Networking for Hackers!

Day12_network.md

by Nathan Hailu

Recalling!

LAST TIME TOPICS

Topics

- Introduction to networking
- Classification of networks
- IP Address
- Mac Address
- OSI Model
- TCP and UDP protocols
- TCP/IP Model
- Networking tools

Introduction to Networking

- A network consists of two or more entities or objects sharing resources and information.
- A computer network consists of two or more computing devices **connected to each other** to share resources and information.
- The network becomes a powerful tool when computers communicate and share resources with other computers on the same network or entirely distinct networks.

...

- Computers on a network can act as a client or a server.

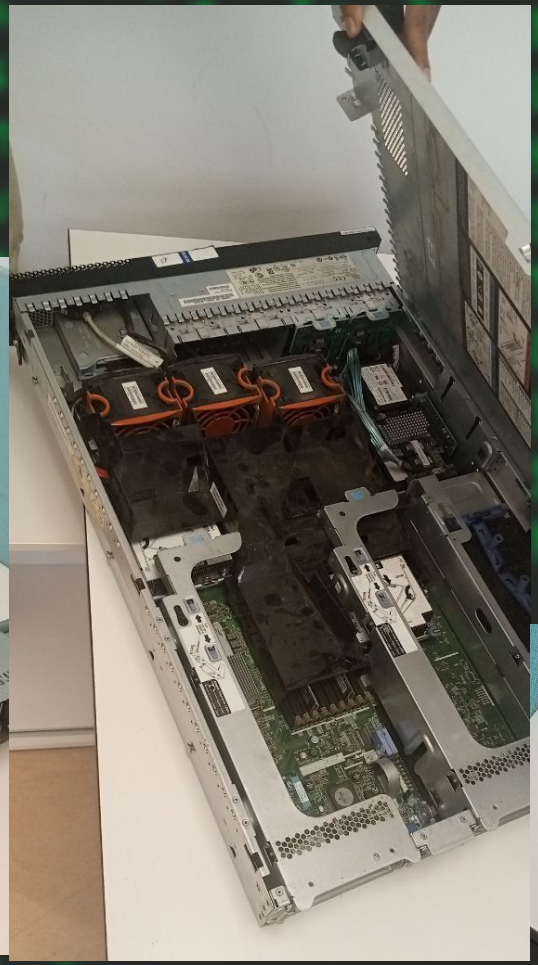
Client computer

- A client is a computer that requests for resources.

Server computer

- A server is a computer that controls and provides access to resources.
- But have higher RAM,CPU and STORAGE

example



Need of Networks

- Enhance communication.
- Share resources.
- Facilitate centralized management
- Internet

Classification of Networks

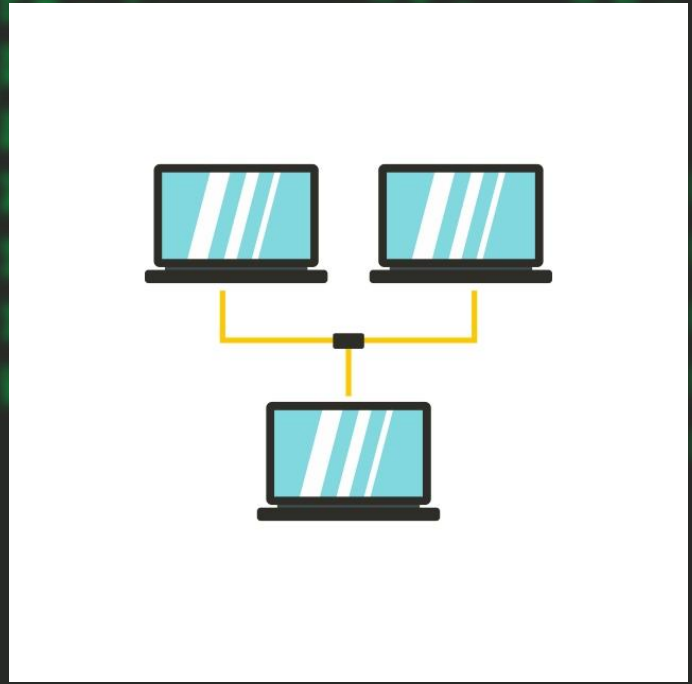
1. Classification by network geography.
2. Classification by component roles.

Classification by Network Geography

- Networks are frequently classified according to the geographical boundaries spanned by the network itself.
- LAN, WAN, and MAN are the basic types of classification, of which LAN and WAN are frequently used

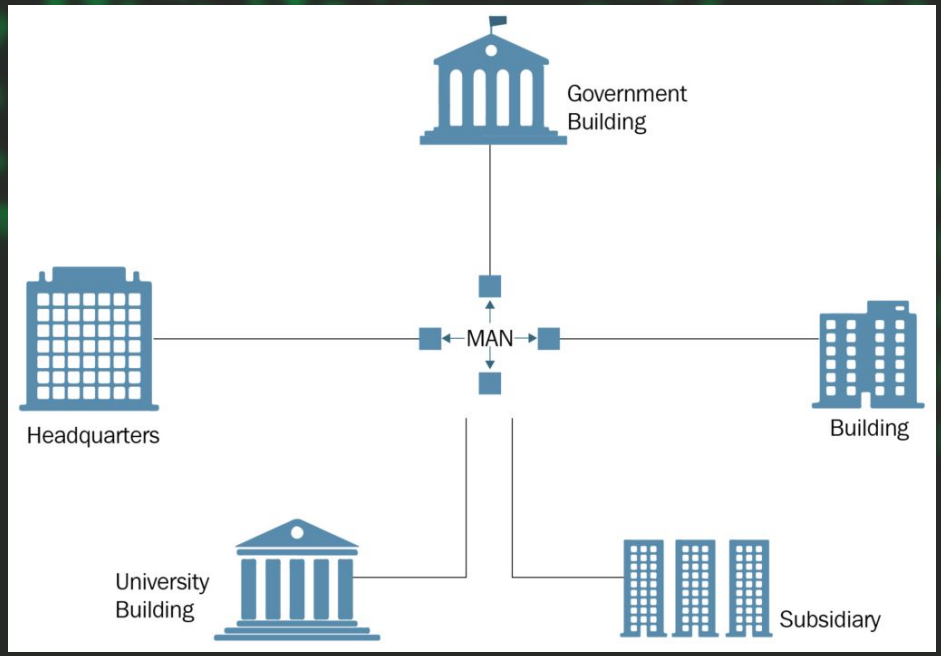
Local area network (LAN)

- A LAN covers a relatively small area such as a classroom, school, or a single building.
- LANs are inexpensive to install and also provide higher speeds.



Metropolitan area network (MAN)

- A MAN spans the distance of a typical metropolitan city.
- The cost of installation and operation is higher.
- MANs use high-speed connections such as fiber optics to achieve higher speeds



Wide area network (WAN)

- WANs span a larger area than a single city.
- These use long distance telecommunication networks for connection, thereby increasing the cost.
- The Internet is a good example of a WAN.

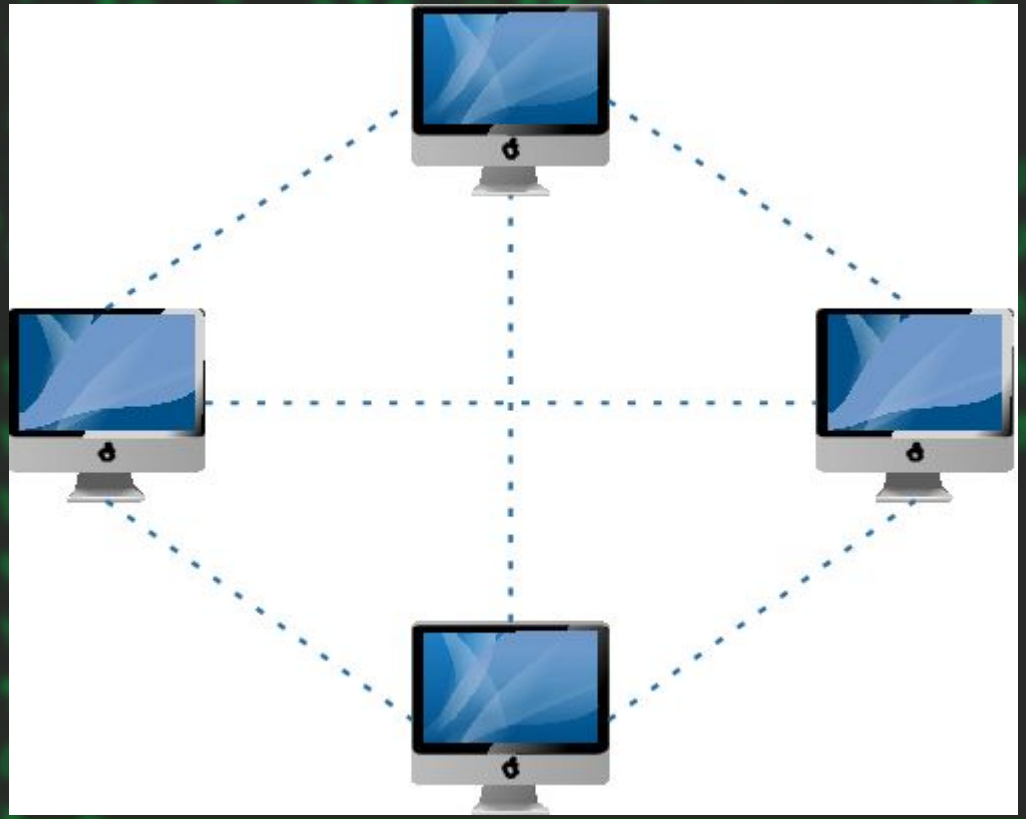
Classification by Component Roles

- Networks can also be classified according to the roles that the networked computers play in the network's operation.
- Peer-to-peer, server-based, and client-based are the types of roles into which networks are classified.

Peer-to-peer

- In a peer-to-peer network, all computers are considered equal.
- Each computer controls its own information and is capable of functioning as either a client or a server depending upon the requirement.
- Peer-to-peer networks are cheap and easy to install.
- They are popular as home networks and for use in small companies.
- Most operating systems come with built-in peer-to-peer networking capability.
- The maximum number of peers that can operate on a peer-to-peer network is **ten**.
- Each peer shares resources and allows others open access to them.

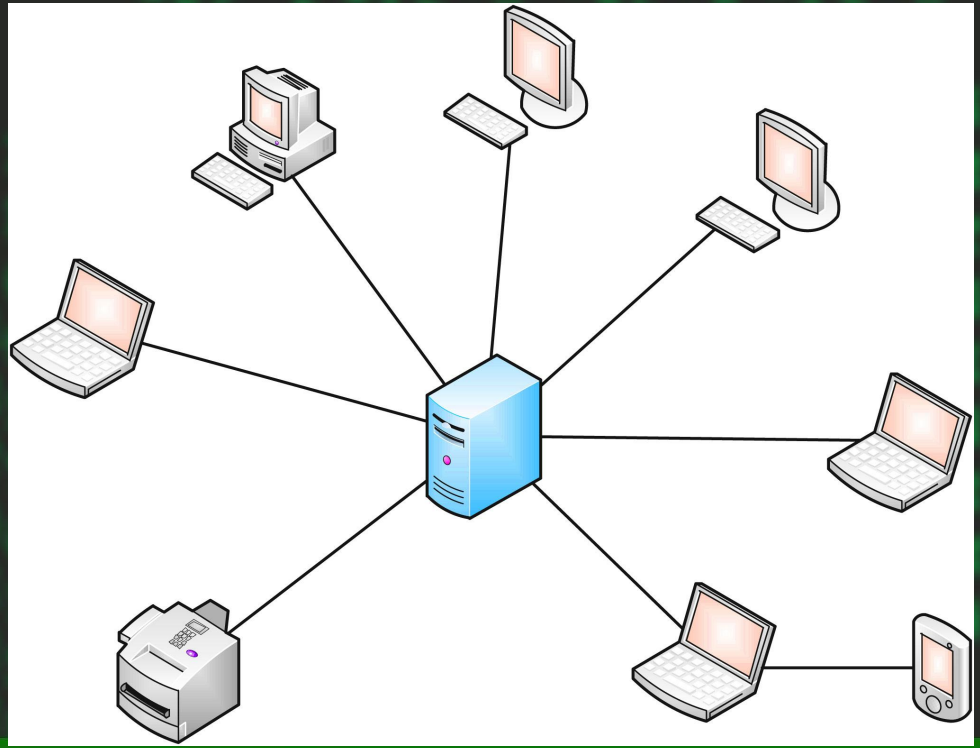
Peer-to-peer



Server based

- A server-based network offers centralized control and is designed for secure operations.
- In a server-based network, a dedicated server controls the network.
- A dedicated server is one that services the network by storing data, applications, resources, and also provides access to resources required by the client.

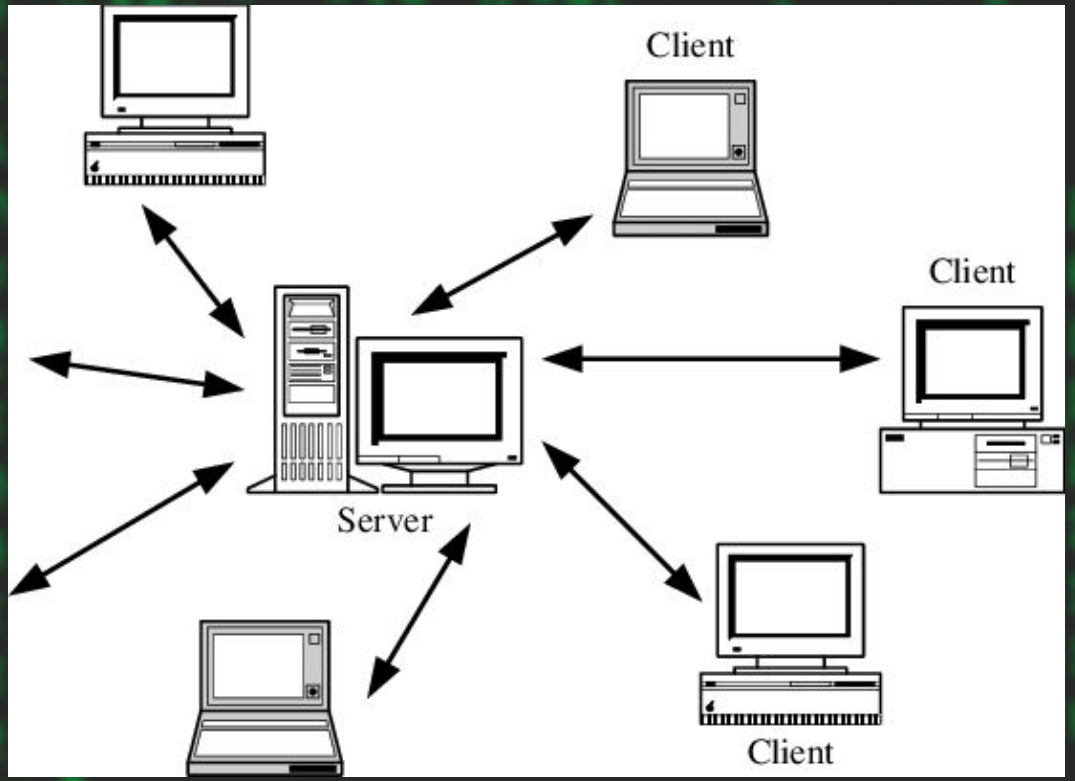
Server-based



Client-based

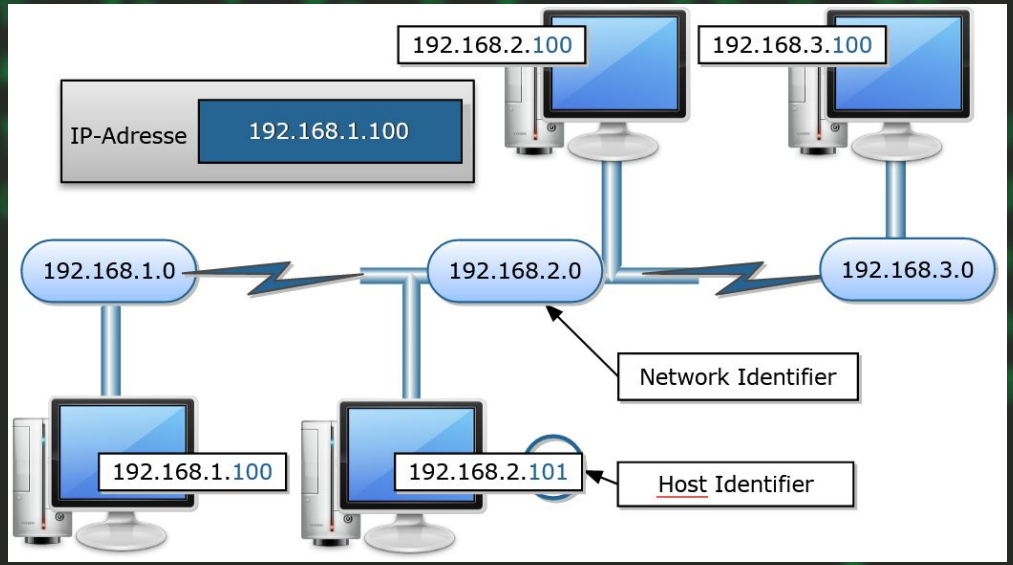
- Client-based network servers process requests from clients and return just the results.
- These networks take advantage of the powerful processing capabilities of both the client and the server.

client-based



IP /Internet Protocol/ address

- IP (Internet Protocol) is a Network Layer Protocol.
- A way to identify machines on a network
- A unique identifier



USAGE of IP's

- Used to connect to another computer or network.
- Allows transfers of files and e-mail
- Identify a device

IP types

- Based On IP versions
  - IPv4
  - IPv6

IPv4 (Internet protocol version 4)

- An IPv4 address is a 32-bit sequence of 1s and 0s.
- To make the IP address **easier to use**, the address is usually written as four decimal numbers separated by periods.
- This way of writing the address is called the dotted decimal format.
- IP generated by DHCP or Manually

IP structure

- IP addresses consist of four sections

```
192.168.123.12
 1    2    3    4
```

- Each section is 8 bits long

```
192      . 168      . 123      . 12
00101110   10100111   11101111   00011100
```

- Each section can range from 0 to 255

Which on is valid ip address?

1. 192.127.32.2
2. 192.259.22.1
3. 10.1.1.1
4. 192,168,1,1

...

- When you connect to some network an IP address will be generated and given(automatically by DHCP or static way).
- Every IP address has two parts:
  - Network: to identify the network(የእናንተ,የጎረቤት)
  - Host: identify the user(ስልክ,PC)

- The first(1) host address is called GATEWAY ADDRESS.

Private and Public IP addresses.

- Any HOST have 2 different IP's
- Public IP:
  - is an ip address that is given to the host on the WAN network
- Private IP:
  - is ip that is given to the host on LAN network.
  - Internet and intranet?

...

- There are 5 classes of private IP address A B C D and E
- CLASS A: Governments
- CLASS B: medium Companies
- CLASS C: small companies
- CLASS D: MultiCasting(streaming)
- CLASS E: Future Use (IETF research)

CLASS A

- Have 24bit of space for HOSTS

10 .	3 .	2 .	1
00101110	10100111	11101111	00011100
Network	HOST	HOST	HOST

Address Class	High-Order Bits	First Octet Address Range	Number of Bits in the Network Address	Number of Networks	Number of Hosts per Network
Class A	0	0-127	8	126	16,777,216

CLASS B

- Have 16bit of space for HOSTS

```
172          .      30          .    21          .    1
00101110     10100111     11101111     00011100
Network      Network      HOST         HOST
```

Address Class	High-Order Bits	First Octet Address Range	Number of Bits in the Network Address	Number of Networks	Number of Hosts per Network
Class B	10	128-191	16	16,384	65,536

CLASS C

- Have 8bit of space for HOSTS and 24-bit of network

```
192          .    168          .   21           .   1
00101110     10100111     11101111     00011100
Network      Network      Network          HOST
```

Address Class	High-Order Bits	First Octet Address Range	Number of Bits in the Network Address	Number of Networks	Number of Hosts per Network
Class C	110	192-223	24	2,097,152	254

CLASS C

- It is Used on Our Home,school and Office Network.
- As we saw the host changes on the last 8 bit only so devices in same network have same starting numbers.

```
192.168.1.1
192.168.1.11
192.168.1.3
192.168.1.9
192.168.1.32
```

Reserved IP Addresses

- Certain host addresses are reserved and cannot be assigned to devices on a network.
  a. Addresses beginning 127 are reserved for loopback and internal testing
  b. An IP address that has binary 0s in all host bit positions is reserved for the network address.
  c. An IP address that has binary 1 or 255s in all host bit positions is reserved for the broadcast address

Examples of Reserved addresses

- 0.0.0.0
- 127.0.0.0
- 128.0.0.0
- 191.255.0.0
- 192.0.0.0
- 223.255.255.0

IPv6 (Internet Protocol Version 6)

- IPv6 is a 128-bit alphanumeric long value that identifies an endpoint devices in IPv6 network.
- **Format of an IPv6 address:**
  - FE80:CD00:0000:0CDE:1257:0000:211E:729C
    - ALPHANumeric
    - Separated by colon(:)
    - IP generated automatically.
- The main difference is the IP-space(host holding) IPv4 holds 32-bit ip address but IPv6 holds 128-bit ip Addresses.

Myth and truth

- WHY do we need IPv6?
- ISP and IP’s
- DO Peoples Hack with IP address?

To know your computer ip address

On windows:

-

```
C:\Windows\system32\cmd.exe
   Connection-specific DNS Suffix  . :

Unknown adapter Local Area Connection 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.1.3
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Nathan Hailu>_
```

ipconfig

...

On Linux

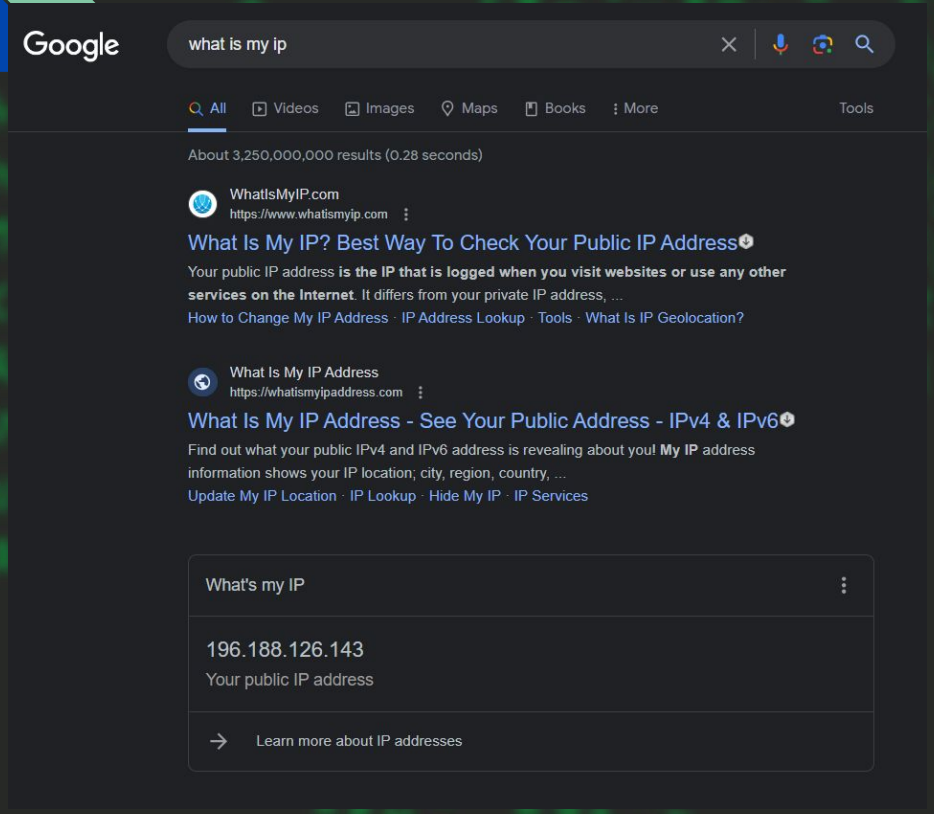
- ifconfig

```
rexder@HunterMachine ~/test> ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1420
        inet 172.17.99.42  netmask 255.255.240.0  broadcast 172.17.111.255
        inet6 fe80::215:5dff:fe65:929d  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:65:92:9d  txqueuelen 1000  (Ethernet)
        RX packets 1788  bytes 320789 (320.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23  bytes 1714 (1.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
┌──(rexder㉿HunterDragon)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:50:a1:51 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 86135sec preferred_lft 86135sec
    inet6 fe80::a00:27ff:fe50:a151/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
    link/none
    inet 10.10.16.75/23 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 dead:beef:4::1049/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::4461:6f98:3677:83de/64 scope link stable-privacy proto kernel_ll
       valid_lft forever preferred_lft forever
```

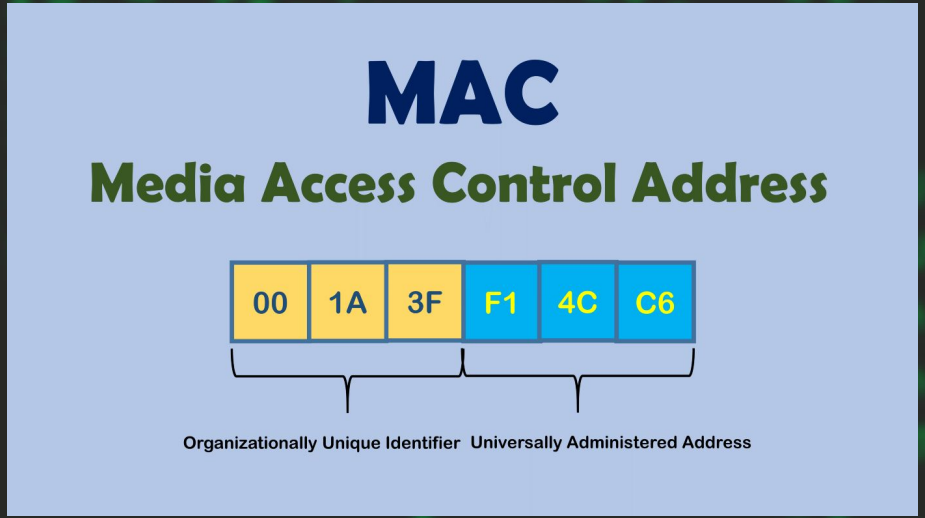
Public ip


Google
what is my ip
All
Videos
Images
Maps
Books
More
Tools
About 3,250,000,000 results (0.28 seconds)
WhatIsMyIP.com
https://www.whatismyip.com
What Is My IP? Best Way To Check Your Public IP Address
Your public IP address is the IP that is logged when you visit websites or use any other services on the Internet. It differs from your private IP address, ...
How to Change My IP Address · IP Address Lookup · Tools · What Is IP Geolocation?
What Is My IP Address
https://whatismyipaddress.com
What Is My IP Address - See Your Public Address - IPv4 & IPv6
Find out what your public IPv4 and IPv6 address is revealing about you! My IP address information shows your IP location; city, region, country, ...
Update My IP Location · IP Lookup · Hide My IP · IP Services
What's my IP
196.188.126.143
Your public IP address
Learn more about IP addresses


(rexder㉿HunterDragon)-[~]
$ curl ifconfig.me
196.188.126.143

MAC(Media Access Control) Address

- It is Given by A manufacturer of that network adapter.
- Network adapter is a hardware device that helps us to have connection (our wifi adapter or our ethernet port)
- It is Alphanumeric, with 2 part
  - Organizational Unique Id
  - Universally Administered Address



MAC(Media Access Control) Address

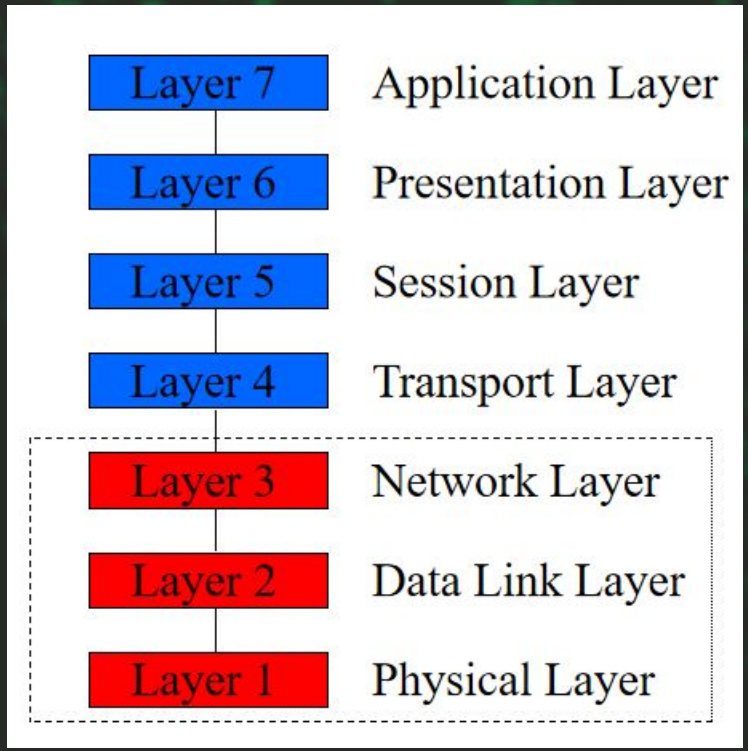
- Flat name space of 48 bits
  - Typically written in six octets in hex
  - E.g., 00-15-C5-49-04-A9 for my Ethernet
- Organizationally unique identifier
  - Assigned by IEEE Registration Authority
  - Determines the first 24 bits of the address
  - E.g., 00-15-C5 corresponds to “Dell Inc”
- Remainder of the MAC address
  - Allocated by the manufacturer
  - E.g., 49-04-A9 for my Ethernet card

OSI(Open Systems Interconnection) Reference model

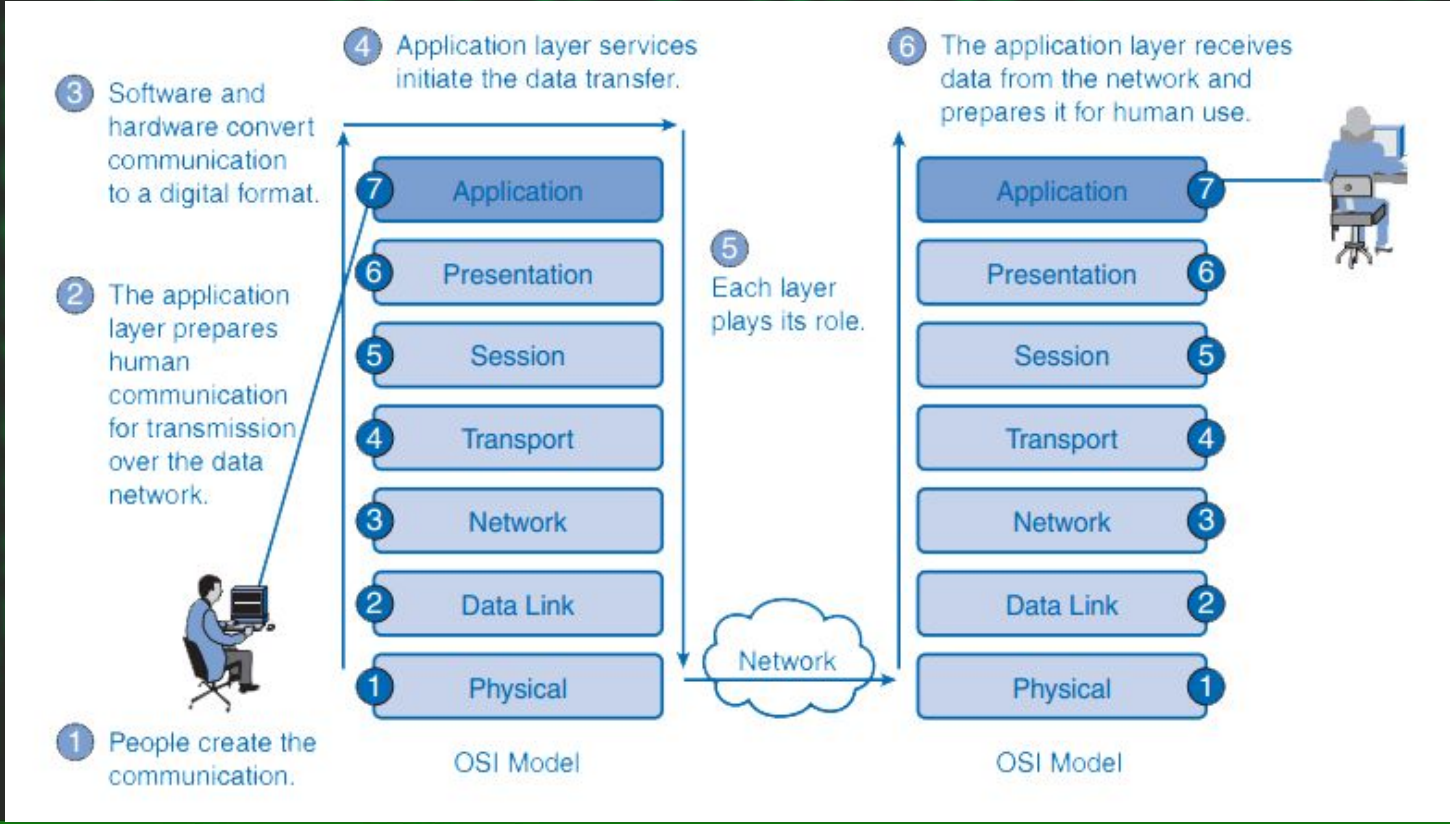
- Back in Days, Different Company Devices can't Communicate or create network
- OSI Reference Model - internationally standardised network architecture.
- Specified in ISO 7498.
- It is an idea model to show the way of network work
- Model has 7 layers.
- It shows How Data transfers between 2 hosts/servers

...

- Layers 1-4 relate to communications technology.
- Layers 5-7 relate to user applications.
- The sequence differ when sender and receiver use it

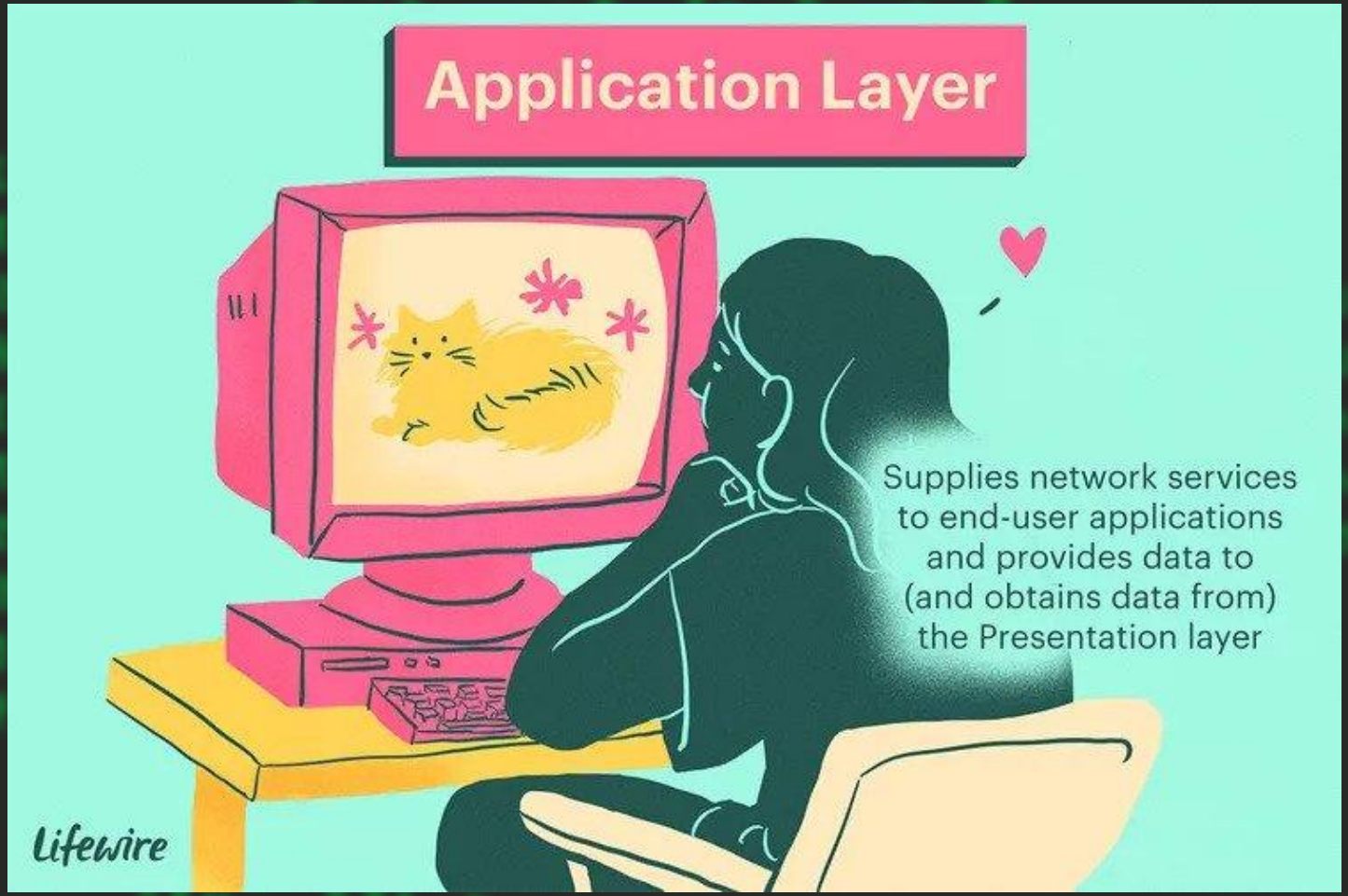


The way data transfer



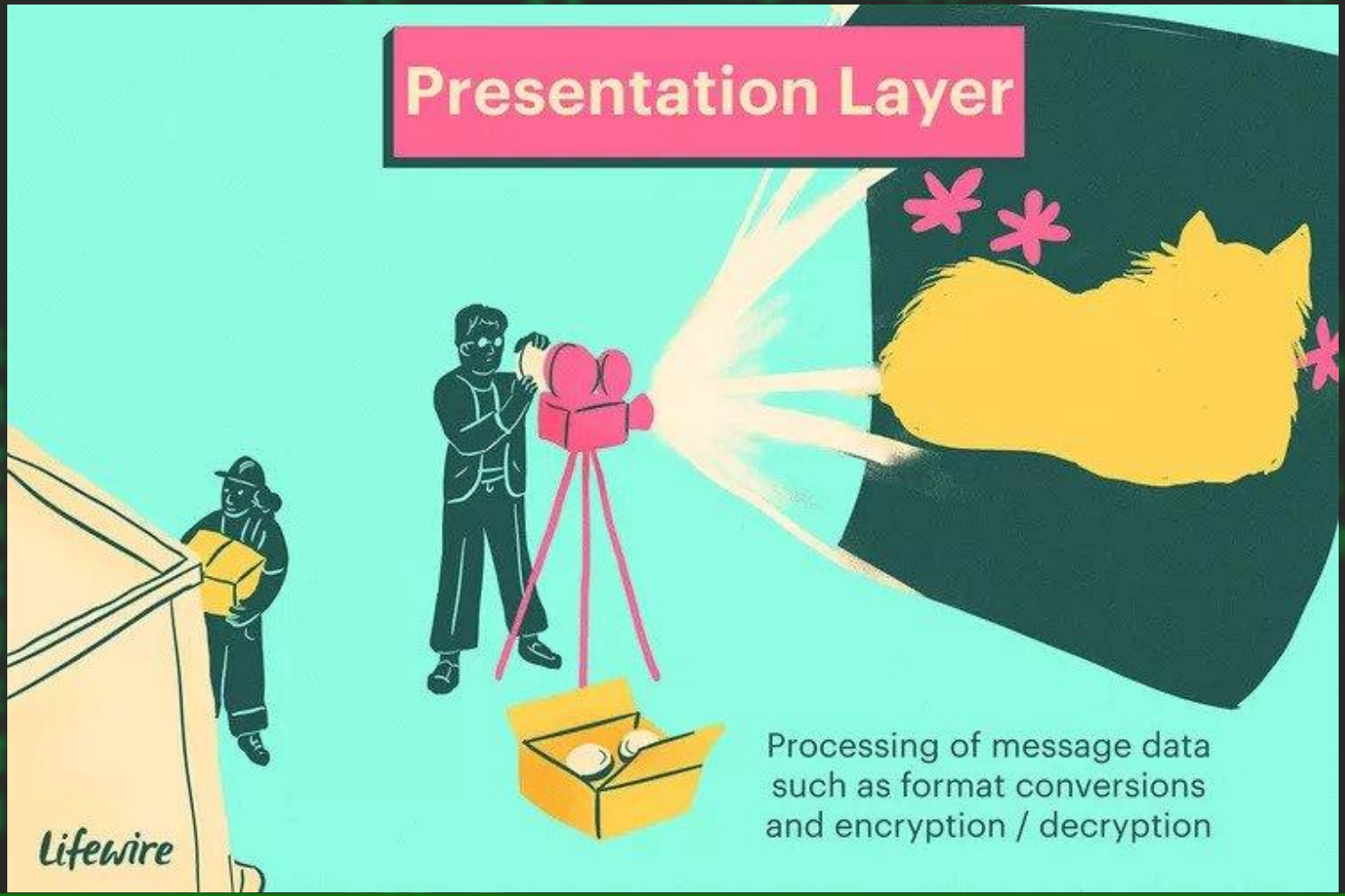
Layer 7: Application Layer

- Level at which applications access network services.
  - Represents services that directly support software applications for file transfers, database access, and electronic mail, BROWSERS etc.
- Your data is DATA
  - PROTOCOLS: HTTP,FTP,SMTP


Application Layer
Supplies network services to end-user applications and provides data to (and obtains data from) the Presentation layer
Lifewire

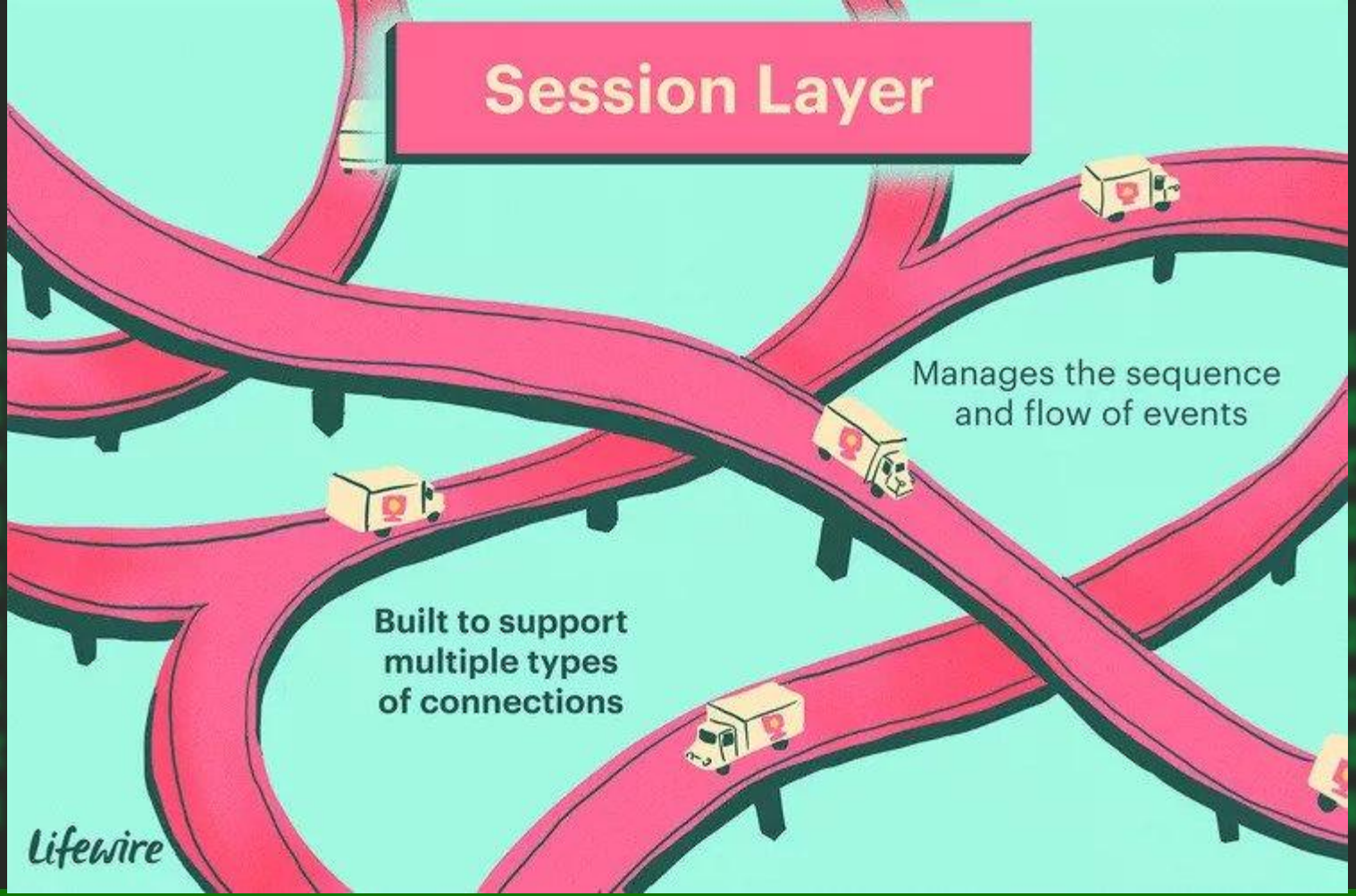
Layer 6: Presentation Layer

- Related to representation of transmitted data
  - Translates different data representations from the Application layer into uniform standard format
- Providing services for secure efficient data transmission
  - e.g. data encryption, and data compression.
- Your data is DATA
- PROTOCOLS: SSL


Presentation Layer
Processing of message data such as format conversions and encryption / decryption
Lifewire

Layer 5: Session Layer

- Allows two applications on different computers to establish, use, and end a session.
  - e.g. file transfer, remote login
- Establishes dialog control
  - Regulates which side transmits, plus when and how long it transmits.
- Performs token management and synchronization.
- Your data is DATA
- PROTOCOLS: RPC,NETBIOS


Session Layer
Manages the sequence and flow of events
Built to support multiple types of connections
Lifewire

Layer 4: Transport Layer

- Manages transmission packets
  - Repackages long messages when necessary into small packets for transmission [sender]
  - Reassembles packets in correct order to get the original message. [receiver]
- Handles error recognition and recovery.
  - Transport layer at receiving acknowledges packet delivery.
  - Resends missing packets
- Your data is SEGMENTS
- PROTOCOLS: TCP,UDP

Transport Layer

Delivers data across network connections like TCP

Different transport protocols may support a range of optional capabilities including:

Error recovery

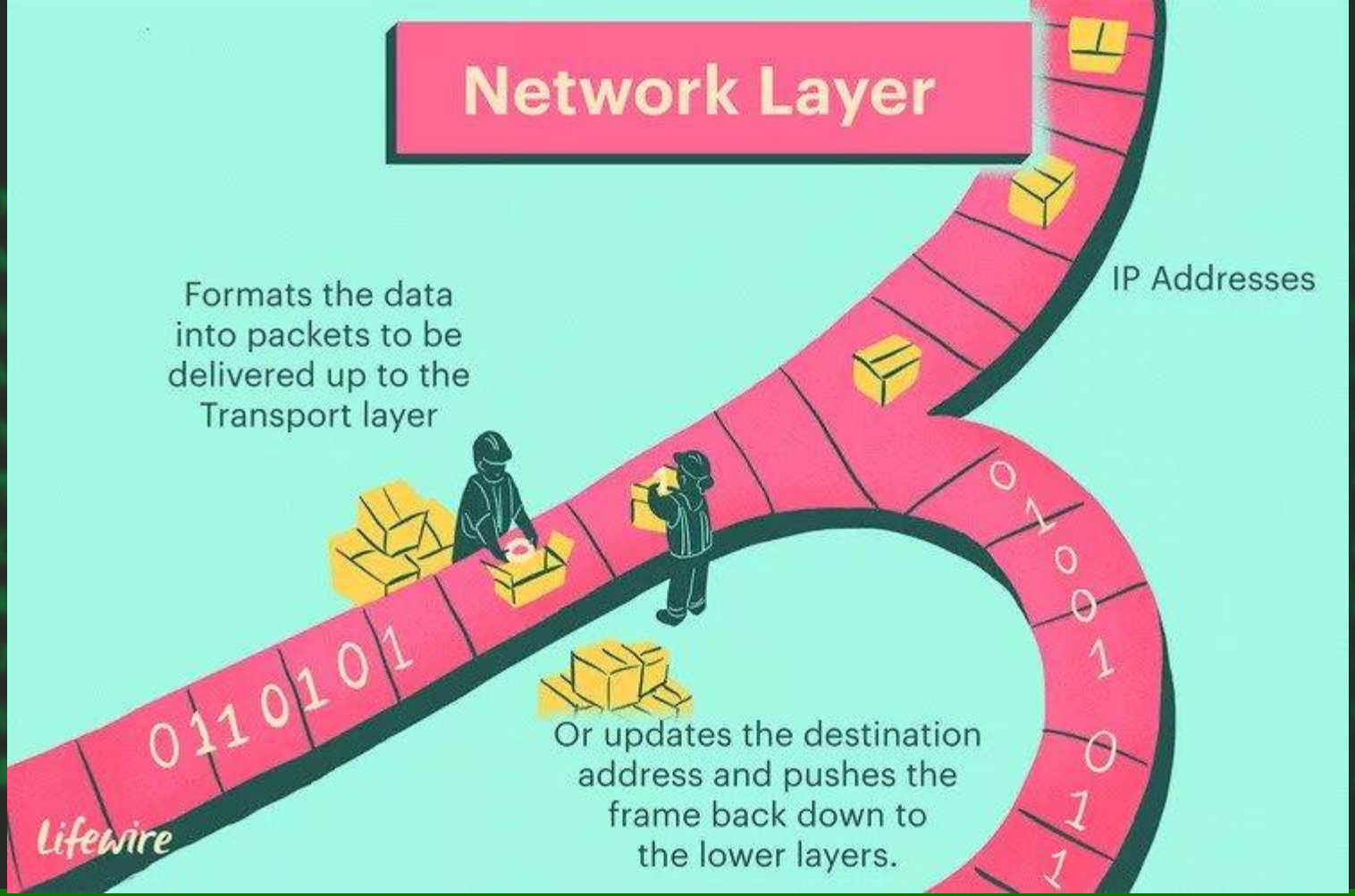
Flow Control

Support for re-transmission

Lifewire

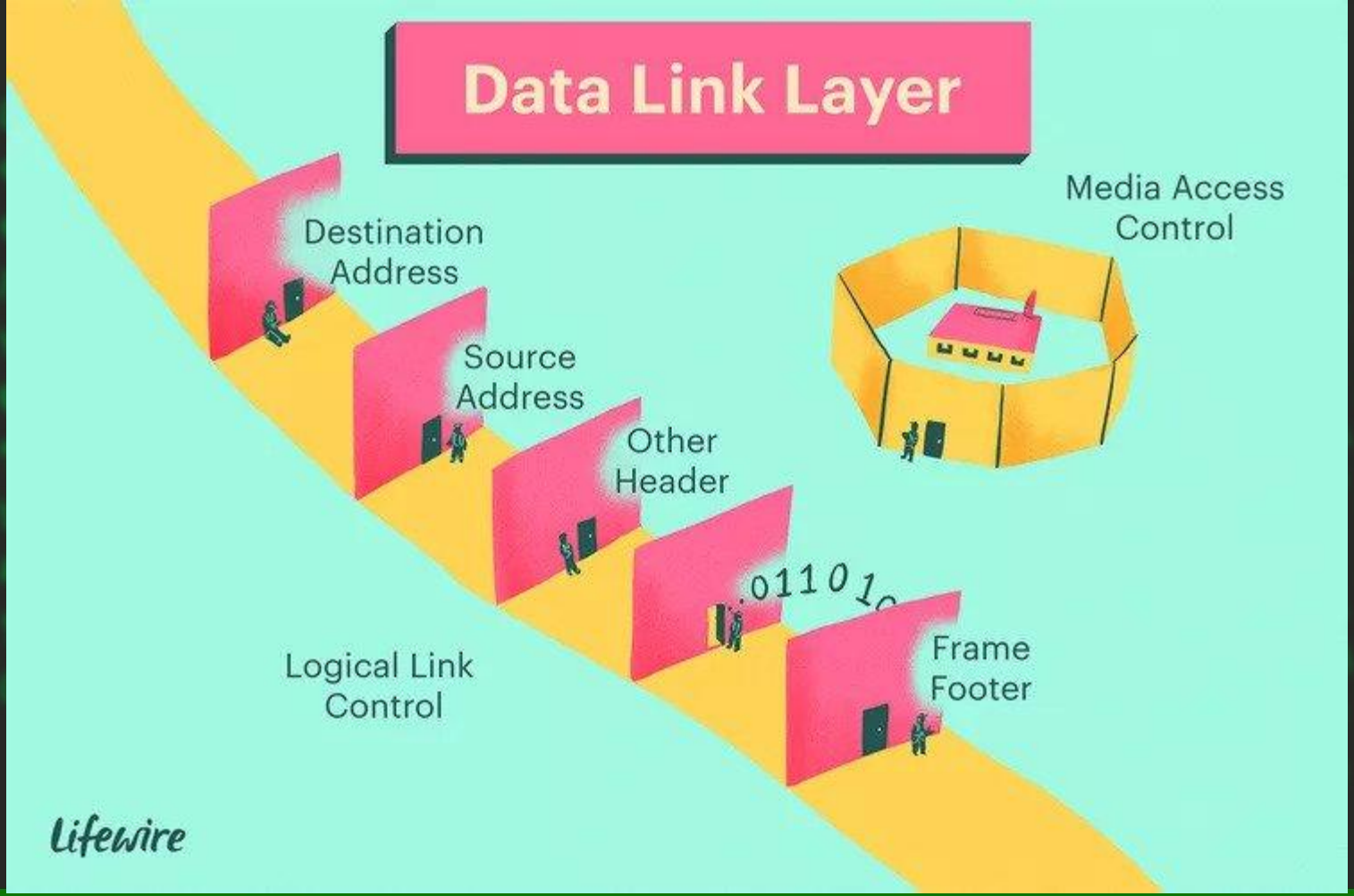
Layer 3: Network Layer

- Manages addressing/routing of data within the ip range
  - Addresses messages and translates logical addresses and names into physical addresses.
  - Determines the route from the source to the destination computer
  - Manages traffic problems, such as switching, routing, and controlling the congestion of data packets.
- Your data is PACKETS
- PROTOCOLS: ICMP,ARP,NAT,IP


Network Layer
Formats the data into packets to be delivered up to the Transport layer
IP Addresses
0110101
Or updates the destination address and pushes the frame back down to the lower layers.
Lifewire

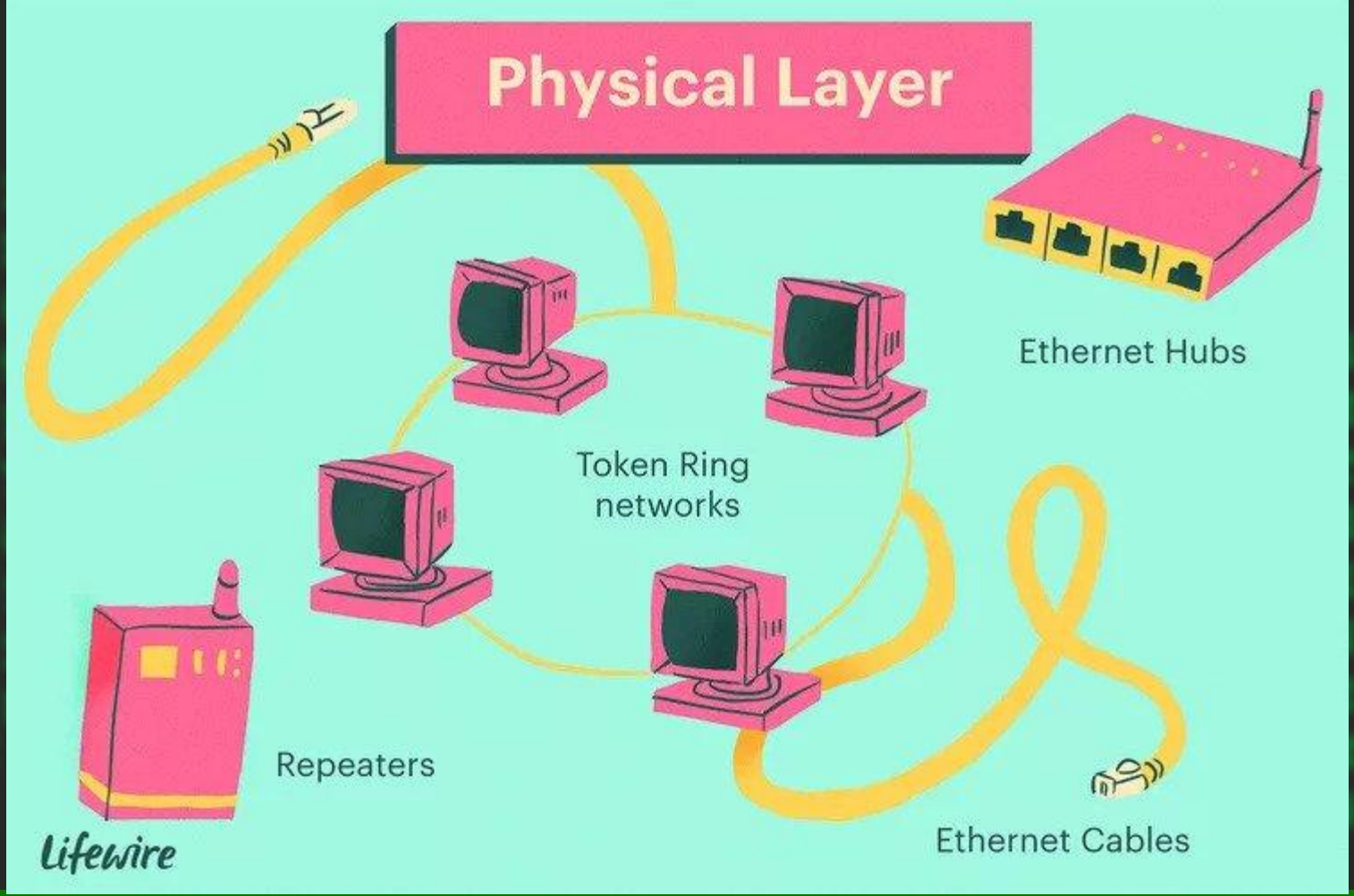
Layer 2: Data Link Layer

- Packages raw bits from the Physical layer into frames (logical, structured packets for data). [receiver]
- Provides reliable transmission of frames
  - It waits for an acknowledgment from the receiving computer.
  - Retransmits frames for which acknowledgement not received
- Your data is FRAMES
- PROTOCOLS: PPP,NDP,CDP

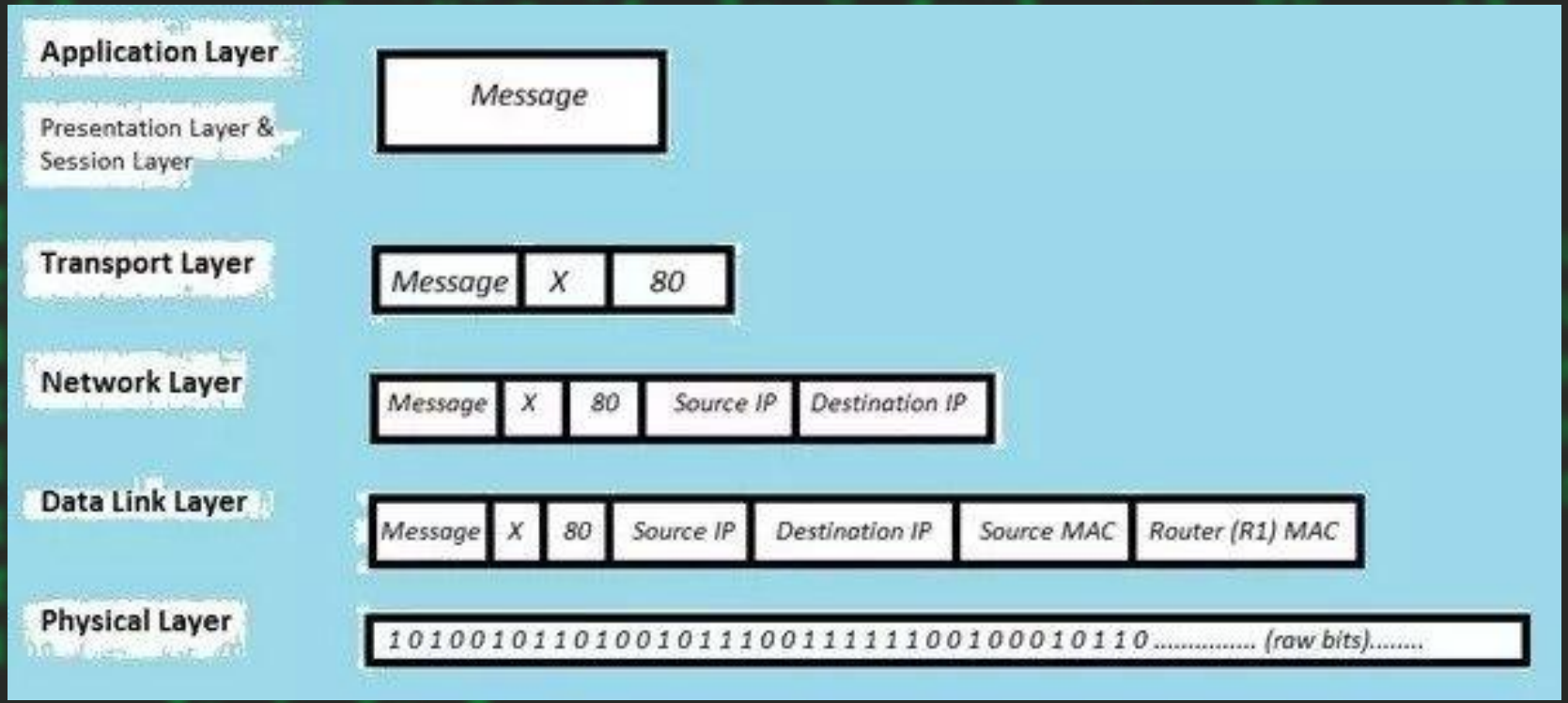

Data Link Layer
Destination Address
Source Address
Other Header
Logical Link Control
Media Access Control
Frame Footer
Lifewire

Layer 1: Physical Layer

- Transmits bits from one computer to another
- Regulates the transmission of a stream of bits over a physical medium.
- Defines how the cable is attached to the network adapter and what transmission technique is used to send data over the cable. Deals with issues like
  - The definition of 0 and 1, e.g. how many volts represents a 1, and how long a bit lasts?
  - How many pins a connector has, and what the function of each pin is?
- Your data is Bits
- PROTOCOLS/DEVICES: RS-449


Physical Layer
Ethernet Hubs
Token Ring
networks
Repeaters
Ethernet Cables
Lifewire

Summary


Application Layer
Presentation Layer & Session Layer
Message
Transport Layer
Message
X
80
Network Layer
Message
X
80
Source IP
Destination IP
Data Link Layer
Message
X
80
Source IP
Destination IP
Source MAC
Router (R1) MAC
Physical Layer
1010010110100101110011111100100010110 ..... (raw bits).....

TCP and UDP

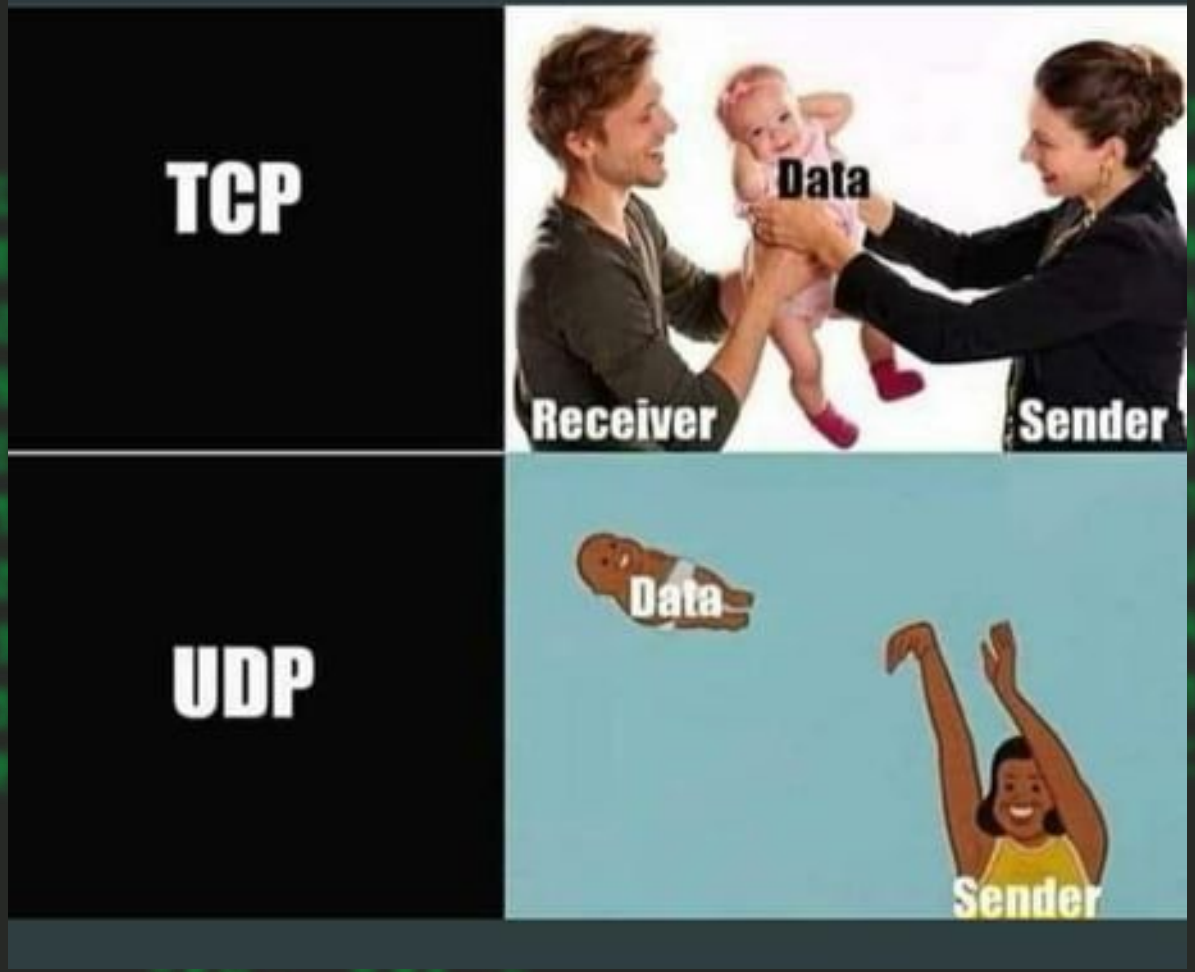
What Is TCP (Transmission Control Protocol)?

- Reliable
- Connection-Oriented protocol
  - Means it establishes a connection between the receiver and sender.
    - It uses 3 way HandShake (more on Network Hacking)
- Used on emails, Chat,watching online videos, simple browsing.

...

What is UDP(User Datagram Protocol)?

- Connectionless
- less reliable, but faster and more straightforward.
- It’s often used in situations where higher speeds are crucial, like in streaming or gaming.

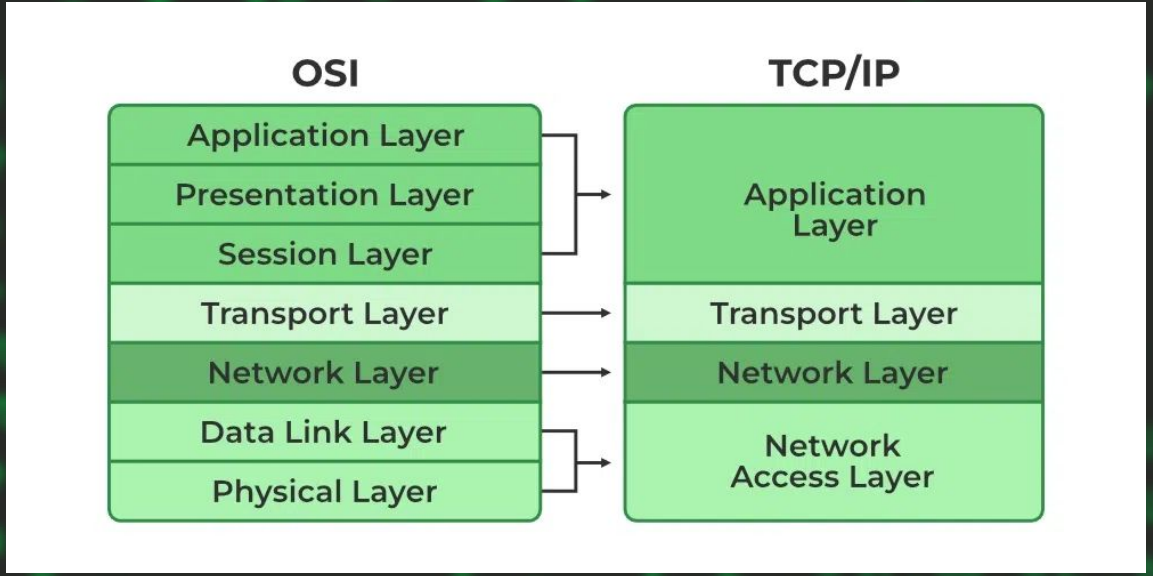

TCP
Data
Receiver
Sender
UDP
Data
Sender

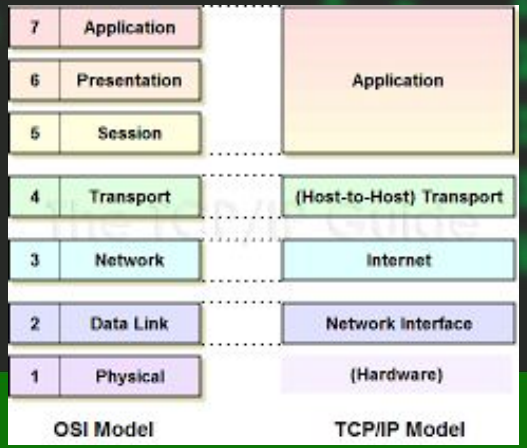
TCP/IP model

- It is A reference model like the OSI model
- TCP/IP is the new and most used Model at this time.
- This model have 4 layers(used to be 5 layer)

...

- Application,Presentation and session layers are combined together and called APPLICATION
- Data link layer and physical layer combined and called network access layer.

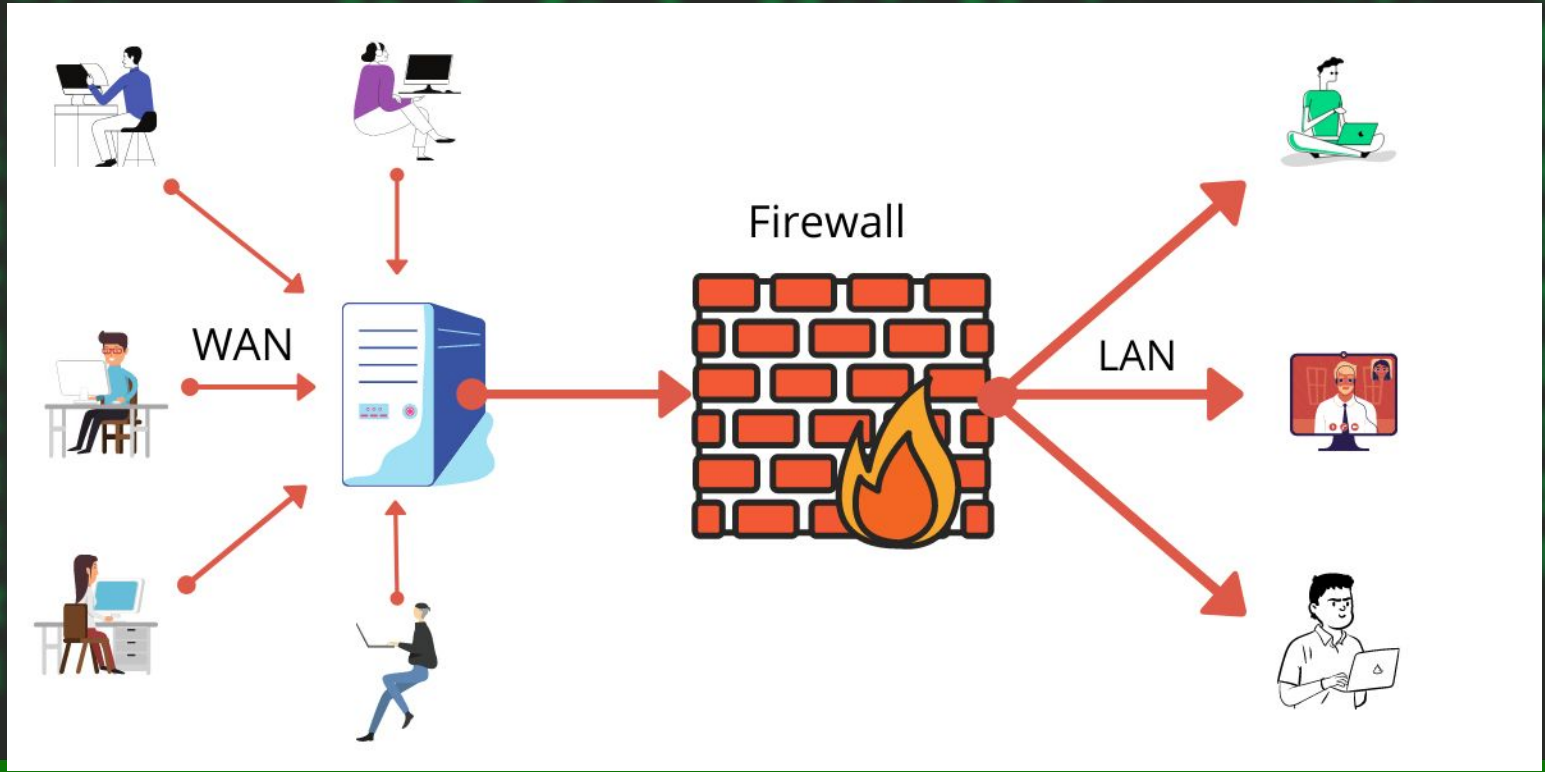




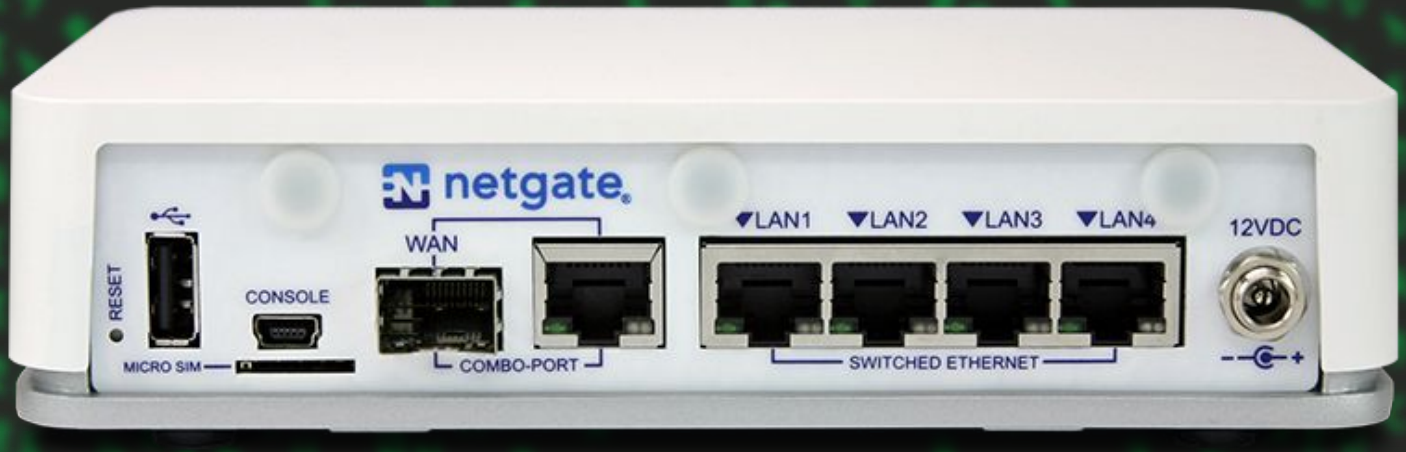
Firewall

- A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
- It is Just A collection of rules to allow and deny network traffics
- Ex: You can’t directly access some host directly from other Network.

Firewall



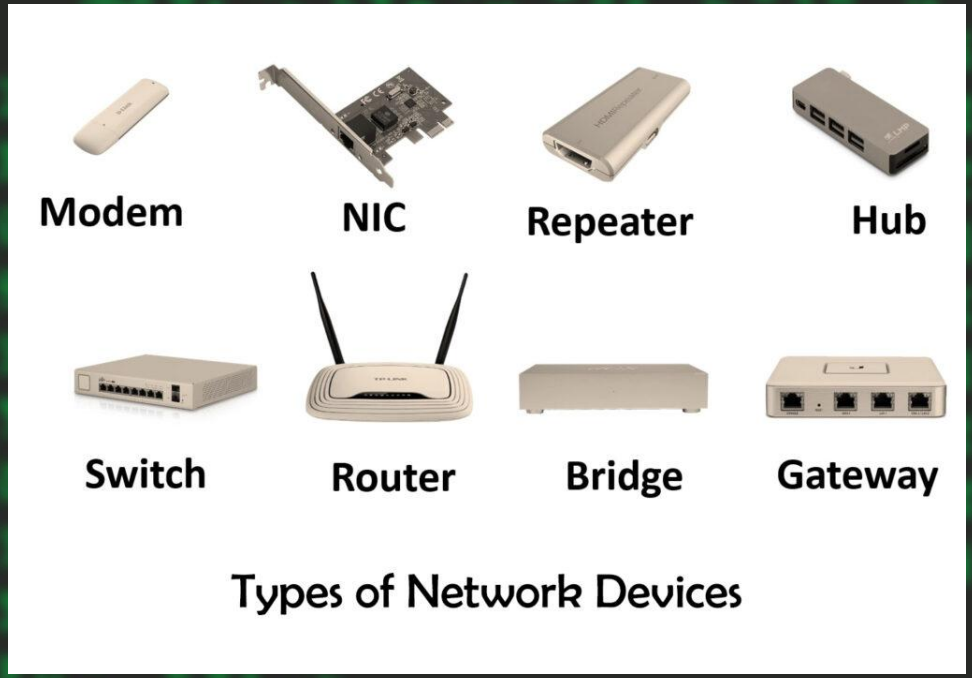
Firewall hardwares



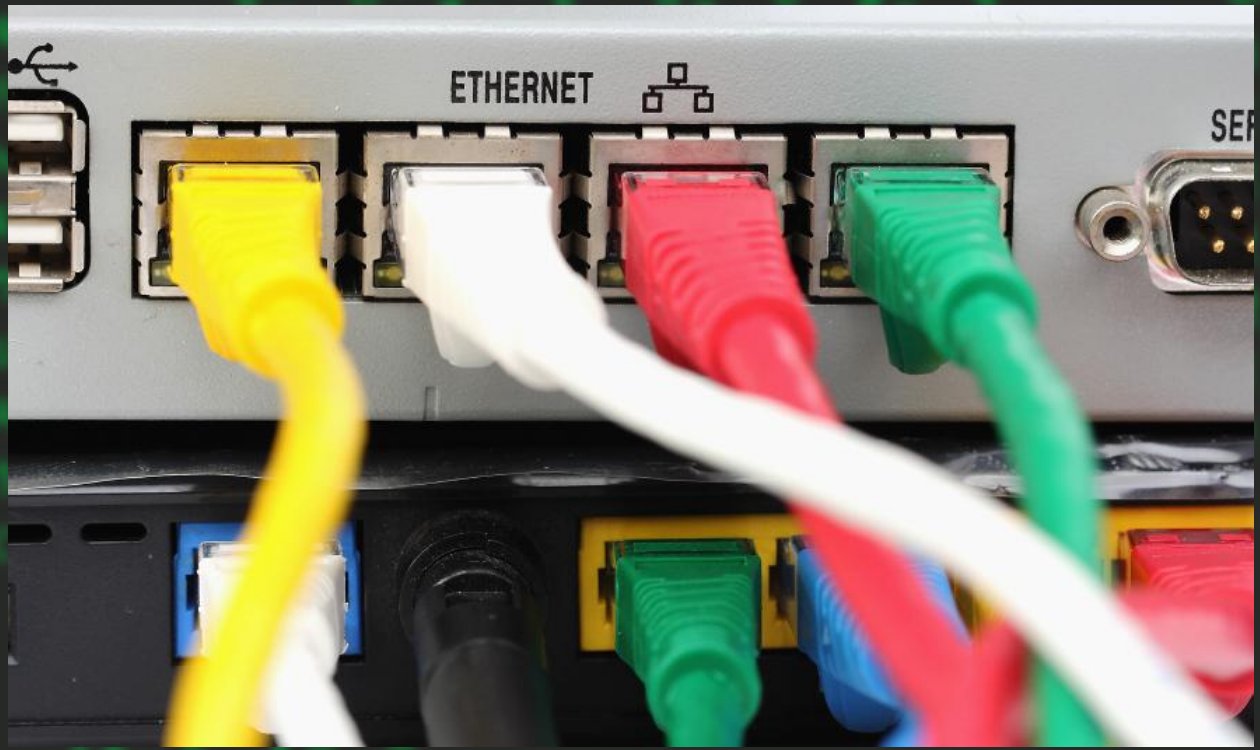
But every OS have firewall Built-in

Networking tools

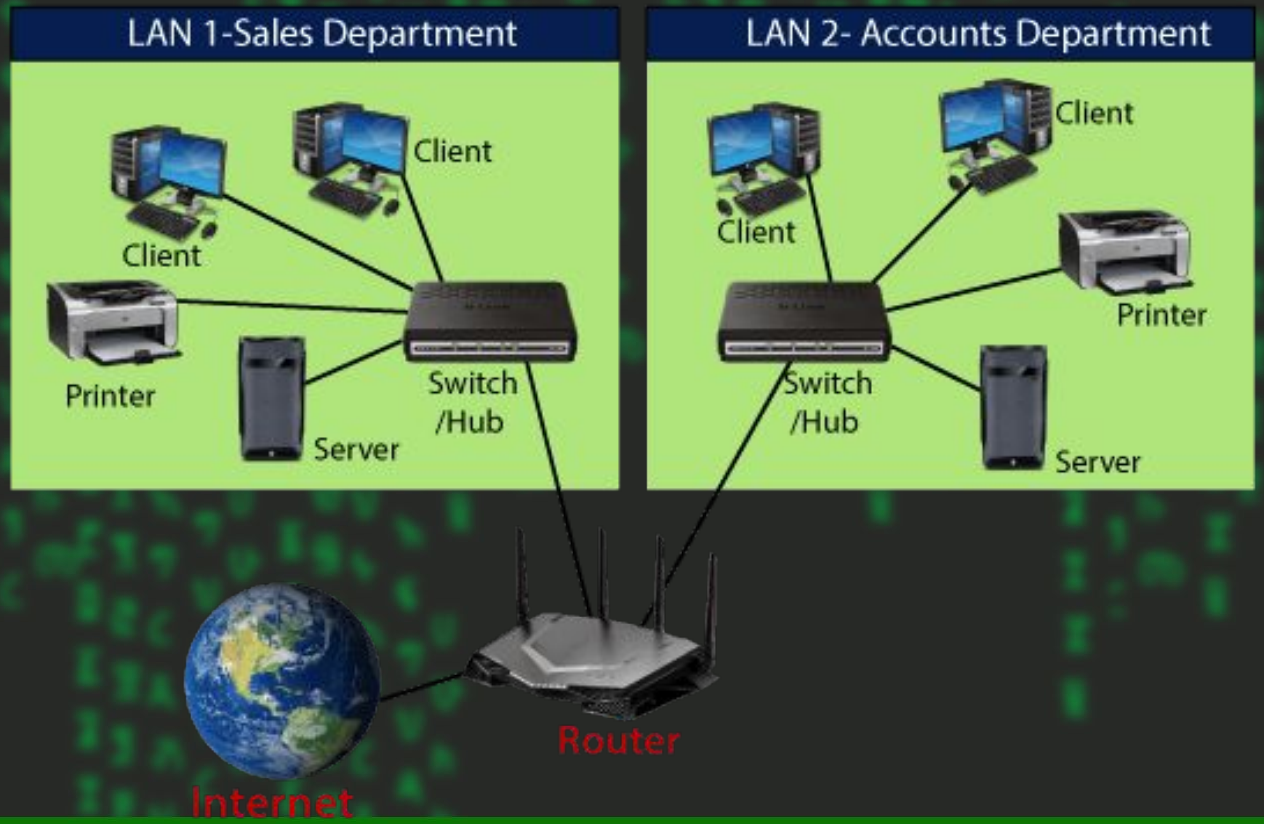
ON Networking there are many hardware devices.



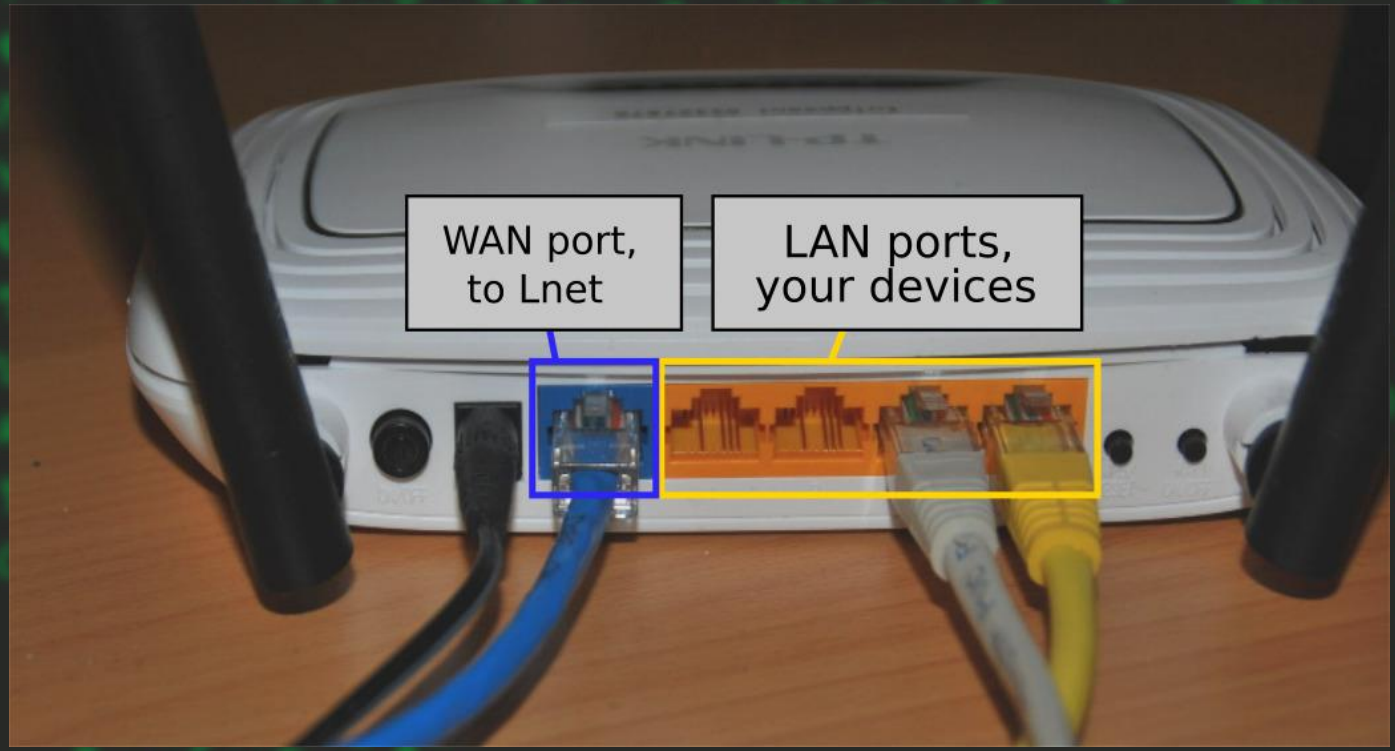
The switches



Switches/Hub and Routers



Modern wifi routers



Repeater

- Helps To boost/amplify the speed of the internet, in long route

Bridge

Used to Connect different LANs

Assignment) 5pts

Video: https://www.youtube.com/watch?v=qulRjRFavJI

Questions

1. Submit the decimal representation of the subnet mask from the following CIDR: 10.200.20.0/27 (2pts)
2. Submit the broadcast address of the following CIDR: 10.200.20.0/27 (2pts)
3. Split the network 10.200.20.0/27 into 4 subnets and submit the network address of the 3rd subnet as the answer. (3pts)
4. Split the network 10.200.20.0/27 into 4 subnets and submit the broadcast address of the 2nd subnet as the answer. (3pts)

Will be posted on the google form , bedenb Google argachu sirut, you have 15 days. you will learn lot of things about subnetting, CIDR notations..., your season 2 exam will include some part from it.

CLASS IS OVER

1) Do note
2) Read it again
3) ASK
4) Prepare Your Kali linux/Parrot machine

You have 1 week break and exam when you come back(next week saturday(20pts), also finish payment.