What is ICMP? How does it work? ICMP functions, type and codes.

- ICMP (Internet Control Message Protocol) is an error-reporting protocol. Network devices like routers use to generate error messages to the source IP address when network problems prevent delivery of IP packets. ICMP creates and sends messages to the source IP address indicating that a gateway to the Internet that a router, service or host cannot be reached for packet delivery. Any IP network device has the capability to send, receive or process ICMP messages. ICMP is *not* a transport protocol that sends data between systems.

- While ICMP is not used regularly in end-user applications, it is used by network administrators to troubleshoot Internet connections in diagnostic utilities including ping and traceroute.

- ICMP is used by routers, intermediary devices or hosts to communicate error information or updates to other routers, intermediary devices or hosts. The widely used IPv4 (Internet Protocol version 4) and the newer IPv6 use similar versions of the ICMP protocol (ICMPv4 and ICMPv6, respectively). ICMP messages are transmitted as datagrams and consist of an IP header that encapsulates the ICMP data. ICMP packets are IP packets with ICMP in the IP data portion. ICMP messages also contain the entire IP header from the original message, so the end system knows which packet failed.

- ICMP is basically required for IP, so one could argue it belongs as part of IP. ICMP is basically the error notification feature of IP. TCP/UDP uses IP for error messages (port unreachable). PMTU is done by ICMP.

- The ICMP header appears after the IPv4 or IPv6 packet header and is identified as IP protocol number 1. The complex protocol contains three fields:

- The major type that identifies the ICMP message;
- The minor code that contains more information about the type field; and
- The checksum that helps detect errors introduced during transmission.

- A few of the most commonly used ICMP types in IPv4 include:

Echo Reply (0) and Echo Request (8): this is ping.
Destination Unreachable (3)
Source Quench (4): An ICMP message used to notify the sender that the router or host is congested, and the sender needs to slow down.
Redirect (5): a message used to say "use this other router instead" to a host that has access to both routers. We'll talk about this in detail in future routing issues of Networking 101.
Router Advertisement Reply (9) and Router Solicitation (10)
Time Exceeded (11): This message has two uses. First, it is used to send an error to the sending system when the IP TTL has been exceeded. Second, it will notify the sending system if a fragmented IP datagram isn't reassembled within a certain time limit.

- Control messages are identified by the value in the *type* field. The *code* field gives additional context information for the message. Some control messages have been deprecated since the protocol was first introduced.

Notable control messages

Type	Code	Status	Description
0 – Echo Reply[5]:14	0		Echo reply (used to ping)

1 and 2		unassigned	*Reserved*
3 – Destination Unreachable[5]:4	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
	14		Host Precedence Violation
	15		Precedence cutoff in effect
4 – Source Quench	0	deprecated	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		deprecated	Alternate Host Address
7		unassigned	*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[5]: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	deprecated	Information Request
16 – Information Reply	0	deprecated	Information Reply

17 – Address Mask Request	0	deprecated	Address Mask Request
18 – Address Mask Reply	0	deprecated	Address Mask Reply
19		reserved	*Reserved* for security
20 through 29		reserved	*Reserved* for robustness experiment
30 – Traceroute	0	deprecated	Information Request
31		deprecated	Datagram Conversion Error
32		deprecated	Mobile Host Redirect
33		deprecated	Where-Are-You (originally meant for IPv6)
34		deprecated	Here-I-Am (originally meant for IPv6)
35		deprecated	Mobile Registration Request
36		deprecated	Mobile Registration Reply
37		deprecated	Domain Name Request
38		deprecated	Domain Name Reply
39		deprecated	SKIP Algorithm Discovery Protocol, Simple Key-Management for Internet Protocol
40			Photuris, Security failures
41		Experimental	ICMP for experimental mobility protocols such as Seamoby [RFC4065]
42 – Extended Echo Request[8]	0		No Error
43 – Extended Echo Reply[8]	0		No Error
	1		Malformed Query
	2		No Such Interface
	3		No Such Table Entry
	4		Multiple Interfaces Satisfy Query
44 through 252		unassigned	*Reserved*
253		Experimental	RFC3692-style Experiment 1 (RFC 4727)
254		Experimental	RFC3692-style Experiment 2 (RFC 4727)
255		reserved	Reserved