ICMP Unreachable Destination Counters

The ICMP Unreachable Destination Counters feature enables you to clear and display packets that have been discarded because of an unreachable destination, and to configure a threshold interval for triggering error messages. When message logging is generated, it displays on your console.

History for the ICMP Unreachable Destination Counters Feature

Release	Modification
12.4(2)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

Information About ICMP Unreachable Destination Counters

To configure the ICMP Unreachable Counters feature, you should understand the following concepts:

CISCO SYSTEMS

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

ICMP Overview

Originally created for the TCP/IP suite in RFC 792, the Internet Control Message Protocol (ICMP) was designed to report a small set of error conditions. ICMP also can report a wide variety of error conditions, provide feedback and testing capabilities. It is a valuable support tool because each message uses a common format and is sent and received by using the same protocol rules.

ICMP enables IP to perform addressing, datagram packaging, and routing by allowing encapsulated messages to be sent and received between IP devices. These messages are encapsulated in IP datagrams just like any other IP message. When the message is generated, the original IP header is encapsulated in the ICMP message and these two pieces are encapsulated within a new IP header to be returned as an error report to the sending device.

ICMP messages are sent in several situations: for example, when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route. To avoid the infinite regress of messages about messages, no ICMP messages are sent about ICMP messages.

ICMP does not make IP reliable or ensure the delivery of datagrams or the return of a control message. Some datagrams may be dropped without any report of their loss. The higher-level protocols that use IP must implement their own reliability procedures if reliable communication is required.

For information about IPv6 and ICMP, refer to *Cisco IOS IPv6 Configuration Guide*, Release 12.4 and *Cisco IOS IPv6 Command Reference*, Release 12.4.

Type 3 Destination Unreachable Error Messages

Type 3 error messages are sent when a message cannot be delivered completely to the application at a destination host. Six codes contained in the ICMP header describe the unreachable condition as follows:

- 0—Network unreachable
- 1—Host unreachable
- 2—Protocol unreachable
- 3—Port unreachable
- 4—Fragmentation needed and Don’t Fragment (DF) bit set
- 5—Source route failed

Cisco IOS software can suppress the generation of ICMP unreachable destination error messages, which is called rate-limiting. The default is no unreachable messages more often than once every half second. Separate intervals can be configured for code 4 and all other unreachable destination error messages. However, there is no method of displaying how many ICMP messages have not been sent.

The ICMP Unreachable Destination Counters feature provides a method to count and display the unsent Type 3 messages. This feature also provides console logging with error messages when there are periods of excessive rate limiting that would indicate a Denial of Service (DoS) attack against the router.

Denial of Service Attack

A DoS attack occurs when a stream of ICMP echo requests (pings) are broadcast to a destination subnet. The source addresses of these requests are falsified to be the source address of the target. For each request sent by the attacker, many hosts on the subnet will respond flooding the target and wasting bandwidth. The most common DoS attack is called a “smurf” attack, named after an executable program and is in the category of network-level attacks against hosts. DoS attacks can be easily detected when error-message logging of the ICMP Unreachable Destination Counters feature is enabled.

How to Configure ICMP Unreachable Destination Counters

This section contains the following procedures:

- Clearing the ICMP Unreachable Destination Packet Statistics, page 3 (required)
- Configuring ICMP Unreachable Destination Counters and Logging Intervals, page 4 (required)
- Displaying the ICMP Unreachable Destination Packets, page 5 (optional)

Clearing the ICMP Unreachable Destination Packet Statistics

Perform this task to clear all of the unreachable destination packet statistics. This task is beneficial to begin a new log after the thresholds have been set.

SUMMARY STEPS

1. **enable**
2. **clear ip icmp rate-limit** [*interface-type interface-number*]
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear ip icmp rate-limit** [*interface-type interface-number*] **Example:** `Router# clear ip icmp rate-limit ethernet 2/3`	Clears all current ICMP unreachable statistics for all configured interfaces. The optional *interface-type* and *interface-number* arguments clear the statistics for only one interface. **Note** Refer to the **interface** command in the *Cisco IOS Interface and Hardware Component Command Reference*, Release 12.4 for valid interface types.
Step 3	**end** **Example:** `Router# end`	Exits to user EXEC mode.

Configuring ICMP Unreachable Destination Counters and Logging Intervals

Perform this task to specify an interval number for unreachable destination messages and a packet counter (threshold) and interval to trigger a logging message to a console. Counting begins as soon as this command is configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip icmp rate-limit unreachable** [**df**] [*ms*] [**log** [*packets*] [*interval-ms*]]
4. **exit**

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.

	Command or Action	Purpose
Step 3	**ip icmp rate-limit unreachable** [**df**] [*ms*] [**log** [*packets*] [*interval-ms*]] **Example:** `Router(config)# ip icmp rate-limit unreachable df log 1100 12000`	Specifies the rate limitation of ICMP unreachable destination messages and the error message log threshold for generating a message. The default is no unreachable messages are sent more often than once every half second. The arguments and keywords are as follows: • **df**—(Optional) When Don't Fragment (DF) bit is set in the ICMP header, a datagram cannot be fragmented. If the **df** keyword is not specified, all other types of destination unreachable messages are sent. • *ms*—(Optional) Interval at which unreachable messages are generated. The valid range is from 1 ms to 4294967295 ms. • **log**—(Optional) List of error messages. The arguments are as follows: – *packets*—(Optional) Number of packets that determine a threshold for generating a log. The default is 1000 packets. – *interval-ms*—(Optional) Time limit for an interval for which a logging message is triggered. The default is 60000 ms, which is 1 minute. **Note** Counting begins as soon as this command is configured.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits to privileged EXEC mode.

Displaying the ICMP Unreachable Destination Packets

Perform this optional task to display all of the unreachable destination packet statistics, which include dropped packets. Counting begins as soon as **ip icmp rate-limit unreachable** command is configured.

SUMMARY STEPS

1. **enable**
2. **show ip icmp rate-limit** [*interface-type interface-number*]
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip icmp rate-limit** [*interface-type interface-number*] **Example:** `Router# show ip icmp rate-limit ethernet 2/3`	Displays all current ICMP unreachable statistics for all configured interfaces. The optional *interface-type* and *interface-number* arguments displays the statistics for only one interface. **Note** Refer to the **interface** command in the *Cisco IOS Interface and Hardware Component Command Reference*, Release 12.4 for valid interface types.
Step 3	**end** **Example:** `Router# end`	Exits to user EXEC mode.

Examples

The following output using the **show ip icmp rate-limit** command displays the unreachable destinations by interface:

```
Router# show ip icmp rate-limit

                          DF bit unreachables       All other unreachables
Interval (millisecond)    500                       500

Interface                 # DF bit unreachables     # All other unreachables
---------                 ---------------------     ------------------------
Ethernet0/0               0                         0
Ethernet0/2               0                         0
Serial3/0/3               0                         19
```

The greatest number of unreachables is on serial interface 3/0/3.

Configuration Examples for ICMP Unreachable Packet Counters

This section provides the following configuration example:

- ICMP Rate-Limit Unreachable Log Configuration: Example, page 6

ICMP Rate-Limit Unreachable Log Configuration: Example

In the following example, console logging begins with a packet threshold of 1200 and every 120,000 ms:

```
ip icmp rate-limit unreachable log 1200 120000
```

Additional References

The following sections provide references related to ICMP Unreachable Destination Counters feature.

Related Documents

Related Topic	Document Title
IP application services configuration tasks	*Cisco IOS IP Addressing and Services Configuration Guide*, Release 12.3
IP application services commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Application Services Command Reference*, Release 12.4T
Interface and hardware component commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Interface and Hardware Component Command Reference*, Release 12.4T

Standards

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

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	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

RFCs	Title
RFC 792	*Internet Control Message Protocol*

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents new and modified commands only.

New Commands

- **clear ip icmp rate-limit**
- **show ip icmp rate-limit**

Modified Commands

- **ip icmp rate-limit unreachable**

clear ip icmp rate-limit

To clear all Internet Control Message Protocol (ICMP) unreachable rate-limiting statistics or all statistics for a specified interface, use the **clear ip icmp rate-limit** command in privileged EXEC mode.

clear ip icmp rate-limit [*interface-type interface-number*]

Syntax Description

interface-type	(Optional) Type of interface to be configured. Refer to the **interface** command in the *Cisco IOS Interface and Hardware Component Command Reference*, Release 12.4 for a list of valid interface types.
interface-number	(Optional) Port, connector, or interface card number. On Cisco 4700 series routers, specifies the network interface module (NIM) or network processor module (NPM) number. The numbers are assigned at the factory at the time of installation or when added to a system, and can be displayed with the **show interfaces** command.

Defaults

All unreachable statistics for all devices are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(2)T	This command was introduced.

Examples

The following example shows how to clear all unreachable statistics on all interfaces:

```
Router# clear icmp rate-limit
```

Related Commands

Command	Description
ip icmp rate-limit unreachable	Limits the rate at which ICMP unreachable messages are generated for a destination.
show ip icmp rate-limit	Displays all ICMP unreachable rate-limiting statistics or all statistics for a specified interface.

ip icmp rate-limit unreachable

To limit the rate at which Internet Control Message Protocol (ICMP) unreachable messages are generated for a destination, use the **ip icmp rate-limit unreachable** command in global configuration mode. To use the default, use the **no** form of this command.

ip icmp rate-limit unreachable [**df**] [*ms*] [**log** [*packets*] [*interval-ms*]]

no ip icmp rate-limit unreachable [**df**] [*ms*] [**log** [*packets*] [*interval-ms*]]

Syntax Description

df	(Optional) Don't Fragment (DF) bit is set. The optional *ms* argument is a time limit in milliseconds (ms) in which one unreachable message is generated. If the **df** keyword is specified, its *ms* argument remains independent from those of general destination unreachable messages. The valid range is from 1 ms to 4294967295 ms. **Note** Counting begins as soon as this command is configured.
log	(Optional) Logging of generated messages that show packets that could not reach a destination at a specified threshold. The optional *packets* argument specifies a packet threshold. When it is reached, a log message is generated on the console. The default is 1000 packets. The optional *interval-ms* argument is a time limit for the interval for which a logging message is triggered. The default is 60000 ms, which is 1 minute.

Defaults

The default value is one ICMP destination unreachable message per 500 ms.

Command Modes

Global configuration

Command History

Release	Modification
12.0	This command was introduced.
12.4(2)T	The *packets* and the *interval-ms* arguments and **log** keyword were introduced.

Usage Guidelines

Counting of packets begins when the command is configured and a packet threshold is specified.

The **no ip icmp rate-limit unreachable** command turns off the previously configured rate limit. To reset the rate limit to its default value, use the **ip icmp rate-limit unreachable** command default.

Cisco IOS software maintains two timers: one for general destination unreachable messages and one for DF destination unreachable messages. Both share the same time limits and defaults. If the **df** option is not configured, the **ip icmp rate-limit unreachable** command sets the time values in ms for DF destination unreachable messages.

Examples

The following example sets the rate of the ICMP destination unreachable message to one message every 10 ms:

```
ip icmp rate-limit unreachable 10
```

The following example turns off the previously configured rate limit:

```
no ip icmp rate-limit unreachable
```

The following example sets the rate limit back to the default:

```
no ip icmp rate-limit unreachable
```

The following example sets a logging packet threshold and time interval:

```
ip icmp rate-limit unreachable log 1200 120000
```

Related Commands

Command	Description
clear ip icmp rate-limit	Clears all ICMP unreachable destination messages or all statistics for a specified interface.
show ip icmp rate-limit	Displays all ICMP unreachable destination messages or all statistics for a specified interface.

show ip icmp rate-limit

To display all Internet Control Message Protocol (ICMP) unreachable destination messages or unreachable destination messages for a specified interface including the number of dropped packets, use the **show ip icmp rate-limit** command in privileged EXEC mode.

show ip icmp rate-limit [*interface-type interface-number*]

Syntax Description

interface-type	(Optional) Interface type. Type of interface to be configured. **Note** Refer to the **interface** command in the *Cisco IOS Interface and Hardware Component Command Reference*, Release 12.4 for a list of interface types.
interface-number	(Optional) Port, connector, or interface card number. On Cisco 4700 series routers, specifies the network interface module (NIM) or network processor module (NPM) number. The numbers are assigned at the factory at the time of installation or when added to a system, and can be displayed with the **show interfaces** command.

Defaults

All unreachable statistics for all devices are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(2)T	This command was introduced.

Examples

The following is sample output when the **show ip icmp rate-limit** command is entered and unreachable messages are generated:

```
Router# show ip icmp rate-limit

                          DF bit unreachables        All other unreachables
Interval (millisecond)    500                        500

Interface                 # DF bit unreachables     # All other unreachables
---------                 ---------------------     ------------------------
Ethernet0/0               0                         0
Ethernet0/2               0                         0
Serial3/0/3               0                         19
```

The greatest number of unreachables on Serial3/0/3 is 19.

The following is sample output when the **show ip icmp rate-limit** command is entered and the rate-limit interval has been set at 500. The packet threshold has been set at 1 by using the **ip icmp rate-limit unreachable** command, so the logging will display on the console when the threshold is exceeded. The total suppressed packets since last log message is displayed.

```
Router# show ip icmp rate-limit

00:04:18: %IP-3-ICMPRATELIMIT: 2 unreachables rate-limited within 60000 milliseconds on
Serial3/0/3. 17 log messages suppressed since last log message displayed on Serial3/0/3
```

Table 1 describes the significant fields shown in the display.

Table 1 show ip icmp rate-limit Field Descriptions

Field	Description
ICMPRATELIMIT	ICMP packets that are rate limited.
suppressed	Packets that have been suppressed because the destination is unreachable.

Related Commands

Command	Description
clear icmp rate-limit	Clears all ICMP unreachable destination messages or all messages for a specified interface.
ip icmp rate-limit unreachable	Limits the rate at which ICMP unreachable messages are generated for a destination.