NAME

icmp − Linux IPv4 ICMP kernel module.

DESCRIPTION

This kernel protocol module implements the Internet Control Message Protocol defined in RFC 792. It is used to signal error conditions and for diagnosis. The user doesn't interact directly with this module; instead it communicates with the other protocols in the kernel and these pass the ICMP errors to the application layers. The kernel ICMP module also answers ICMP requests.

A user protocol may receive ICMP packets for all local sockets by opening a raw socket with the protocol **IPPROTO_ICMP**. See**raw**(7) for more information. The types of ICMP pack ets passed to the socket can be filtered using the **ICMP_FILTER** socket option. ICMP packets are always processed by the kernel too, even when passed to a user socket.

Linux limits the rate of ICMP error packets to each destination. **ICMP_REDIRECT** and **ICMP_DEST_UNREACH** are also limited by the destination route of the incoming packets.

/proc interfaces

ICMP supports a set of */proc* interfaces to configure some global IP parameters. The parameters can be accessed by reading or writing files in the directory */proc/sys/net/ipv4/*. Most of these parameters are rate limitations for specific ICMP types. Linux 2.2 uses a token bucket filter to limit ICMPs. The value is the timeout in jiffies until the token bucket filter is cleared after a burst. A jiffy is a system dependent unit, usually 10ms on i386 and about 1ms on alpha and ia64.

icmp_destunreach_rate (Linux 2.2 to Linux 2.4.9)
: Maximum rate to send ICMP Destination Unreachable packets. This limits the rate at which packets are sent to any individual route or destination. The limit does not affect sending of **ICMP_FRAG_NEEDED** packets needed for path MTU discovery.

icmp_echo_ignore_all (since Linux 2.2)
: If this value is nonzero, Linux will ignore all **ICMP_ECHO** requests.

icmp_echo_ignore_broadcasts (since Linux 2.2)
: If this value is nonzero, Linux will ignore all **ICMP_ECHO** packets sent to broadcast addresses.

icmp_echoreply_rate (Linux 2.2 to Linux 2.4.9)
: Maximum rate for sending **ICMP_ECHOREPLY** packets in response to **ICMP_ECHOREQUEST** packets.

icmp_errors_use_inbound_ifaddr (Boolean; default: disabled; since Linux 2.6.12)
: If disabled, ICMP error messages are sent with the primary address of the exiting interface.

  If enabled, the message will be sent with the primary address of the interface that received the packet that caused the ICMP error. This is the behavior that many network administrators will expect from a router. And it can make debugging complicated network layouts much easier.

  Note that if no primary address exists for the interface selected, then the primary address of the first non-loopback interface that has one will be used regardless of this setting.

icmp_ignore_bogus_error_responses (Boolean; default: disabled; since Linux 2.2)
: Some routers violate RFC1122 by sending bogus responses to broadcast frames. Such violations are normally logged via a kernel warning. If this parameter is enabled, the kernel will not give such warnings, which will avoid log file clutter.

icmp_paramprob_rate (Linux 2.2 to Linux 2.4.9)
: Maximum rate for sending **ICMP_PARAMETERPROB** packets. These packets are sent when a packet arrives with an invalid IP header.

icmp_ratelimit (integer; default: 1000; since Linux 2.4.10)
: Limit the maximum rates for sending ICMP packets whose type matches *icmp_ratemask* (see below) to specific targets. 0 to disable any limiting, otherwise the minimum space between responses in milliseconds.

icmp_ratemask (integer; default: see below; since Linux 2.4.10)
Mask made of ICMP types for which rates are being limited.

Significant bits: IHGFEDCBA9876543210
Default mask: 0000001100000011000 (0x1818)

Bit definitions (see the Linux kernel source file *include/linux/icmp.h*):

0 Echo Reply
3 Destination Unreachable *
4 Source Quench *
5 Redirect
8 Echo Request
B Time Exceeded *
C Parameter Problem *
D Timestamp Request
E Timestamp Reply
F Info Request
G Info Reply
H Address Mask Request
I Address Mask Reply

The bits marked with an asterisk are rate limited by default (see the default mask above).

icmp_timeexceed_rate (Linux 2.2 to Linux 2.4.9)
Maximum rate for sending **ICMP_TIME_EXCEEDED** packets. These packets are sent to prevent loops when a packet has crossed too many hops.

ping_group_range (two integers; default: see below; since Linux 2.6.39)
Range of the group IDs (minimum and maximum group IDs, inclusive) that are allowed to create ICMP Echo sockets. The default is "1 0", which means no group is allowed to create ICMP Echo sockets.

VERSIONS

Support for the **ICMP_ADDRESS** request was removed in Linux 2.2.

Support for **ICMP_SOURCE_QUENCH** was removed in Linux 2.2.

NOTES

As many other implementations don't support **IPPROTO_ICMP** raw sockets, this feature should not be relied on in portable programs.

ICMP_REDIRECT packets are not sent when Linux is not acting as a router. They are also accepted only from the old gateway defined in the routing table and the redirect routes are expired after some time.

The 64-bit timestamp returned by **ICMP_TIMESTAMP** is in milliseconds since the Epoch, 1970-01-01 00:00:00 +0000 (UTC).

Linux ICMP internally uses a raw socket to send ICMPs. This raw socket may appear in **netstat**(8) output with a zero inode.

SEE ALSO

ip(7), **rdisc**(8)

RFC 792 for a description of the ICMP protocol.