<https://chatgpt.com/c/c44c0288-6a50-4ba1-a367-b087780d3caa>

https://www.cloudflare.com/learning/ddos/glossary/internet-control-message-protocol-icmp/

1. What is ICMP protocol?
2. Layer 3 (Network layer) protocol.
3. used by network devices to diagnose network communication issues. ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner.
4. Commonly, the ICMP [protocol](https://www.cloudflare.com/learning/network-layer/what-is-a-protocol/) is used on network devices, such as [routers](https://www.cloudflare.com/learning/network-layer/what-is-a-router/).
5. ICMP is crucial for error reporting and testing, but it can also be used in [distributed denial-of-service (DDoS) attacks](https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/).
6. What is ICMP used for?

a. The primary purpose of ICMP is for error reporting. When two devices connect over the Internet, the ICMP generates errors to share with the sending device in the event that any of the data did not get to its intended destination.

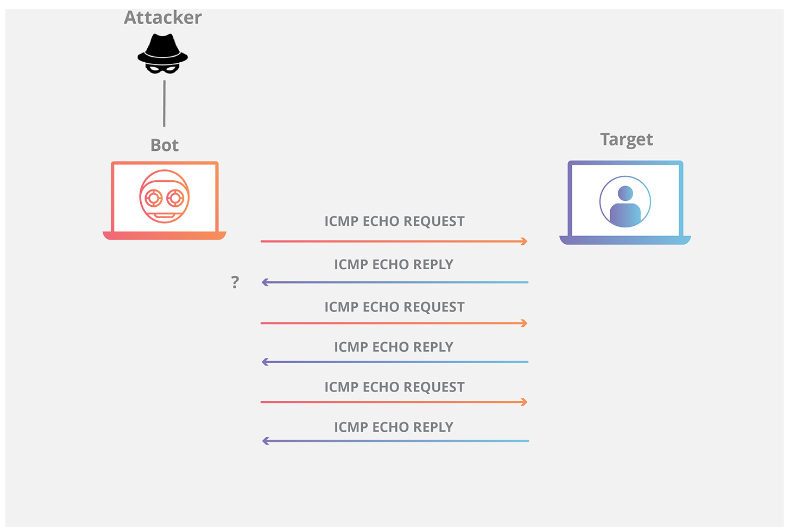
b. For example, if a [packet](https://www.cloudflare.com/learning/network-layer/what-is-a-packet/) of data is too large for a router, the router will drop the packet and send an ICMP message back to the original source for the data.

c. A secondary use of ICMP protocol is to perform network diagnostics; the commonly used terminal utilities traceroute and ping both operate using ICMP.

d. A ping will test the speed of the connection between two devices and report exactly how long it takes a packet

of data to reach its destination and come back to the sender’s device.

1. Traceroute gives the exact number of hops taken to reach a domain.
2. The ICMP echo-request and echo-reply messages are commonly used for the purpose of performing a ping.
3. Unfortunately network attacks can exploit this process, creating means of disruption such as the [ICMP flood attack](https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack/) and the [ping of death](https://www.cloudflare.com/learning/ddos/ping-of-death-ddos-attack/) attack.



1. How does ICMP work?
2. Unlike the [Internet Protocol (IP)](https://www.cloudflare.com/learning/network-layer/internet-protocol/), ICMP is not associated with a transport layer protocol such as [TCP](https://www.cloudflare.com/learning/ddos/glossary/tcp-ip/) or [UDP](https://www.cloudflare.com/learning/ddos/glossary/user-datagram-protocol-udp/).
3. Connection-less protocol-one device does not need to open a connection with another device before sending an ICMP message.
4. An ICMP packet is a packet that uses the ICMP protocol. ICMP packets include an ICMP header after a normal IP header. When a router or server needs to send an error message, the ICMP packet body or data section always contains a copy of the IP header of the packet that caused the error.
5. ICMP message structure?
6. An ICMP message is encapsulated within an IP packet. The structure typically includes:
   1. **Type**: Specifies the type of the message (e.g., Echo Request, Echo Reply).
   2. **Code**: Provides additional context about the message type (e.g., for Destination Unreachable, it indicates why the destination is unreachable).
   3. **Checksum**: Used for error-checking the message.
   4. **Data**: Varies depending on the type of ICMP message. For example, in an Echo Request, this field contains the data to be echoed back in the Echo Reply.