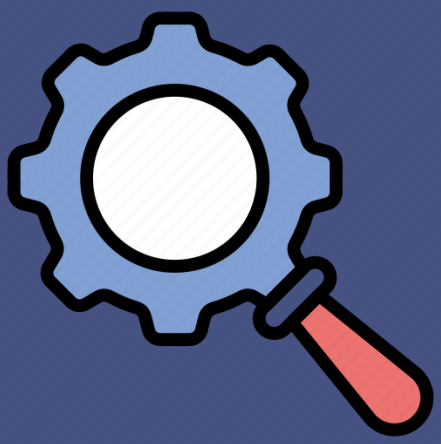
ICMP

All you need to know

1

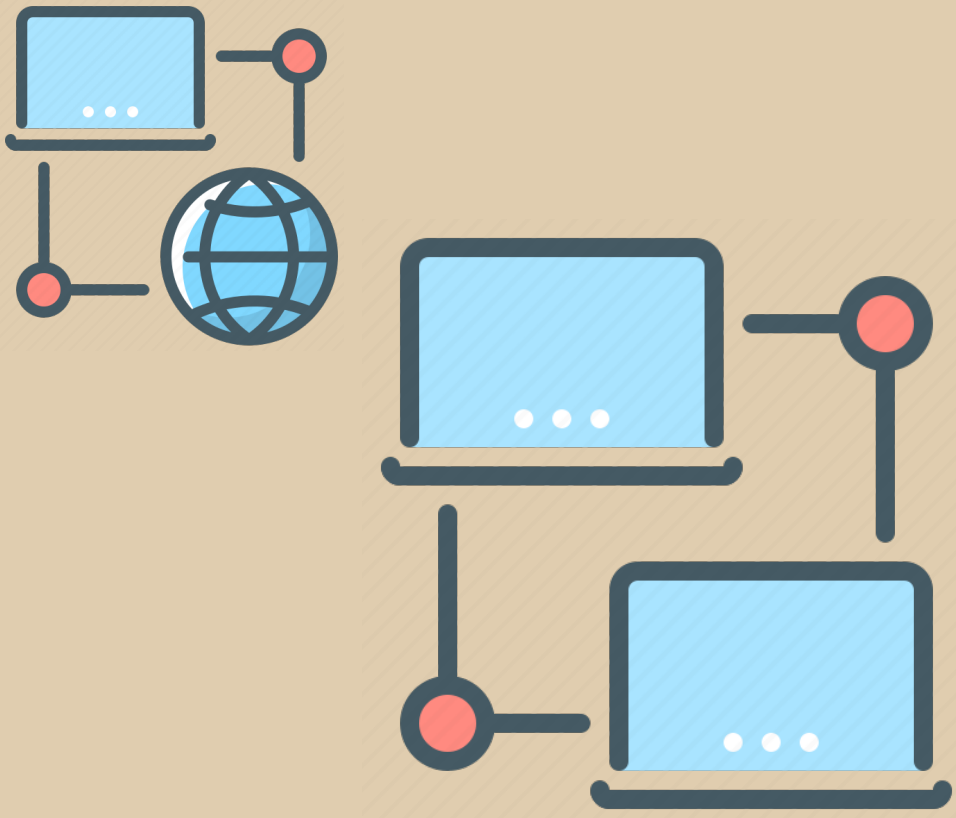
Introduction and History



What is ICMP, from where it came from, and to what you can use it

So, what is ICMP?

If you answered I Can Make Pings, well, you’re not wrong, but the reality is that you can make a lot more than just pings with ICMP,that actually means Internet Control Message Protocol.



To what we can use it?

ICMP is mainly used to send control and diagnostic messages about the state of the network, such as in the case of 'ping' packets to check connectivity between devices, and to assist in the proper delivery of IP packets and in communicating network errors. However, it does not carry any user data. It is a protocol that operates at Layer 3 of the OSI (Open Systems Interconnection) model, the Network Layer.

To what we can use it?

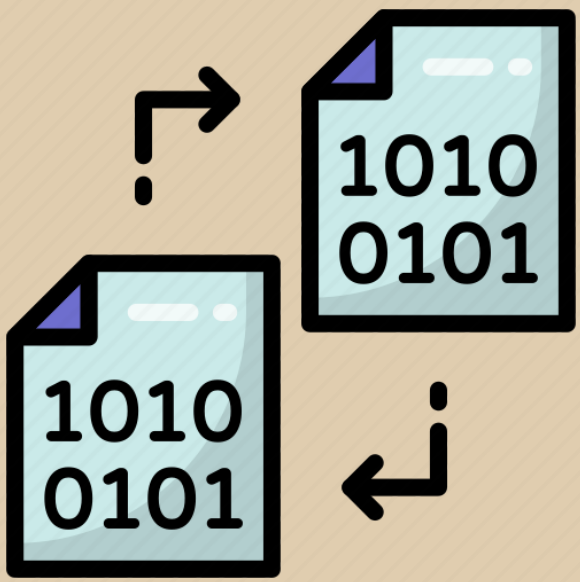
The way ICMP works in network communication is similar to the communication that happens between a carpenter building a house and a hardware store. The store sends nails, flooring, roofing materials, insulation, and much more, as long as each component arrives in the correct order.

To what we can use it?

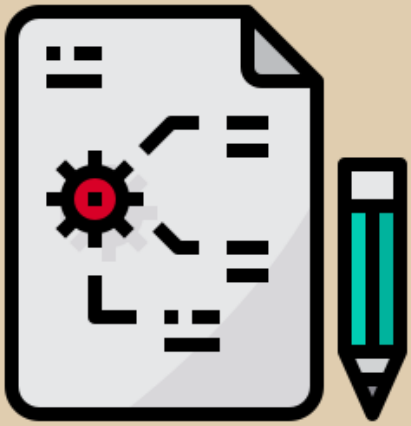
For example, when the carpenter starts building a wall, he requests 28 studs, 5 kilos of nails, and a door. He needs to place the nails first, the studs second, and the door last. The hardware store sends them in that order, but the door arrives first. This won't work because there's no way to hang a door without first having a wall. So, the carpenter asks the store to resend the nails and studs, and the store resends them, instructing the driver to take a different route.

To what we can use it?

ICMP works like the communication between the carpenter and the store. It transmits messages from the receiver to the sender about the data that should arrive. If the data doesn't reach the receiver or arrives in the wrong order, ICMP informs the sender so the data can be resent. In this way, ICMP is simply a protocol for communicating information about data, but it doesn't manage the data itself.



History



ICMP was introduced as part of the Internet protocol suite with the creation of IPv4. Its development was necessary to handle error control and diagnostics in IP network communication. It was initially specified in 1981 in the RFC 792 document by Jon Postel.

History

ICMP was created to provide a way to send error messages and other operational information, helping Internet communication to be more efficient and robust. Unlike protocols such as TCP or UDP, ICMP is not used to transfer application data between devices; rather, it is used to report errors and provide operational information, such as network troubleshooting diagnostics. Over time, ICMP has evolved to include more functionalities and versions.

2

Messages

Types of messages, classes, and categories.

Error Messages

Code 3 - Destination Unreachable

Indicates that a destination is unreachable due to a variety of reasons (such as unreachable network, host, port, or protocol).

Error Messages

Code 11 - Time Exceeded

Informs that the time to live (TTL) of a packet has expired (TTL=0), typically used in route tracing (ex. Traceroute).

Error Messages

Code 12 - Parameter Problem

Signals an error in a field of the IP packet header.

Error Messages

Code 5 - Redirect

Indicates that a host should use a different route to reach the destination.

Error Messages

Code 4 - Source Quench

Is used to inform the sender that the traffic is being sent too quickly and that it should reduce the packet sending rate.

Informational Messages

Codes 8 and 0 - Echo Request and Echo Reply

Are used for testing connectivity between network devices (ex., the ping command).

Informational Messages

Codes 13 and 14 - Timestamp Request and Timestamp Reply

Are used to synchronize times between devices.

Informational Messages

Codes 17 and 18 - Address Mask Request and Address Mask Reply

Are used to obtain the subnet mask of a device.

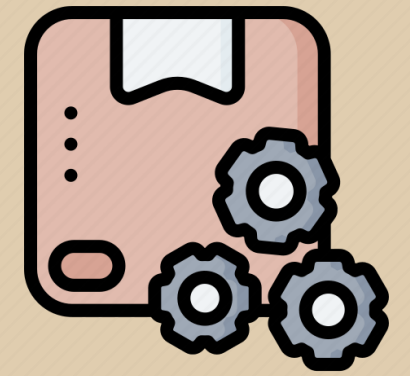
3

ICMP Packet Structure

Components and Operation of ICMP Packets

Components-Header

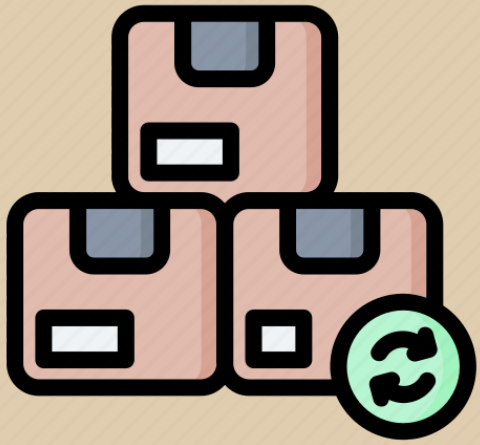
An ICMP packet consists of an ICMP header and an ICMP data section.



The ICMP header contains information about the type of packet, its code, the checksum, and an identifier. When ICMP packets are sent, the recipient of the message reads the header information. Based on the packet type, it performs the appropriate action. For example, if the type is an echo request, the recipient will send back an echo reply with the same data. If the type is destination unreachable, the recipient will respond with a destination unreachable message.

Components-Data Section

The data section in an ICMP message includes information such as the destination IP address or the cause of the failure. It also contains error codes or numerical codes that identify the errors, such as a destination unreachable code (Type 3) indicating that the recipient's device does not exist on the network, or a redirect code (Type 5) sending a message to another router indicating a better route to the destination.



Difference from IP and TCP

Unlike the Internet Protocol (IP), ICMP is not associated with a transport layer protocol like TCP or UDP. This makes ICMP a connectionless protocol: a device does not need to establish a connection with another device before sending an ICMP message. Regular IP traffic is sent using TCP, which means that any two devices exchanging data will first perform a TCP handshake to ensure that both devices are ready to receive data. ICMP does not establish a connection in this way. The ICMP protocol also does not allow for directing to a specific port on a device.

4

ICMP Security

Vulnerabilities and Common Attacks on the ICMP Protocol

How and why

ICMP, originally designed for status communication between devices, lacks robust authentication and encryption mechanisms. This makes it susceptible to attacks such as the ICMP Smurf, ICMP Flood, and ICMP Redirect Attack, where attackers can exploit the protocol to perform denial of service (DoS) or redirect malicious traffic. Since ICMP is generally allowed for diagnostic purposes, it can serve as an entry point for attackers if not properly filtered or monitored.

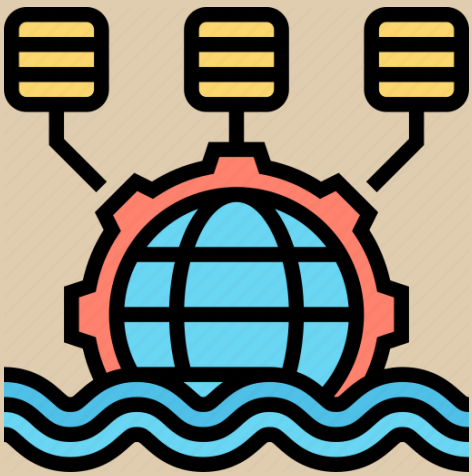
How and why

ICMP, originally designed for status communication between devices, lacks robust authentication and encryption mechanisms. This makes it susceptible to attacks such as the ICMP Smurf, ICMP Flood, and ICMP Redirect Attack, where attackers can exploit the protocol to perform denial of service (DoS) or redirect malicious traffic. Since ICMP is generally allowed for diagnostic purposes, it can serve as an entry point for attackers if not properly filtered or monitored.

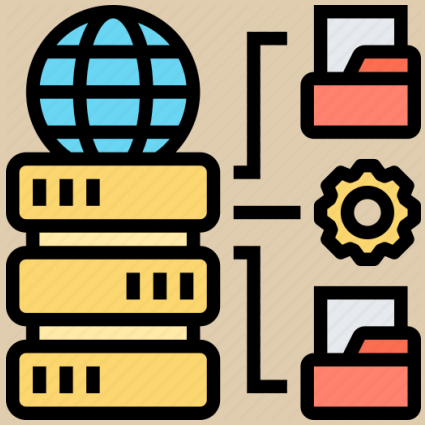
Attacks

Ping Flood

A Denial of Service (DoS) attack where the attacker overwhelms the target with ICMP Echo Requests (pings). This attack consumes both incoming and outgoing bandwidth, congesting the network and slowing down the target's connectivity, potentially taking it offline.



Attacks



Ping of Death

Ping of Death: Another type of Denial of Service (DoS) attack that involves sending ICMP packets (usually "ping") larger than the limit allowed by the IP protocol. This can cause the target system to experience bugs, crashes, or freeze, as it cannot properly handle fragmented packets that, when reassembled, exceed the allowed limit of 65,535 bytes.

Attacks

ICMP Smurf Attack

This attack uses a mechanism called “Spoofing,” where the attacker uses a forged source address that resembles the victim's. The attacker then sends large numbers of requests to devices on a network, all of which respond with ICMP packets to the victim, overwhelming it.

Attacks

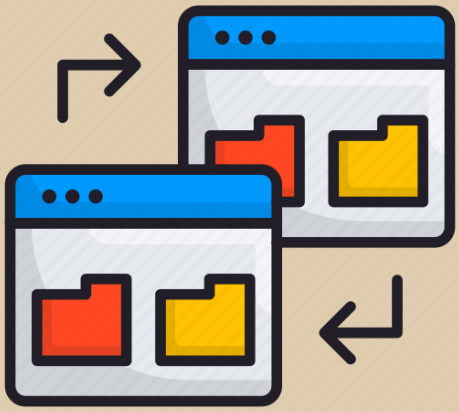
ICMP Redirect Attack

ICMP Redirect Attack: The ICMP redirect attack exploits the legitimate traffic redirection functionality used to alter packet routes. An attacker can send a false ICMP redirect message to a host, causing it to modify its routing table and redirect traffic to a route controlled by the attacker, enabling data interception or manipulation.

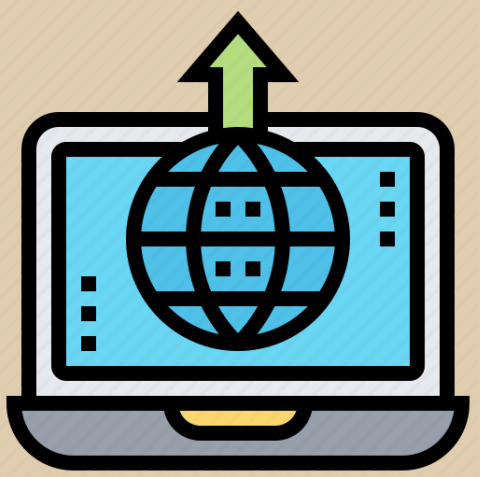
Attacks

ICMP Tunneling

ICMP tunneling is a technique that allows the use of the ICMP protocol to encapsulate and transmit data between two systems, creating a hidden communication channel. This can be used by attackers to bypass firewalls or other security measures, as ICMP traffic is generally allowed for network diagnostics.



Attacks



ICMP Flood Attack

Very similar to the Ping Flood attack, this involves the attacker sending a large number of ICMP packets to a target to overwhelm it, but this attack does not require waiting for responses to the sent packets.

Attacks

Traceroute Flood

In the Traceroute Flood attack, the attacker uses the "traceroute" command to send large volumes of ICMP TTL (Time to Live) packets to a server or network. The goal is to overwhelm the destination with an excessive amount of ICMP TTL responses, causing slowdowns or service outages.

4

Practical Example

How you can test ICMP Protocol from your house

Step One
Discovering your IP Adress

The first step to 'ping' an address is to find the address of the machine you want to test the connection with. In this example, we will ping our own machine. First, we need to find out the IP address that has been assigned to it. We can do this by opening a command prompt and typing the command *'ipconfig'* for Windows and *'ifconfig'* for Linux.

Step Two
Identifying the network adapter

After executing the command we saw earlier, a list of all the network adapters configured on your machine should appear. All you need to do is navigate through the list and identify which one your connection is using.

Some information should appear along with the adapter's name, including the IP address being used by the machine, the subnet mask, and the default gateway.

Step Three
Let’s ping!

Memorize the IPv4 address of your network adapter (you can write it down somewhere if you prefer), and just type *'ping'* followed by the address we just found, with a space between them. You will see the ping packets being sent and the response packets arriving at your machine.

Congratulations! You have just put the ICMP protocol into practice using its codes *8* and *0*, *echo request* and *echo reply*.

Step One Again!

Another way to test the ICMP Protocol is through the *‘tracert’* command. It will list all the route that is necessary to arrive at some sever on the internet, and all the IP adresses it must go through in the process. To test it, it’s just think about one website of your preference, that you would like to see all the steps your machine takes to arrive to it.

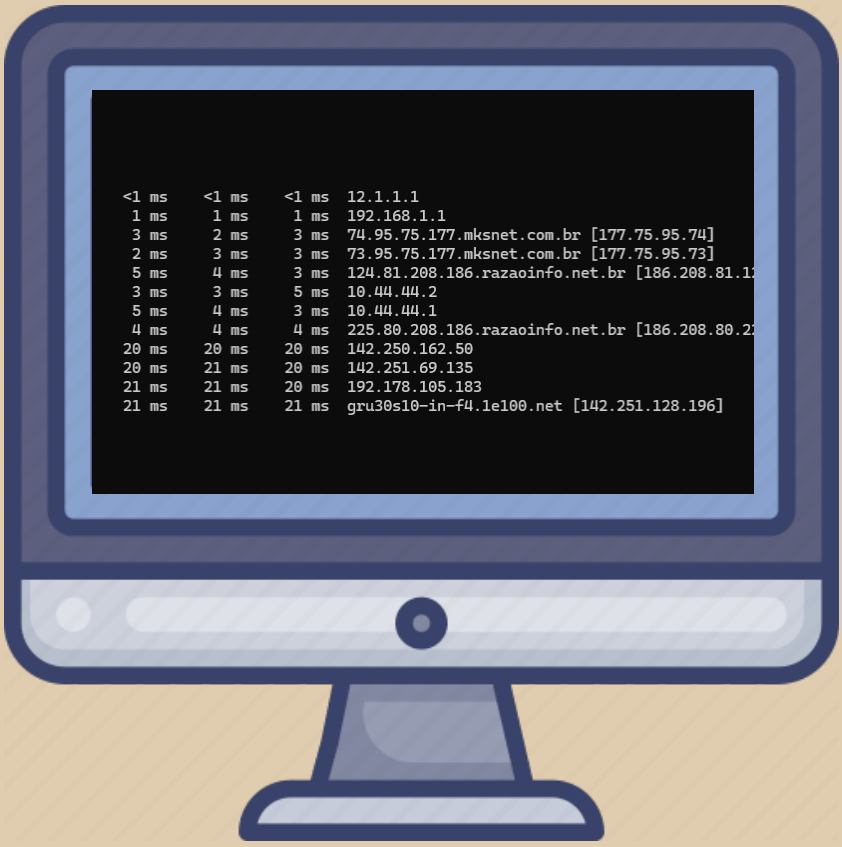
Step Two
Let’s travel!

The *‘tracert’* command is very simple. It’s just open a command prompt in your computer, and type *‘tracert’* plus the address of the website you want to travel around all the IPs with, with a space between them.

For example, if we want to travel until the google server, we just need to type *‘tracert www.google.com’*, and click enter, and it’s done!

Step Three
View the path

You'll see all the history of the path your machine had to take to arrive at the google server! With the time each one taked to redirect to the next.



Fantastic, isn't?!

5

How to learn more

If you want to learn more abou the ICMP, we can help you!

How to find help!

If you have any questions, or would like to talk a little bit more about the subjects you've found in this book, you can contact us!

nathalielaise@gmail.com

instagram.com/grey.wind_

github.com/NathaliePatzer

linkedin.com/in/nathaliepatzer

Thank you! ;)