Internet Control Message Protocol

From Wikipedia, the free encyclopedia

The **Internet Control Message Protocol** (**ICMP**) is one of the core protocols of the Internet Protocol Suite. It is chiefly used by the operating systems of networked computers to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached. ICMP can also be used to relay query messages.[1] It is assigned protocol number 1.[2]

ICMP[3] differs from transport protocols such as TCP and UDP in that it is not typically used to exchange data between systems, nor is it regularly employed by end-user network applications (with the exception of some diagnostic tools like ping and traceroute).

ICMP for Internet Protocol version 4 (IPv4) is also known as ICMPv4. IPv6 has a similar protocol, ICMPv6.

Contents

Internet protocol suite

Application layer
BGP · DHCP · DHCPv6 · DNS · FTP · HTTP · IMAP · IRC · LDAP · MGCP · NNTP · NTP · POP · RIP · RPC · RTP · RTSP · SIP · SMTP · SNMP · SOCKS · SSH · Telnet · TLS/SSL · XMPP · (more)

Transport layer
TCP · UDP · DCCP · SCTP · RSVP · ECN · (more)

Internet layer
IP (IPv4 · IPv6) · **ICMP** · ICMPv6 · IGMP · IPsec · (more)

Link layer
ARP/InARP · NDP · OSPF · Tunnels (L2TP) · PPP · Media access control (Ethernet · DSL · ISDN · FDDI) · (more)

Technical details

Internet Control Message Protocol is part of the Internet Protocol Suite as defined in RFC 792. ICMP messages are typically generated in response to errors in IP datagrams (as specified in RFC 1122) or for diagnostic or routing purposes. ICMP errors are always reported to the original source IP address of the originating datagram.[1]

An example ICMP error message is the Time To Live Exceeded message. Every machine (such as an intermediate router) that forwards an IP datagram has to decrement the time to live (TTL) field of the IP header by one. If the TTL reaches 0, an ICMP Time to live exceeded in transit message is sent to the source of

the datagram.

Each ICMP message is encapsulated directly within a single IP datagram, and thus, like UDP, ICMP is unreliable.

Although ICMP messages are contained within standard IP datagrams, ICMP messages are usually processed as a special case, distinguished from normal IP processing, rather than processed as a normal sub-protocol of IP. In many cases, it is necessary to inspect the contents of the ICMP message and deliver the appropriate error message to the application that generated the original IP packet, the one that prompted the sending of the ICMP message.

Many commonly-used network utilities are based on ICMP messages. The tracert (traceroute), Pathping commands are implemented by transmitting UDP datagrams with specially set IP TTL header fields, and looking for ICMP Time to live exceeded in transit (above) and "Destination unreachable" messages generated in response. The related ping utility is implemented using the ICMP "Echo request" and "Echo reply" messages.

ICMP segment structure

Header

The ICMP header starts after the IPv4 header. All ICMP packets will have an 8-byte header and variable-sized data section. The first 4 bytes of the header will be consistent. The first byte is for the ICMP type. The second byte is for the ICMP code. The third and fourth bytes are a checksum of the entire ICMP message. The contents of the remaining 4 bytes of the header will vary based on the ICMP type and code.[1]

ICMP error messages contain a data section that includes the entire IP header plus the first 8 bytes of data from the IP datagram that caused the error message. The ICMP datagram is then encapsulated in a new IP datagram.[1]

Bits	0–7	8–15	16–23	24–31
0	Type	Code	Checksum	
32	Rest of Header			

- **Type** – ICMP type as specified below.
- **Code** – Subtype to the given type.
- **Checksum** – Error checking data. Calculated from the ICMP header+data, with value 0 for this field. The checksum algorithm is specified in RFC 1071 (http://tools.ietf.org/html/rfc1071) .
- **Rest of Header** – Four byte field. Will vary based on the ICMP type and code.

Padding data

Padding data follows the ICMP header (in octets):

- Windows "ping.exe" adds, by default, 32 bytes of padding
- The Linux "ping" utility adds, by default, 56 bytes of padding

List of permitted control messages (incomplete list)

Type	Code	Description
0 – Echo Reply[4]	0	Echo reply (used to ping)
1 and 2		*Reserved*
3 – Destination Unreachable[5]	0	Destination network unreachable
	1	Destination host unreachable
	2	Destination protocol unreachable
	3	Destination port unreachable
	4	Fragmentation required, and DF flag set
	5	Source route failed
	6	Destination network unknown
	7	Destination host unknown
	8	Source host isolated
	9	Network administratively prohibited
	10	Host administratively prohibited
	11	Network unreachable for TOS
	12	Host unreachable for TOS
	13	Communication administratively prohibited
4 – Source Quench	0	Source quench (congestion control)
5 – Redirect Message	0	Redirect Datagram for the Network
	1	Redirect Datagram for the Host

	2	Redirect Datagram for the TOS & network
	3	Redirect Datagram for the TOS & host
6		Alternate Host Address
7		*Reserved*
8 – Echo Request	0	Echo request (used to ping)
9 – Router Advertisement	0	Router Advertisement
10 – Router Solicitation	0	Router discovery/selection/solicitation
11 – Time Exceeded[6]	0	TTL expired in transit
	1	Fragment reassembly time exceeded
12 – Parameter Problem: Bad IP header	0	Pointer indicates the error
	1	Missing a required option
	2	Bad length
13 – Timestamp	0	Timestamp
14 – Timestamp Reply	0	Timestamp reply
15 – Information Request	0	Information Request
16 – Information Reply	0	Information Reply
17 – Address Mask Request	0	Address Mask Request
18 – Address Mask Reply	0	Address Mask Reply
19		*Reserved* for security
20 through 29		*Reserved* for robustness experiment
30 – Traceroute	0	Information Request
31		Datagram Conversion Error
32		Mobile Host Redirect
33		Where-Are-You (originally meant for IPv6)
34		Here-I-Am (originally meant for IPv6)

35		Mobile Registration Request
36		Mobile Registration Reply
37		Domain Name Request
38		Domain Name Reply
39		SKIP Algorithm Discovery Protocol, Simple Key-Management for Internet Protocol
40		Photuris, Security failures
41		ICMP for experimental mobility protocols such as Seamoby [RFC4065]
42 through 255		*Reserved*

(Sources: IANA ICMP Parameters (http://www.iana.org/assignments/icmp-parameters) [1] (http://freebie.fatpipe.org/~mjb/Drawings/UDP_ICMP_Headers.png) and *Computer Networking – A Top-Down Approach* by Kurose and Ross) //

See also

- PMTUD
- ICMPv6
- IRDP
- Smurf attack
- TCP
- ping
- traceroute
- ICMP tunnel

References

1. ^ [a] [b] [c] [d] Forouzan, Behrouz A. (2007). *Data Communications And Networking* (Fourth ed.). Boston: McGraw-Hill. pp. 621–630. ISBN 0-07-296775-7.
2. ^ "Protocol Numbers" (http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xml) . *http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xml*. Internet Assigned Numbers Authority. http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xml. Retrieved 2011-06-23.
3. ^ Postel, J. (September 1981). *Internet Control Message Protocol* (http://tools.ietf.org/html/rfc792) . IETF. RFC 792. http://tools.ietf.org/html/rfc792.
4. ^ http://tools.ietf.org/html/rfc792#page-14
5. ^ http://tools.ietf.org/html/rfc792#page-4

6. ^ http://tools.ietf.org/html/rfc792#page-6

External links

- RFCs
  - RFC 792, *Internet Control Message Protocol*
  - RFC 1122, *Requirements for Internet Hosts – Communication Layers*
  - RFC 1716, *Towards Requirements for IP Router*
- IANA (http://www.iana.org/assignments/icmp-parameters)
- ICMP Sequence Diagram (http://www.eventhelix.com/RealtimeMantra/Networking/Icmp.pdf)
- ICMP ping simulation (http://www.visualland.net/view.php?cid=1124&protocol=ICMP&title=1.%20Ping%20basics)
- ICMP traceroute simulation (http://www.visualland.net/view.php?cid=1127&protocol=ICMP&title=6.%20Traceroute&ctype=1)
- IANA protocol numbers (http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xml)

Retrieved from "http://en.wikipedia.org/w/index.php?title=Internet_Control_Message_Protocol&oldid=463434648"
Categories: Internet protocols | Internet standards | Internet Layer protocols | Network layer protocols

---

- This page was last modified on 1 December 2011 at 03:58.
- Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. See Terms of use for details.
  Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.