CISCO-IP-URPF-MIB Support

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

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Prerequisites for CISCO-IP-URPF-MIB Support

Before you configure CISCO-IP-URPF-MIB, you must configure the following features:

- Cisco Express Forwarding switching
- IP routing
- SNMP
- Unicast RPF

Restrictions for CISCO-IP-URPF-MIB Support

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

Information About CISCO-IP-URPF-MIB Support

Implementation of Unicast RPF Notification

Unicast RPF 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, Unicast RPF drops the packet. IP verification of the source is done to prevent the DoS attacks by detecting problems with the incoming packets on an interface. However, deploying Unicast RPF without some automated monitoring capability is a challenge.

The CISCO-IP-URPF-MIB lets you specify a Unicast RPF drop-rate threshold on interfaces of a managed device that will send an SNMP notification when the threshold is exceeded. The MIB includes objects for specifying global and per-interface drop counts and drop rates and a method to generate SNMP traps when the drop rate exceeds a configurable per-interface threshold.

Although you can configure some parameters globally, you must configure the CISCO-IP-URPF-MIB on individual interfaces.

Elements of Unicast RPF Notification

The elements described in the following sections make Unicast RPF drop-rate notification work:

- Drop-Rate Computation, on page 2
- Global Scalars, on page 3
- Global Tables, on page 3
- How to Configure Unicast RPF Drop-Rate Notification, on page 4
- Per-Interface Configuration, on page 3

Drop-Rate Computation

Whenever Unicast RPF is configured on an interface, the drop-rate calculation is done periodically (at intervals specified by the cipUrpfComputeInterval object). Drop rates are computed over a constantly sliding window,

whose period starts at the configured number of seconds before the calculation and ends with the performance of the calculation.

Global Scalars

The following global scalars affect how the MIB agent computes all drop rates and generates notifications:

- cipUrpfDropRateWindow--This object specifies the window of time in the recent past over which the drop rate computation occurs. If there was no window (that is, the window is the epoch since booting up), an identical drop count burst at a later time would produce a lower drop rate than the 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 the global drop count and drop-rate objects per packet flow. These global rates are useful for quickly determining whether the managed device had Unicast RPF activity at a specific time.
- cipUrpfVrfTable--This table contains the index drop counters by VRF (if a VRF routing table is used to determine Unicast RPF checking). The table provides a method for VRF to index all the Unicast RPF-enabled interfaces.

Per-Interface Configuration

The following MIB objects enable per-interface configuration:

- cipUrpfIfDropRateNotifyEnable--This object specifies whether the system produces the cipUrpfIfDropRateNotify notification because Unicast RPF has dropped version cipUrpfIfIpVersion IP packets on the specified interface.
- cipUrpfIfNotifyDropRateThreshold--This object specifies the drop-rate threshold value above which a notification is generated.

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 Unicast RPF drops on an interface. Snapshots of this value are used in the drop-rate computation. The computed drop rate is specified in the cipUrpfIfDropRate object. If Unicast RPF is configured on a subinterface, drop rates are computed.

How to Configure Unicast RPF Drop-Rate Notification

Configuring Unicast RPF Drop-Rate Notification via Syslog

Perform this task to configure the Unicast RPF drop-rate threshold and computation parameters for notification via syslog.

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. **interface** *type number*
7. **ip verify unicast notification threshold** *packets-per-second*
8. **end**
9. **show ip interface** *type number*
10. **debug ip verify mib**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
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 Unicast RPF 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 using the **ip verify drop-rate compute interval** command.
Step 4	**ip verify drop-rate compute interval** *seconds* **Example:**	Configures the interval of time, in seconds, between Unicast RPF drop-rate computations.

	Command or Action	Purpose
	`Router(config)# ip verify drop-rate compute interval 60`	• 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 using 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 Unicast RPF drop-rate notifications. • The range is from 30 to 300. The default is 300.
Step 6	**interface** *type number* **Example:** `Router(config)# interface ethernet 3/0`	Configures an interface and enters interface configuration mode.
Step 7	**ip verify unicast notification threshold** *packets-per-second* **Example:** `Router(config-if)# ip verify unicast notification threshold 750`	Configures the threshold value, in packets per second, which determines whether to send a Unicast RPF drop-rate notification. • The range is from 0 to 2147483647. The default is 1000. **Note** If you configure the threshold as 0, every packet drop triggers a notification.
Step 8	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 9	**show ip interface** *type number* **Example:** `Router# show ip interface ethernet 2/3`	(Optional) Displays the verification drop rate and the number of verification drops when Unicast RPF is configured for an interface.
Step 10	**debug ip verify mib** **Example:** `Router# debug ip verify mib`	(Optional) Displays output that is useful for troubleshooting Unicast RPF notification.

Configuring Unicast RPF Drop-Rate Notification via SNMP

Perform this task to configure the Unicast RPF drop-rate threshold and computation parameters for notification via SNMP.

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. **interface** *type number*
7. **ip verify unicast notification threshold** *packets-per-second*
8. **snmp trap ip verify drop-rate**
9. **end**
10. **show ip interface** *type number*
11. **debug ip verify mib**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
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 Unicast RPF 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 using 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 Unicast RPF 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 using the **ip verify drop-rate compute window**command.
Step 5	**ip verify drop-rate notify hold-down** *seconds* **Example:**	Configures the minimum time, in seconds, between Unicast RPF drop-rate notifications.

	Command or Action	Purpose
	`Router(config)# ip verify drop-rate notify hold-down 60`	• The range is from 30 to 300. The default is 300.
Step 6	**interface** *type number* **Example:** `Router(config)# interface ethernet 3/0`	Configures an interface and enters interface configuration mode.
Step 7	**ip verify unicast notification threshold** *packets-per-second* **Example:** `Router(config-if)# ip verify unicast notification threshold 750`	Configures the threshold value, in packets per second, which determines whether to send a Unicast RPF drop-rate notification. • The range is from 0 to 2147483647. The default is 1000. **Note** If you configure the threshold to be 0, every packet drop triggers 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 Unicast RPF drop rate exceeds the configured threshold.
Step 9	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 10	**show ip interface** *type number* **Example:** `Router# show ip interface ethernet 2/3`	(Optional) Displays the verification drop rate and the number of verification drops when Unicast RPF is configured for an interface.
Step 11	**debug ip verify mib** **Example:** `Router# debug ip verify mib`	(Optional) Displays output that is useful for troubleshooting Unicast RPF notification.

Configuration Examples for CISCO-IP-URPF-MIB Support

Example Configuring Unicast RPF Drop-Rate Notification via Syslog

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

```
Router> enable
Router# configure terminal
Router(config)# ip verify drop-rate compute window 60
Router(config)# ip verify drop-rate compute interval 60
Router(config)# ip verify drop-rate notify hold-down 60
Router(config)# i
nterface ethernet 3/0
Router(config-if)# ip verify unicast notification threshold 750
Router(config-if)# end
```

Example Configuring Unicast RPF Drop-Rate Notification via SNMP

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

```
Router> enable
Router# configure terminal
Router(config)# ip verify drop-rate compute window 60
Router(config)# ip verify drop-rate compute interval 60
Router(config)# ip verify drop-rate notify hold-down 60
Router(config)# interface ethernet 3/0
Router(config-if)# ip verify unicast notification threshold 750
Router(config-if)# snmp trap ip verify drop-rate
Router(config-if)# end
```

Example Verifying and Troubleshooting the Unicast RPF Configuration

The following is sample output from the **show ip interface** command. The output displays the verification drop rate and the number of verification drops when Unicast RPF is configured for an interface. The last five lines in the following example show the output of the **show ip interface**command when Unicast RPF is configured:

```
Router# show ip interface ethernet 2/3
Ethernet2/3 is up, line protocol is up
  Internet address is 10.10.5.4/16
  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 is sample output from the **debug ip verify mib** command. The command displays output that is useful for troubleshooting Unicast RPF notification:

```
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
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Security commands	*Cisco IOS Security Command Reference*
Configuring Unicast RPF	"Configuring Unicast Reverse Path Forwarding" module in the *Cisco IOS Security Configuration Guide: Securing the Data Plane*
Configuring SNMP	"Configuring SNMP Support" module in the *Network Management Configuration Guide*

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
None	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for CISCO-IP-URPF-MIB Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 1: Feature Information for CISCO-IP-URPF-MIB Support

Feature Name	Releases	Feature Information
CISCO-IP-URPF-MIB Support	Cisco IOS XE Release 3.9S	The CISCO-IP-URPF-MIB provides SNMP notification when a specified drop-rate threshold on a managed device is exceeded. You can use the IP Unicast RPF feature to avert DoS attacks by verifying the validity of the source IP of an incoming packet. You can configure the Unicast RPF drop-rate threshold globally for a device or per interface. The following commands were introduced or modified: **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**