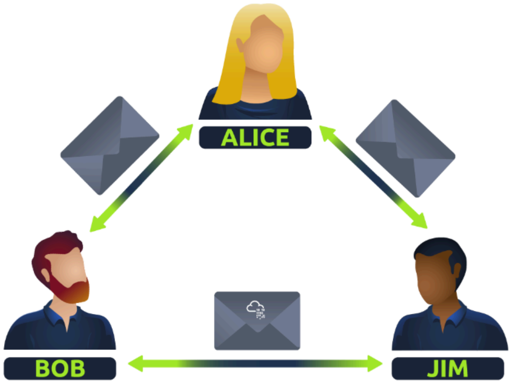
Network

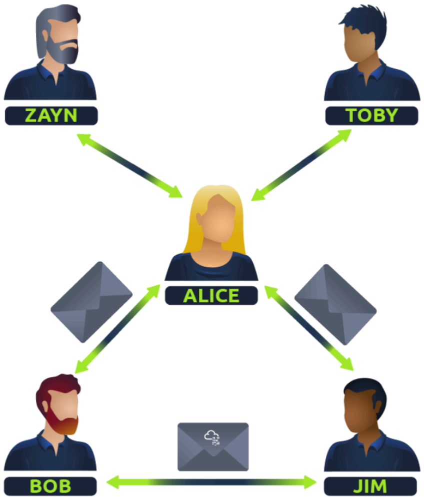
Networks are simply things connected. For example, your friendship circle: you are all connected because of similar interests, hobbies, skills and sorts.

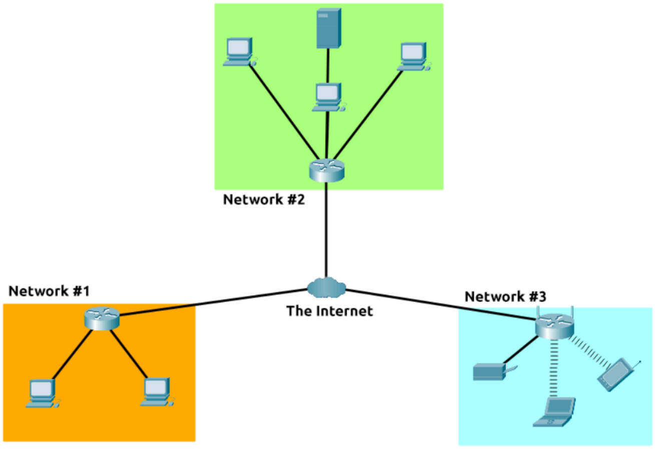
In computing, a network can be formed by anywhere from 2 devices to billions. These devices include everything from your laptop and phone to security cameras, traffic lights and even farming!



Internet

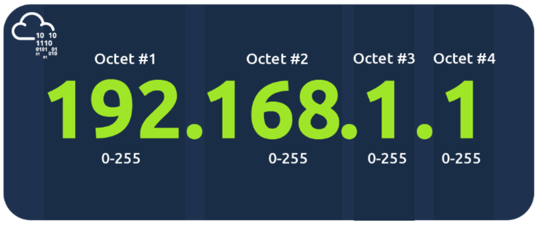
The Internet is one giant network that consists of many, many small networks within itself.



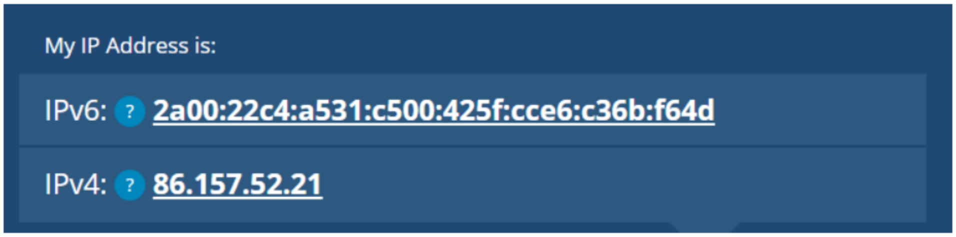


IP Address

IP (Internet Protocol) address can be used as a way of identifying a host on a network.



A public address is used to identify the device on the Internet, whereas a private address is used to identify a device amongst other devices.



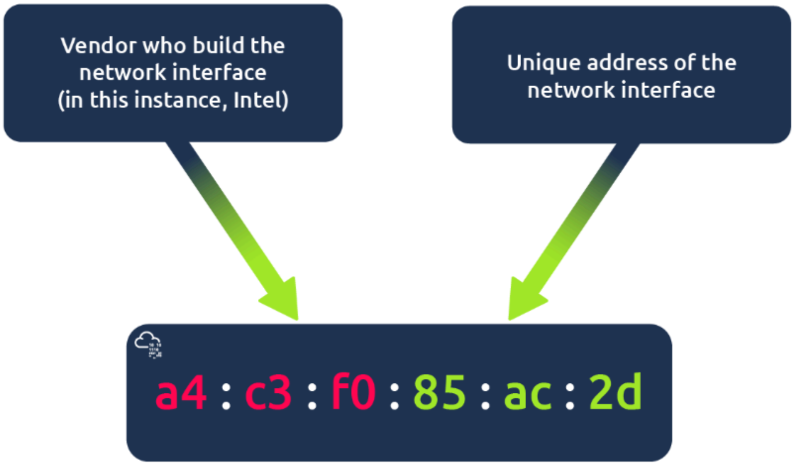
My IP Address is:

IPv6: ? 2a00:22c4:a531:c500:425f:cce6:c36b:f64d

IPv4: ? 86.157.52.21

MAC Address

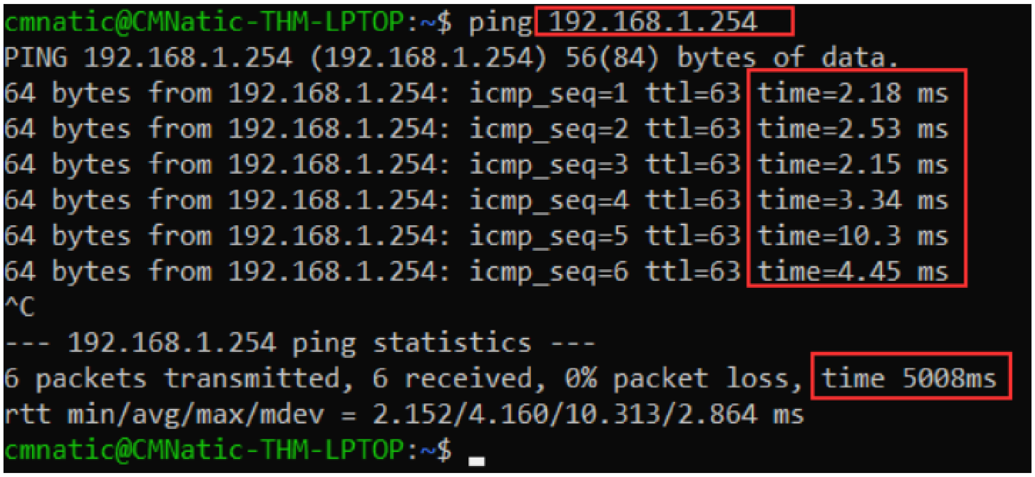
Devices on a network will all have a physical network interface, which is a microchip board found on the device's motherboard. This network interface is assigned a unique address at the factory it was built at, called a MAC (Media Access Control) address. The MAC address is a twelve-character hexadecimal number. The first six characters represent the company that made the network interface, and the last six is a unique number.


Vendor who build the network interface (in this instance, Intel)
Unique address of the network interface
a4 : c3 : f0 : 85 : ac : 2d

Ping

Ping is one of the most fundamental network tools available to us. Ping uses ICMP (Internet Control Message Protocol) packets to determine the performance of a connection between devices, for example, if the connection exists or is reliable.

Ping can be performed against devices on a network, such as your home network or resources like websites. This tool can be easily used and comes installed on Operating Systems (OSs) such as Linux and Windows. The syntax to do a simple ping is `ping IP address or website URL`. Let's see this in action in the screenshot below.



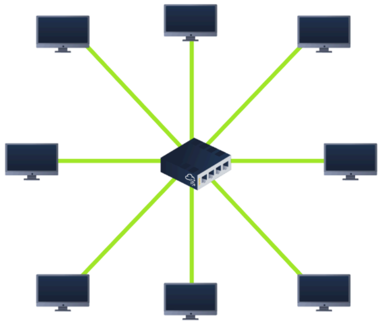
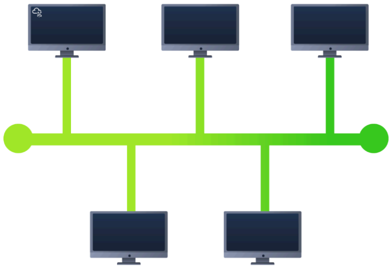
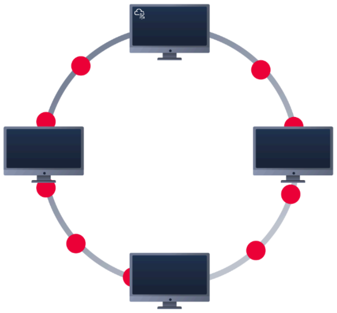
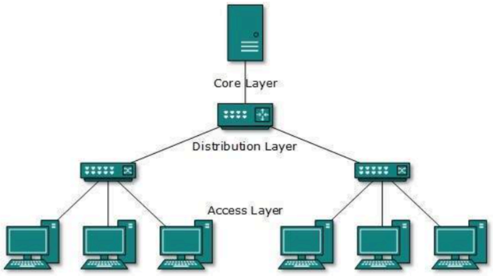
```
cmnatic@CMNatic-THM-LPTOP:~$ ping 192.168.1.254
PING 192.168.1.254 (192.168.1.254) 56(84) bytes of data.
64 bytes from 192.168.1.254: icmp_seq=1 ttl=63 time=2.18 ms
64 bytes from 192.168.1.254: icmp_seq=2 ttl=63 time=2.53 ms
64 bytes from 192.168.1.254: icmp_seq=3 ttl=63 time=2.15 ms
64 bytes from 192.168.1.254: icmp_seq=4 ttl=63 time=3.34 ms
64 bytes from 192.168.1.254: icmp_seq=5 ttl=63 time=10.3 ms
64 bytes from 192.168.1.254: icmp_seq=6 ttl=63 time=4.45 ms
^C
--- 192.168.1.254 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 2.152/4.160/10.313/2.864 ms
cmnatic@CMNatic-THM-LPTOP:~$
```

Here we are pinging a device that has the private address of 192.168.1.254. Ping informs us that we have sent six ICMP packets, all of which were received with an average time of 4.16 milliseconds.

LAN (Local Area Network)

A Local Area Network (LAN) is a network that connects computers and devices within a small geographical area, such as a home, office, school, or laboratory.

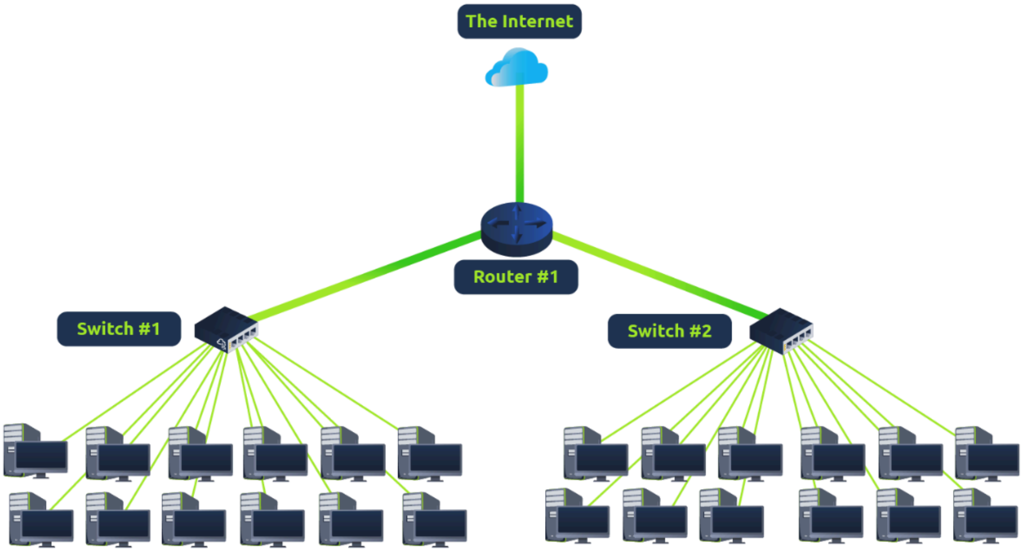
Local Area Network (LAN) Topologies:

1.Star Topology: All devices connect to a central device (Switch or Hub). If the hub fails, connectivity of all hosts to all other hosts fails.	
2. Bus Topology: This type of connection relies upon a single connection which is known as a backbone cable. It is one of the simple forms of networking where a failure of a device does not affect the other devices. But failure of the shared communication line can make all other devices stop functioning.	
3. Ring Topology: In ring topology, each host machine connects to exactly two other machines, creating a circular network structure. Failure of any host results in failure of the whole ring.Thus, every connection in the ring is a point of failure.	
4. Tree Topology: Also known as Hierarchical Topology, this is the most common form of network topology in use presently. if the root goes down, then the entire network suffers even.though it is not the single point of failure.	

Switch & Hub

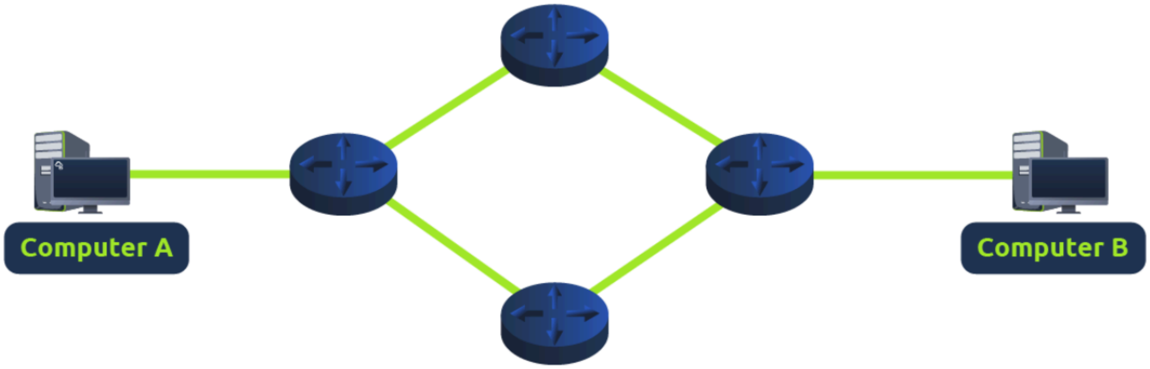
A Switch is a networking device that connects devices in a LAN and forwards data only to the intended destination device.

A Hub is a basic networking device that connects multiple computers in a LAN and broadcasts data to all connected devices.



Router

A Router is a networking device that connects different networks and routes data packets between them using IP addresses.

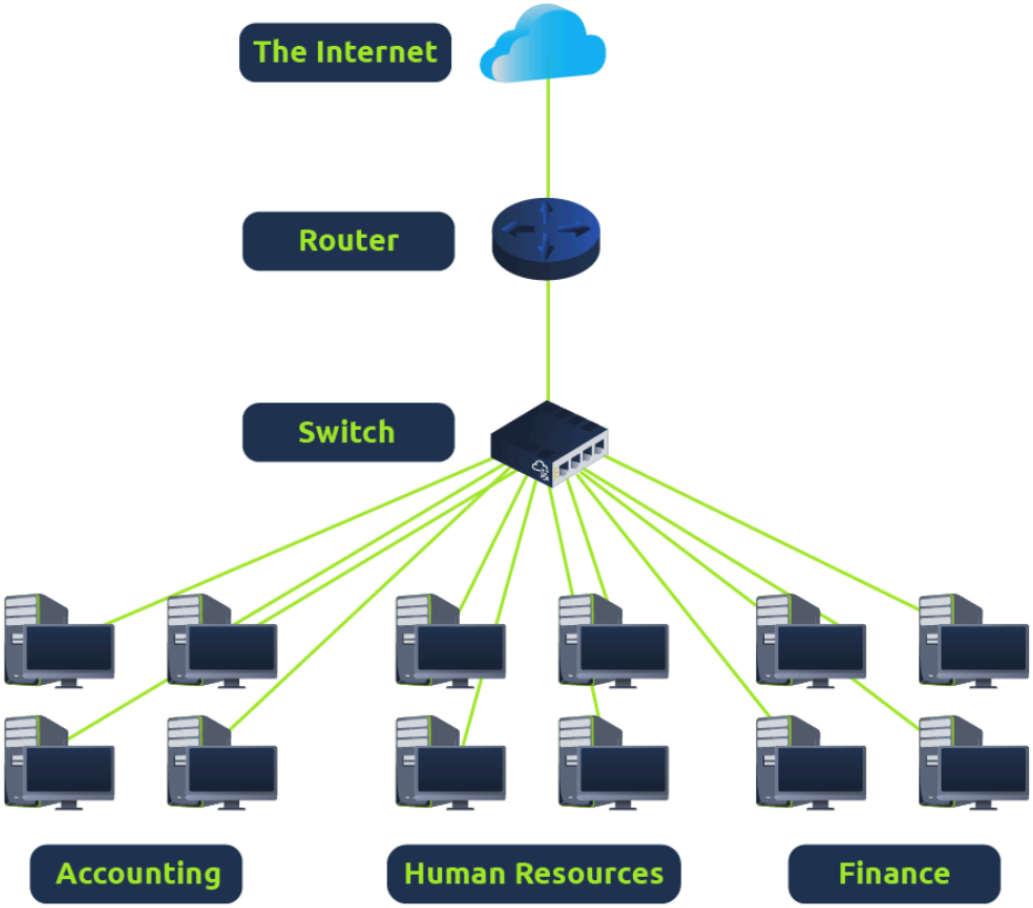


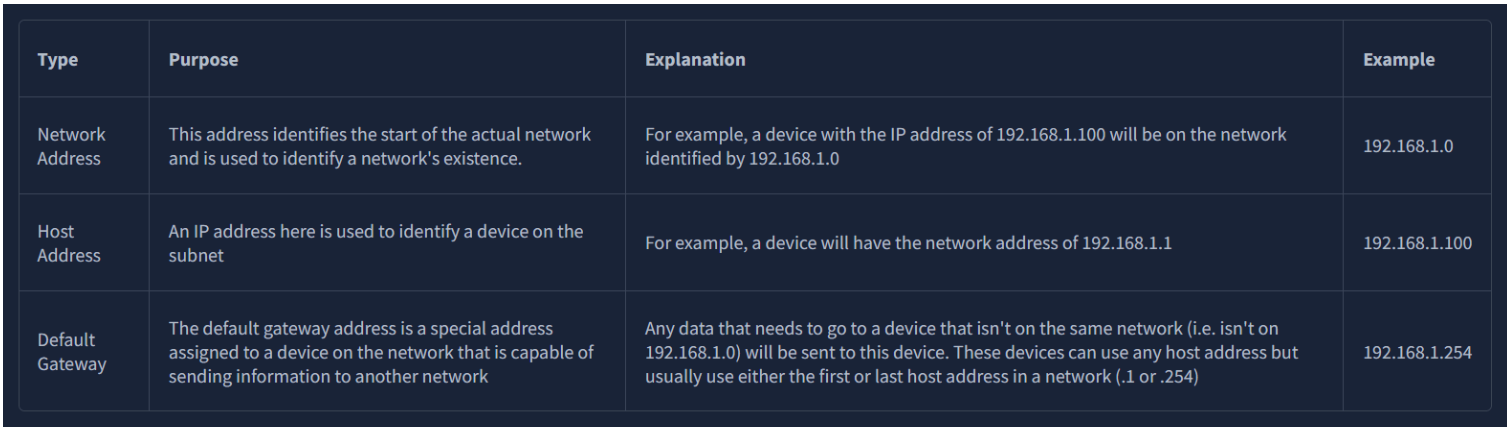
Subnetting

Subnetting is the process of dividing a large network into smaller networks (subnets) to improve performance, security, and management.

Take a business, for example; You will have different departments such as:

1. Accounting
2. Finance
3. Human Resources





Type	Purpose	Explanation	Example
Network Address	This address identifies the start of the actual network and is used to identify a network's existence.	For example, a device with the IP address of 192.168.1.100 will be on the network identified by 192.168.1.0	192.168.1.0
Host Address	An IP address here is used to identify a device on the subnet	For example, a device will have the network address of 192.168.1.1	192.168.1.100
Default Gateway	The default gateway address is a special address assigned to a device on the network that is capable of sending information to another network	Any data that needs to go to a device that isn't on the same network (i.e. isn't on 192.168.1.0) will be sent to this device. These devices can use any host address but usually use either the first or last host address in a network (.1 or .254)	192.168.1.254

Network address:
The network address identifies the start of a network. It represents the network itself, not any device.
If a device has IP 192.168.1.100, it belongs to the 192.168.1.0 network.
Host address:
A host address is assigned to a device (PC, phone, printer, server).
Valid Host Addresses:
192.168.1.1 → 192.168.1.254
Default gateway:
The default gateway is the device (usually a router) that sends data outside the local network.
Default Gateway: 192.168.1.254
(or sometimes 192.168.1.1)
If a device wants to access Google, traffic goes to the default gateway first.

ARP (Address Resolution Protocol)

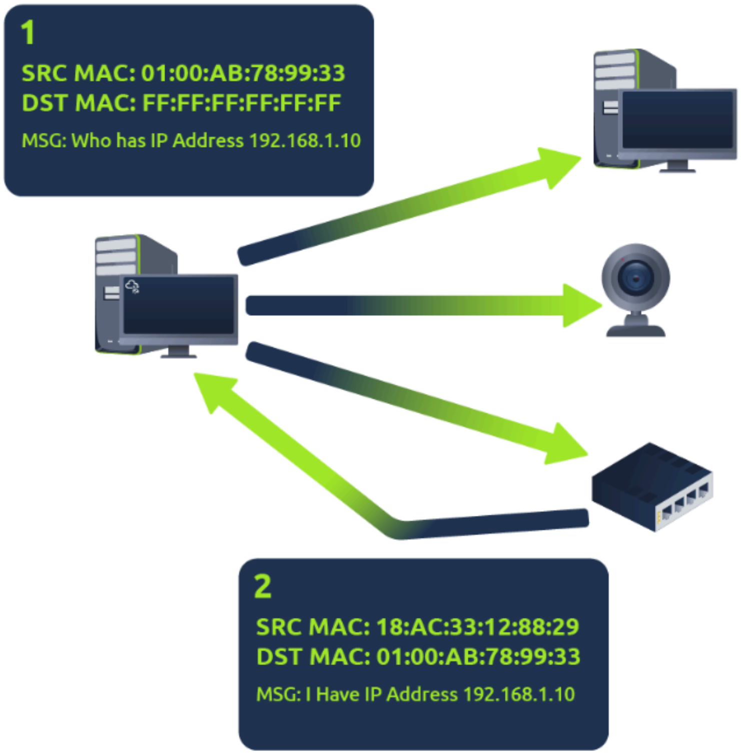
The Address Resolution Protocol or ARP for short, is the technology that is responsible for allowing devices to identify themselves on a network.

ARP (Address Resolution Protocol) is used to map an IP address to a MAC address inside a local network (LAN)
Computers communicate using MAC addresses, but users work with IP addresses — ARP connects the two.

In order to map these two identifiers together (IP address and MAC address), ARP sends two types of messages:

ARP Request:	**ARP Reply:**
An ARP Request is a broadcast message sent by a device to ask: “Who has this IP address?” A device wants to send data to 192.168.1.5 ↓ It checks its ARP cache ↓ If MAC not found → sends ARP Request ↓ Message is broadcast to all devices	An ARP Reply is a unicast message sent by the device that owns the requested IP address, providing its MAC address. Device with IP 192.168.1.5 receives ARP Request ↓ It responds with its MAC address ↓ Sender stores this info in ARP cache ↓ Data transmission begins

This process is illustrated in the diagram below:



1

SRC MAC: 01:00:AB:78:99:33
DST MAC: FF:FF:FF:FF:FF:FF

MSG: Who has IP Address 192.168.1.10

2

SRC MAC: 18:AC:33:12:88:29
DST MAC: 01:00:AB:78:99:33

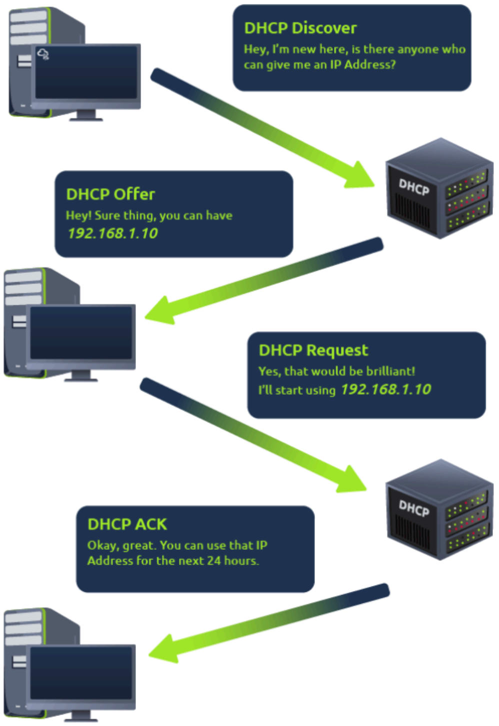
MSG: I Have IP Address 192.168.1.10

DHCP (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) is a network protocol that automatically assigns IP addresses and other network settings to devices on a network. It removes the need for manual IP configuration.

DHCP works in 4 steps, called DORA:

Discover: Client broadcasts: “Is there any DHCP server?”
Offer: Server responds with: “You can use this IP address”
Request: Client replies: “I accept this IP address”
Acknowledge: Server confirms: “IP address assigned”



DHCP Discover
Hey, I'm new here, is there anyone who can give me an IP Address?

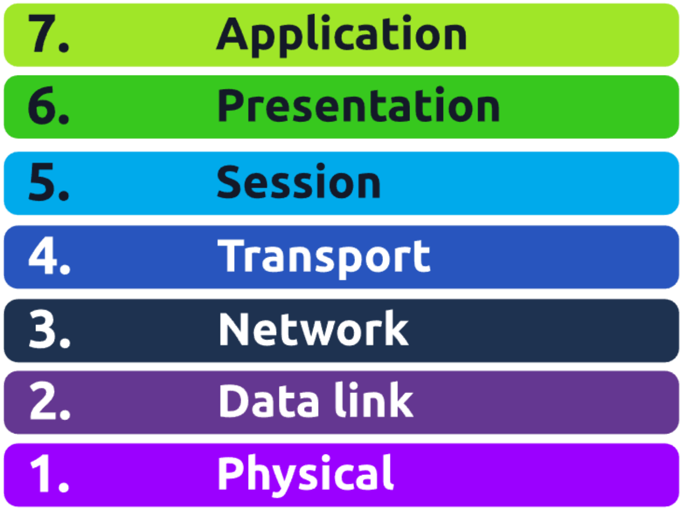
DHCP Offer
Hey! Sure thing, you can have *192.168.1.10*

DHCP Request
Yes, that would be brilliant!
I'll start using *192.168.1.10*

DHCP ACK
Okay, great. You can use that IP Address for the next 24 hours.

OSI Model

The OSI Model is a 7-layer conceptual model that explains how data travels from one device to another over a network. It helps in understanding, designing, and troubleshooting networks.



Layer-7 (Application): The Application Layer provides network services directly to the end user. It allows user applications like web browsers and email clients to communicate with the network.
Example: Opening a website, sending an email, or chatting on WhatsApp.

Layer-6 (Presentation): The Presentation Layer is responsible for formatting and translating data so that different systems can understand it. It also handles encryption, decryption, and data compression to ensure secure communication.
Example: HTTPS encrypting your password, images being displayed correctly on your phone.

Layer-5 (Session): The Session Layer manages and controls communication sessions between devices. It establishes, maintains, and terminates connections to ensure smooth data exchange.
Example: Staying logged into a Zoom meeting or an online exam session.

Layer-4 (Transport): The Transport Layer ensures reliable or fast delivery of data between devices. It controls error checking, flow control, and data segmentation.
Example: File download using TCP, video streaming or online gaming using UDP.

Layer-3 (Network): The Network Layer is responsible for logical addressing and routing of data between different networks. It determines the best path for data to reach its destination.
Example: Sending data from your home network to a server in another country.

Layer-2 (Data link): The Data Link Layer manages physical addressing using MAC addresses. It ensures error-free data transfer between two directly connected devices.
Example: Your Wi-Fi router sending data to your laptop instead of your phone.

Layer-1 (Physical): The Physical Layer deals with the physical transmission of raw bits over a communication medium. It defines cables, voltage levels, connectors, and signal types.
Example: Ethernet cable, Wi-Fi signals, fiber-optic cables.

Packet & Frames

1. Packet: A packet is a unit of data created at the Network Layer (Layer 3). It contains IP addresses that help data travel from one network to another. Packets are used when data needs to move between different networks (LAN to LAN or LAN to Internet). Routers read packet information to decide the best path for the data.

What a Packet Contains:

1. Source IP address
2. Destination IP address
3. Data (payload)

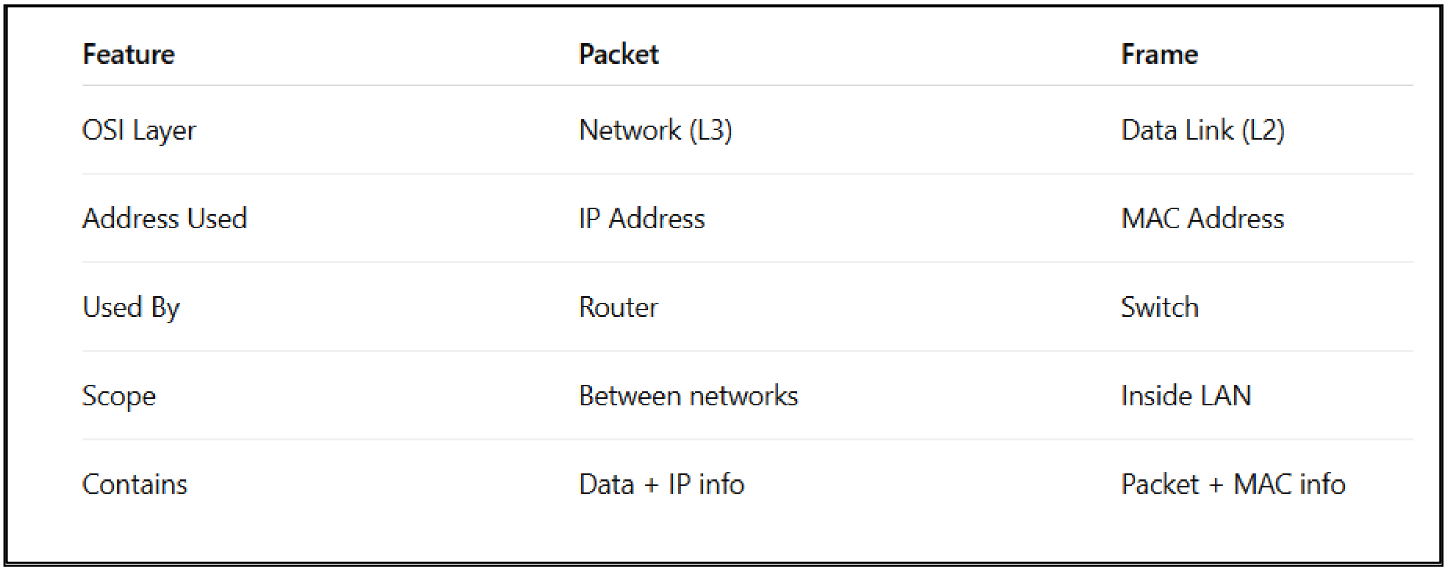
Example:
When you send a message on WhatsApp, the message is broken into packets that travel across the Internet using IP addresses.

2. Frame: A frame is a unit of data created at the Data Link Layer (Layer 2). It contains MAC addresses that help data move inside a local network (LAN). Frames are responsible for delivering data from one device to another within the same network. Switches use frame information to send data to the correct device.

What a Frame Contains:

1. Source MAC address
2. Destination MAC address
3. Encapsulated packet
4. Error-checking information

Example:
When your Wi-Fi router sends data to your laptop at home, the data is sent as a frame using MAC addresses.



Feature	Packet	Frame
OSI Layer	Network (L3)	Data Link (L2)
Address Used	IP Address	MAC Address
Used By	Router	Switch
Scope	Between networks	Inside LAN
Contains	Data + IP info	Packet + MAC info

TCP (Transmission Control Protocol)

TCP (Transmission Control Protocol) is a connection-oriented protocol used to send data reliably over a network. It ensures that data is delivered accurately, in order, and without loss. TCP is used when data accuracy is more important than speed. It is commonly used for applications where losing data is unacceptable. TCP establishes a connection before data transmission begins. This connection remains active until all data is successfully sent and received. OSI layer: 4.

Example: File transfer, emails, web pages.

TCP Header section:

1. Source port number: The source port identifies the application that is sending the data. It helps the receiver know which application sent the data.

2. Destination port number: The destination port identifies the application that should receive the data. It ensures data reaches the correct service.

3. Sequence number: The sequence number keeps track of the order of data segments. It helps TCP reassemble data in the correct order.

4. Acknowledgement number: The acknowledgment number confirms which data has been successfully received. It tells the sender what data should be sent next.

5. Header length: This field specifies the size of the TCP header. It tells where the actual data begins.

6. Window size: The window size controls how much data can be sent before receiving an acknowledgment. It prevents the receiver from being overloaded.

7. Checksum: The checksum is used for error detection. It ensures the data was not corrupted during transmission.

8. Urgent pointer: The urgent pointer indicates urgent data that must be processed immediately. It is rarely used today.

9. Data: This header is where the data, i.e. bytes of a file that is being transmitted, is stored.

TCP Flags (Control Bits)

TCP flags are small on/off indicators used to control communication.

1. SYN (Synchronize): The SYN flag is used to start a TCP connection. It synchronizes sequence numbers between client and server.

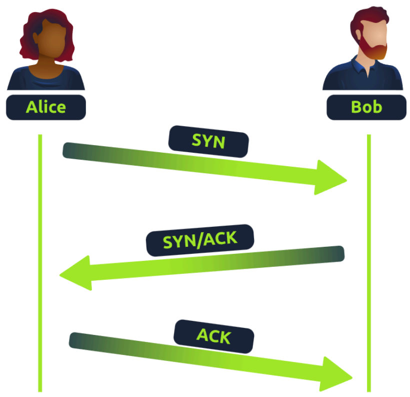
2. ACK (Acknowledgement): The ACK flag confirms that data has been received successfully. It is used in almost every TCP segment after connection setup.

3. DATA: Once a connection has been established, data (such as bytes of a file) is sent via the "DATA" message.

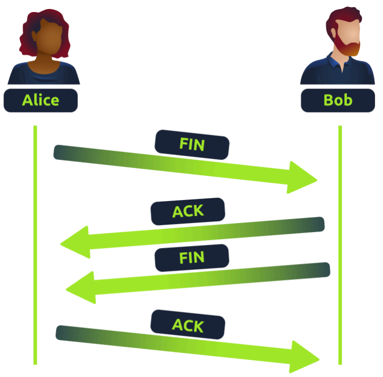
4. FIN (Finish): The FIN flag is used to gracefully close a TCP connection. It indicates that the sender has finished sending data.

5. RST (Reset): The RST flag immediately terminates a connection. It is sent when a problem or error occurs.

Establishing connection



Terminating connection



UDP (User Datagram Protocol)

UDP (User Datagram Protocol) is a connectionless transport layer protocol used to send data without establishing a connection. It focuses on speed rather than reliability. UDP is used when fast data delivery is more important than accuracy. It does not check whether data is lost, duplicated, or arrives in order. UDP does not establish a connection before sending data. Data is sent directly without any handshake. OSI layer: 4.

Example: Live video, voice calls, online games.

UDP Header section:

1. Time To Live (TTL): Limits how long a packet can stay in the network. Prevents packets from looping forever.

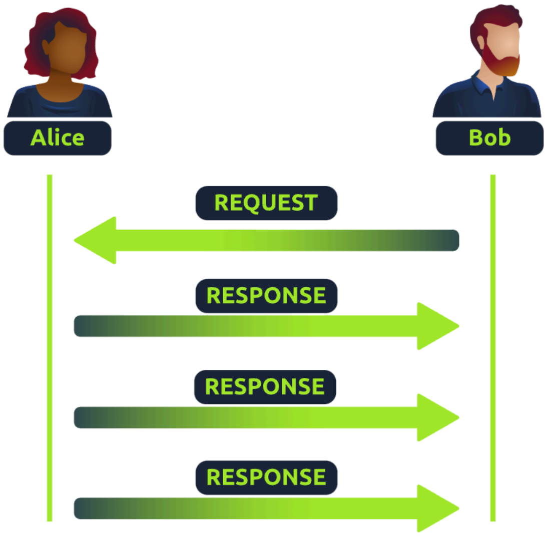
2. Source Address: IP address of the sender. It is used so replies can be sent back.

3. Destination Address: IP address of the receiver. It tells the packet where to go.

4. Source Port: Port number used by the sender's application. It helps identify the sending process.

5. Destination Port: Port number of the receiving application or service. This ensures data reaches the correct service (e.g., 80 for HTTP).

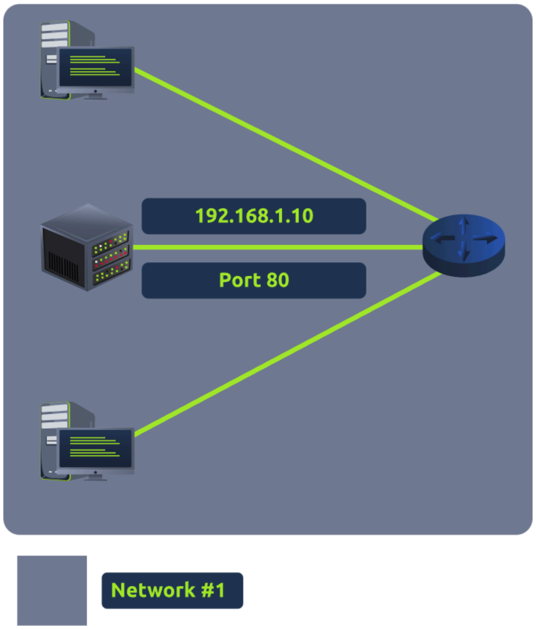
6. Data: Actual information being transmitted. Contains the message or file content.



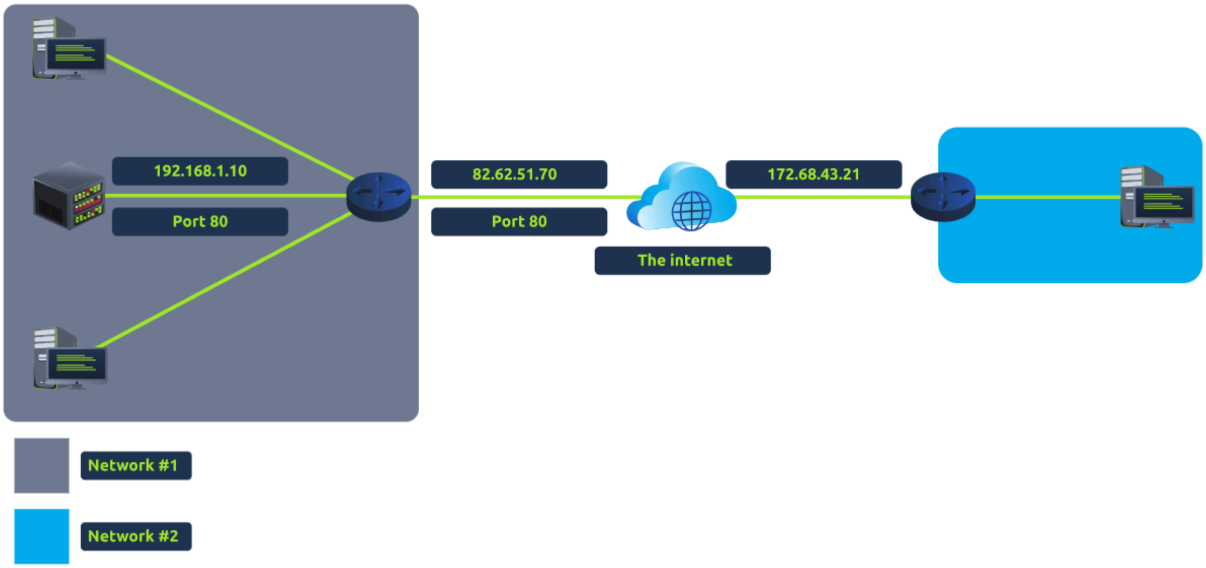
Port forwarding

Port forwarding is a technique used on a router to allow external (internet) traffic to access a specific device or service inside a private network.Normally, devices inside a LAN are hidden behind the router.

Take the network below as an example. Within this network, the server with an IP address of "192.168.1.10" runs a webserver on port 80. Only the two other computers on this network will be able to access it (this is known as an intranet).



If the administrator wanted the website to be accessible to the public (using the Internet), they would have to implement port forwarding, like in the diagram below:



Firewall

A firewall is a security device or software that controls network traffic by allowing or blocking data based on predefined rules. It acts like a gatekeeper between a trusted network (LAN) and an untrusted network (Internet).

A firewall decides to permit or deny traffic based on:

1. Source IP (where traffic comes from)
2. Destination IP (where traffic is going)
3. Port number (e.g., 80, 443)
4. Protocol (TCP, UDP, ICMP)

Firewalls do this using packet inspection.

Stateful firewall:

A stateful firewall tracks the entire connection, not just individual packets.
It understands connection states like TCP handshake (SYN, SYN-ACK, ACK) and makes decisions dynamically.

Key points:

1. Keeps a session table
2. More secure but resource-heavy
3. If a connection is malicious, the entire host can be blocked

Example:
Allows a TCP connection only if the handshake is valid.

Stateless firewall:

A stateless firewall checks each packet independently using fixed rules.
It does not remember previous packets or connections.

Key points:

1. Faster and uses fewer resources
2. Less intelligent
3. Only blocks packets that match exact rules

Example:
Blocks all traffic to port 23 (Telnet), regardless of session state.

VPN (Virtual Private Network)

A VPN creates a secure, encrypted tunnel over the Internet so devices on different networks can communicate as if they were on the same private network. It protects data from sniffing, hides traffic from ISPs, and allows remote access to internal resources.

VPN Technologies:

1. PPP (Point-to-Point Protocol): PPP is responsible for authentication and encryption of data. It cannot route data over the Internet by itself, so it needs another protocol to carry the data.

2. PPTP (Point-to-Point Tunneling Protocol): PPTP creates the tunnel that allows PPP data to travel across networks. It is easy to configure and widely supported, but security is weak compared to modern standards.

3. IPsec (Internet Protocol Security): IPsec encrypts data using the IP protocol framework. It provides strong encryption, integrity, and authentication, but is harder to configure.

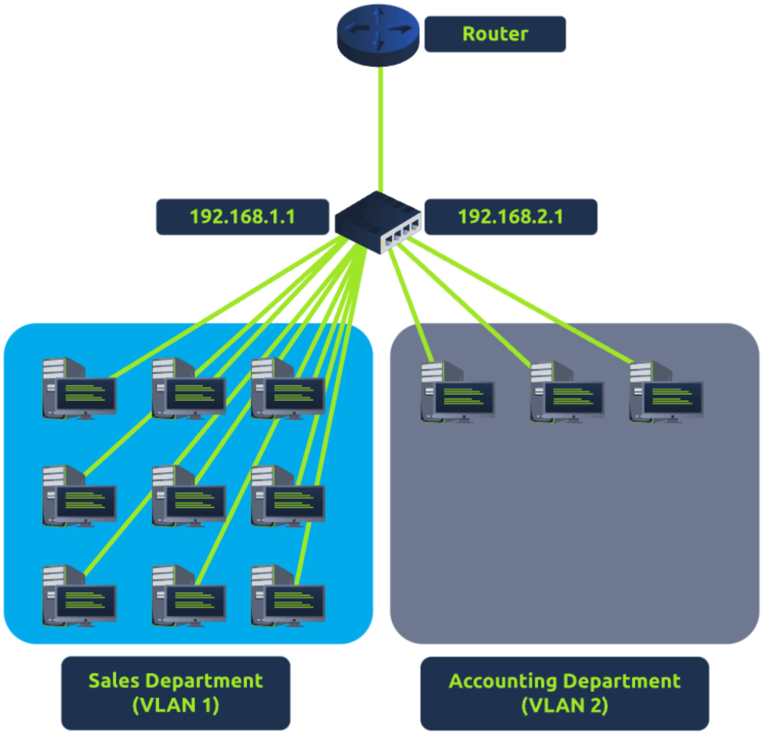
VLAN (Virtual Local Area Network)

A VLAN allows a single physical network (switch) to be logically divided into multiple separate networks. Devices in different VLANs behave as if they are on different networks, even though they are connected to the same switch

VLAN 1 – Sales Department
Network: 192.168.1.0/24
Gateway / Interface: 192.168.1.1

VLAN 2 – Accounting Department
Network: 192.168.2.0/24
Gateway / Interface: 192.168.2.1

Each department is isolated from the other at Layer 2.


Router
192.168.1.1
192.168.2.1
Sales Department (VLAN 1)
Accounting Department (VLAN 2)