial3        unassigned      YES  unset   administratively down   down
```

Table 2 describes the significant fields shown in the display.

Table 2 show ip interface brief Field Descriptions

Field	Description
Interface	Type of interface.
IP-Address	IP address assigned to the interface.
OK?	"Yes" means that the IP Address is currently valid. "No" means that the IP Address is not currently valid.
Method	The method field has the following possible values: • RARP or SLARP—Reverse Address Resolution Protocol (RARP) or Serial Line Address Resolution Protocol (SLARP) request • BOOTP—Bootstrap protocol • TFTP—Configuration file obtained from TFTP server • manual—Manually changed by CLI command • NVRAM—Configuration file in NVRAM • IPCP—**ip address negotiated** command • DHCP—**ip address dhcp** command • unassigned—No IP address • unset—Unset • other—Unknown
Status	Indicates the status of interface. Valid values and their meanings are: • up—Interface is administratively up. • down—Interface is administratively down. • administratively down—Interface is administratively down.
Protocol	Indicates the operational status of the routing protocol on this interface.

Related Commands

Command	Description
ip address	Sets a primary or secondary IP address for an interface.
ip vrf autoclassify	Enables VRF autoclassify on a source interface.
match ip source	Specifies a source IP address to match to required route maps that have been set up based on VRF connected routes.
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.
set vrf	Enables VPN VRF selection within a route map for policy-based routing VRF selection.
show ip arp	Displays the ARP cache, in which SLIP addresses appear as permanent ARP table entries.
show route-map	Displays static and dynamic route maps.

snmp trap ip verify drop-rate

To configure the router to send a simple network management protocol (SNMP) notification when the unicast reverse path forwarding (URPF) drop rate exceeds the configured threshold, use the **snmp trap ip verify drop-rate** command in interface configuration mode. To disable SNMP notification, use the **no** form of this command.

snmp trap ip verify drop-rate

no snmp trap ip verify drop-rate

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled (no SNMP notifications are sent).

Command Modes

Interface configuration

Command History

Release	Modification
12.2(31)SB2	This command was introduced.

Usage Guidelines

This command enables **cipUrpfIfDropRateNotify** notification. This notification is sent when the URPF drop rate exceeds the threshold.

Examples

The following example shows how to configure SNMP notification for the URPF drop rate:

```
snmp trap ip verify drop-rate
```

Related Commands

Command	Description
ip verify drop-rate compute window	Configures the interval of time over which the URPF drop count used in the drop rate computation is collected.
ip verify unicast notification threshold	Configures the URPF drop count threshold which, when exceeded, triggers a notification.

Feature Information for CISCO-IP-URPF-MIB Support

Table 3 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 3 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 3 Feature Information for CISCO-IP-URPF-MIB Support

Feature Name	Releases	Feature Information
CISCO-IP-URPF-MIB Support	12.2(31)SB2	The CISCO-IP-URPF-MIB has been defined to provide Simple Network Management Protocol (SNMP) notification when a specified URPF drop-rate threshold on a managed device is exceeded.

partnership relationship between Cisco and any other company. (0711R)