How the Web Works

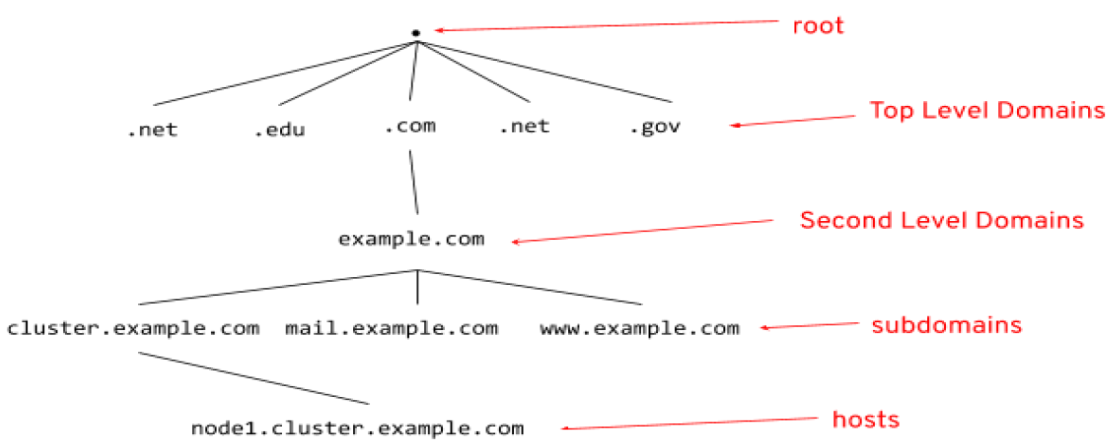
DNS in detail

DNS (Domain Name System) (port 53):

- When a client sends a request to the server **DNS translates domain names to their equivalent IP addresses**
- It is **called the phonebook of the internet**
- DNS is an **Application-layer protocol.**
- For example, www.amazon.com to 192.0. 2.85.

Subdomain:

- A subdomain name is a **piece of additional information added to the beginning of a website's domain name.**
- The **main domain and the subdomain act as two different websites**
- This **allows organizations to create a different website for different functionality which is in line with the main domain name**
- It allows websites to separate and organize content for a specific function
- **Example. mail.google.com, maps.google.com**



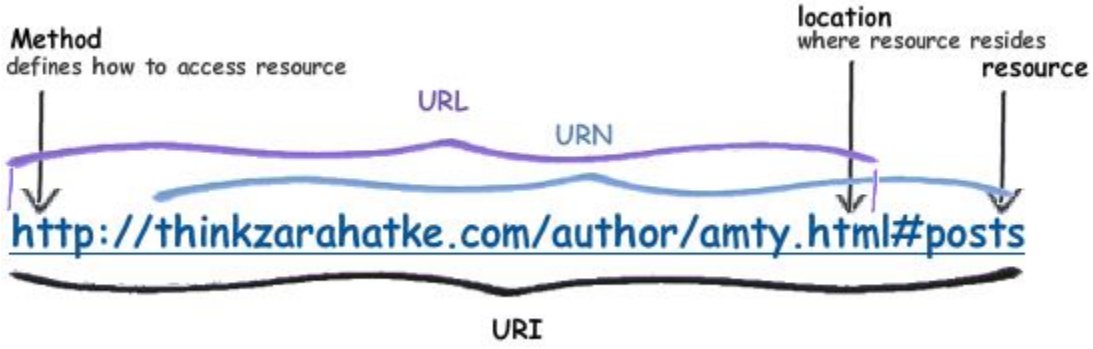
HTTP in detail

HTTP (HyperText Transfer Protocol) (Port: 80)

1. HTTP protocol is the set of rules used for communicating with web servers
2. HTTP is the **protocol used for communication, between web servers and clients, allowing for the transfer of data such as HTML, images, and videos.**
3. **The communication between the client and web server is done in clear text**
4. HTTP is an **application layer protocol**

HTTPS (HyperText Transfer Protocol Secure) (Port: 443)

1. HTTPS is the **secure version of HTTP.**
2. HTTPS **uses TLS (SSL) to encrypt normal HTTP requests and responses** (TLS is an updated, more secure version of SSL.)
3. TLS(SSL) **encrypts data sent between a client and a Server** or (between two servers)
4. **Prevents MIM attack (Man in the Middle attack)**



URI (Uniform Resource Identifier):

It used to identify a resource on the internet either by location or a name or both
URI is a superset of URL & URN

URL(Uniform Resource Locator):

- URL is **used to locate resources on the Internet**
- URL is an i**nstruction on how to access a resource on the internet.**
- URL is **used to make requests to the web server based on the request web server will provide the response**
- It identifies the resource by Location

URN (Uniform Resource Name):

- It identifies the resource by name

HTTP Headers:

- Headers are add**itional bits of data or context that the client and server send with an HTTP request or response.**
- Headers are like metadata

Example Request:

```
GET / HTTP/1.1
Host: tryhackme.com
User-Agent: Mozilla/5.0 Firefox/87.0
Referer: https://tryhackme.com/
//blank line to inform the web server that the request has finished.
```

Example Response:

```
HTTP/1.1 200 OK
Server: nginx/1.15.8
Date: Fri, 09 Apr 2021 13:34:03 GMT
Content-Type: text/html
Content-Length: 98
```

```
<html>
<head>
  <title>TryHackMe</title>
</head>
<body>
   Welcome To TryHackMe.com
</body>
</html>
```

Common Request Headers

These are headers that are sent from the client (usually your browser) to the server.

Host: Some web servers host multiple websites so by providing the host headers you can tell it which one you require, otherwise you'll just receive the default website for the server.

User-Agent: This is your browser software and version number, telling the web server your browser software helps it format the website properly for your browser and also some elements of HTML, JavaScript and CSS are only available in certain browsers.

Content-Length: When sending data to a web server such as in a form, the content length tells the web server how much data to expect in the web request. This way the server can ensure it isn't missing any data.

Accept-Encoding: Tells the web server what types of compression methods the browser supports so the data can be made smaller for transmitting over the internet.

Cookie: Data sent to the server to help remember your information (see cookies task for more information).

Common Response Headers

These are the headers that are returned to the client from the server after a request.

Every response has a **Response Code**

1. 200s: Successes
2. 300s: Redirects
3. 400s: Client Error (Failed access)
4. 500s: Server Error

Set-Cookie: Information to store which gets sent back to the web server on each request (see cookies task for more information).

Cache-Control: How long to store the content of the response in the browser's cache before it requests it again

Content-Type: This tells the client what type of data is being returned, i.e., HTML, CSS, JavaScript, Images, PDF, Video, etc. Using the content-type header the browser then knows how to process the data.

Content-Encoding: What method has been used to compress the data to make it smaller when sending it over the internet.

HTTP Methods:

HTTP Method **defines what action the client wants to perform whenever it is sending a HTTP request to the server**
client uses HTTP methods to show **what action the client wants to perform while sending a request to the web server**

GET Request: This is used for getting information from a web server.

POST Request: This is used for submitting data to the web server and potentially creating new records

PUT Request: This is used for submitting data to a web server to update information

DELETE Request: This is used for deleting information/records from a web server.

HTTP Status Code:

HTTP Status Code indicates the outcome of the request sent by the client

100-199 - Information Response	These are sent to tell the client the first part of their request has been accepted and they should continue sending the rest of their request. These codes are no longer very common.
200-299 - Success	This range of status codes is used to tell the client their request was successful.
300-399 - Redirection	These are used to redirect the client's request to another resource. This can be either to a different webpage or a different website altogether.
400-499 - Client Errors	Used to inform the client that there was an error with their request. (Client side error)
500-599 - Server Errors	This is reserved for errors happening on the server side and usually indicates quite a major problem with the server handling the request. (Server-side error)

Cookies:

1. A cookie is **a small piece of data that is stored in the browse that allows the web application to remember information about the client/user.**
2. when the browser requests a web page from the server. The server can send the webpage cookie which is stored on a computer's hard drive
3. **Cookies are saved when the client receives a "Set-Cookie" header in the response from the web server.**

Types of cookies:

Session cookies: Delete immediately after you close your browser. For example, these cookies keep items in an online shopping cart.

Persistent cookies: save data for some time but expire after a specific date. For example, these cookies allow websites to store username and password information for visitors.

Third-party cookies: collect data on online behavior and send it back to website owners who want to tailor ads to site visitors

Load Balancers:

The l**oad balancer will receive your request first and then forward it to one of the multiple servers behind it. The load balancer uses different algorithms to help it decide which server is best to deal with the request.** A couple of examples of these algorithms are **round-robin,** which **sends it to each server in turn**, or **weighted, which checks how many requests a server is currently dealing with and sends it to the least busy server.**

WAF (Web Application Firewall)

- A WAF **sits between your web request and the web server**
- It **protects the webserver from hacking or denial of service attacks.**
- **It analyses the web requests for common attack techniques, whether the request is from a real browser rather than a bot.**

- It also **checks if an excessive amount of web requests are being sent, If a request is deemed a potential attack, it will be dropped and never sent to the webserver.**
- **Example: Cloudflare**

Client:

1. **Anything that can make HTTP requests to the server**
2. Usually a web browser, also: netcat, cURL, wget
3. **Clients make HTTP requests**

Servers:

1. Refers to both machines and software
2. **A server is where the content of a web application or website is stored**
3. The server provides information to the **clients** (browser/user) which makes HTTP requests for the information
4. Web servers **provide** data over **Hyper Text Transfer Protocol (HTTP)**

Types of servers

There are many types of servers, which are as follows:

- Webserver
- Application server
- Blade server

- Cloud server
- Database server
- Dedicated server
- Print server
- Proxy server
- File server
- Mail server
- Standalone server
- Domain name service

Database:

A database is an **organized collection of structured information, or data, typically stored electronically in a computer system**. A database is usually **controlled by a database management system (DBMS).**

Session:

Typically, a session is started when a user authenticates their identity using a password or another authentication protocol.

Cache

It is a temporary storage of internet files stored by the client. It allows quick access to commonly requested sites. The content is stored on browser. Cache expires manually.

CIA:

Confidentiality

Integrity
Availability

- **Confidentiality** means only authorized persons can access the data
- **Integrity** means that the data sent is accurate, consistent, and not tampered with before reaching its destination.
- **Availability** means the data should be available whenever it is needed

Non-repudiation

It is a guarantee that the sender of a message can't later deny having sent the message and that the recipient can't deny having received the message. Digital signatures are used to ensure this.

Digital signature

It is a process to validate the authenticity and integrity of a message, software, or digital document.

Networking Fundamentals

Networking:

- Computer networking means the **interconnection of two or more devices that can share data and resources over physical or wireless connections**
- **It uses a set of rules, called protocols, to transmit information**

Internet:

- **The interconnection of multiple networks is called the internet**
- **The Internet is one giant network that consists of many, many small networks within itself.**
- **These small networks are called private networks, whereas networks connecting these small networks are called public networks -- or the Internet!**
- **A private network:** (your home network where all the devices are connected to your home network by Private IP)
- **A public network:** (Public network **connects the private network to other networks or the internet by public IP Address which is provided by ISP)**

In a network, every device has Its own private IP but while communicating outside of the network every device uses the same IP called Public IP

Every device on the network or internet identifies itself by IP Address

The generic term node or host refers to any device on a network

Client is browser

Local-area network (LAN) (Intranet):

A network that connects computers within a limited area such as a residence, school, laboratory, university campus or office

Metropolitan-area network (MAN) (ISP):

A network that connects two or more local-area networks(LAN) over a potentially large geographic area like towns, cities, etc.

Wide-area network (WAN) (Internet):

A WAN is a network that connects multiple LANs and MANs over long distances areas like countries, or even continents.

IP Addresses:

- An IP address is a **unique address that identifies a device on the internet or a local network.** IP stands for "Internet Protocol". These protocols are a set of rules that force many devices to communicate in the same language,
- **It is also called logical addressing**
- IP address is Layer 3 Protocols (Network Layer) (router)

1. Private IP Address:

- A private IP address is **used to identify a device on a network or amongst other devices**
- A private IP address is **a non-internet-facing IP address used in an internal network**.

- These are **provided by network devices like routers using nat (network address translation)** and can be used over again.p

2. **Public IP Address:**

- A public IP address is **used to identify the device on the Internet**
- A public IP address is **an IP address that can be accessed directly over the Internet and is assigned to your network router by your Internet service provider (ISP)**.

example

ip: 192.168.1.139

subnet mask: 255.255.255.0

The 255.255.255 value of the subnet mask indicates that the first three octets of the IP (192.168.1) won't change and the 0 value of the subnet mask indicates that the last octet of the ip (139) is available for host allocation within the range of 255. The first 3 octets (192.168.1) of the ip are called as the network section and the last section (139) is the host.

network address: 192.168.1.0

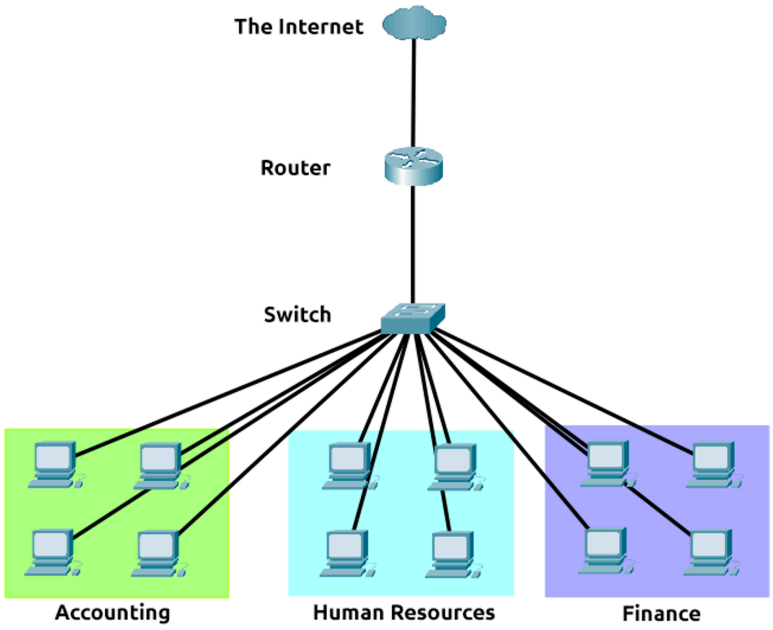
broadcast address: 192.168.1.255

total number of ip address: 253

Subnetting:

Subnetting is dividing a network into smaller, miniature networks within itself or The practice of dividing a network into two or more networks is called subnetting.
example; You will have different departments such as:

- Accounting
- Finance
- Human Resources
- Technical department



1. Network address/subnet address

- The first address in the subnet
- This Address is mostly given to router
- For example, a device with the IP address of 192.168.1.100 will be on the network identified by 192.168.1.0

2. Broadcast address

- A broadcast address is the one that is used by one host to communicated to another host on the same network
- The last address in the subnet

3. Host

Subtract 2 from because 1st address is given to the Network/ Subnet Address and the last address is given to the Broadcast address

4. First available host address

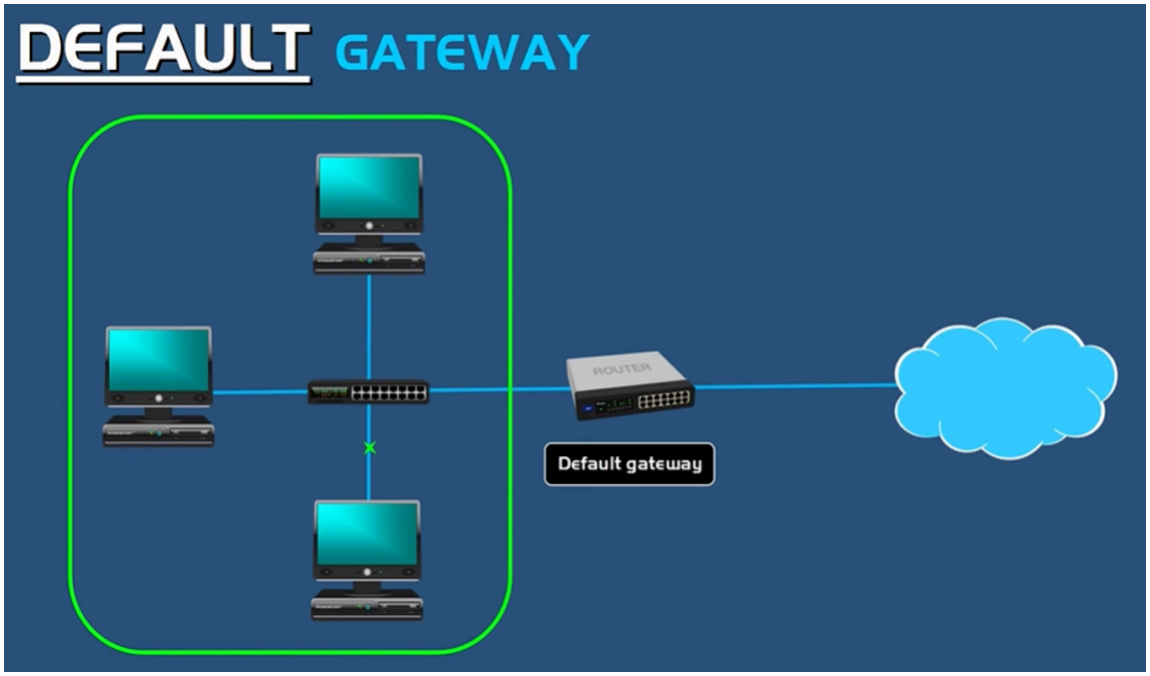
One more than the network address

5. Last available host address

-One less than the broadcast address

Default Gateway:

- default gateway is a **device that forwards data from one network to another. And most of the time, this will be a router.**
- A default gateway lets devices from one network, communicate with devices on another network.
- **If you want to communicate with a device that is not on your network your communication happens through the gateway IP address**
- **It is also called a protocol converter because it helps to connect two different network using different protocols**



Default Gateway Explained and Subnet mask

Subnet Mask:

- Computer uses subnet mask to know if the computer they want to communicate is on their own network or on a different network
- A subnet mask reveals how many bits in the IP address are used for the network by masking the network portion of the IP address .

ARP:

- It binds MAC address with IP address
- In order to map these two identifiers together (IP address and MAC address), the ARP protocol sends two types of messages:
    1. ARP Request
    2. ARP Reply

When an **ARP request** is sent, a message is broadcasted to every other device found on a network by the device, asking whether or not the device's MAC address matches the requested IP address. If the device does have the requested IP address, an **ARP reply** is returned to the initial device to acknowledge this. The initial device will now remember this and store it within its cache (an ARP entry).

RARP (Reverse address resolution protocol)

It maps MAC addresses to IP addresses.

Types of IP Address:

IPV4:

- **Decimal notation**
- 255.255.255.255=11111111.11111111.11111111.11111111 (binary)
- The length is **32 bits** (4 bytes: 8+8+8+8=32bits) (1byte=8bit)
- **4 octets** (Eg: 192.168.1.1)
- 2^32=**4,294,967,296 (4 billion)**

IPV6:

- **Hexadecimal notation**
- The length is **128 bit** (16 bytes: 16+16+16+16+16+16+16+16=128bit)
- **8 octets** (Eg: 2a00:22c4:a531:c500:425f:cce6:c36b:f64d)
- 2^128= 340 trillion-plus

NAT(Network Address Translation):

1. **NAT is used in routers.**
2. **NAT allows multiple devices in a LAN o access the Internet through a single public address by translating their Private IP to Public IP given by ISP**
3. NAT translates a set of IP addresses to another set of IP addresses.
4. **NAT translates:**

- **Private to public**
- **Public to private**

DHCP (dynamic host configuration protocol) (67, 68) (udp)

Each computer runs a dhcp client (which runs on udp port 68), and this will allow the computer to ask for an ip address. Somewhere on the network, there will be a dhcp server (which runs on udp port 67). This is where the ip addresses are managed. DHCP servers can be run on routers or servers. At home it is likely built in to your router, but in an enterprise network, it is likely handled by a server. When you turn your pc on, if it doesn't have an ip, it looks for a dhcp server.

working

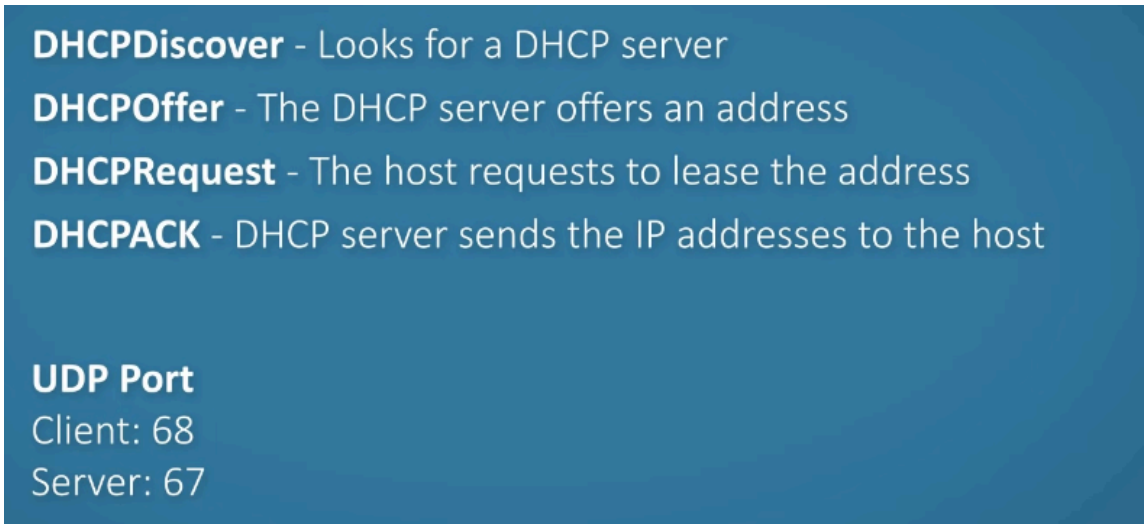
Dhcp discover
Your computer sends a broadcast message to all the devices connected to the network looking for a dhcp server. The other devices look at this message and drop it.

Dhcp offer
When the dhcp server gets the message, it then sends the offer to the host. If more than one offer is given, host will choose the first one it receives.

Dhcp request
The host accepts the offer, and sends the request to the dhcp server.

Dhcp ack
The dhcp sends the ip to the host along with a subnet mask, the default gateway, and the server. The dhcp server keeps a record of all the leased ip addresses and their leased times. When the dhcp server gives out an address, it gives it a lease time. The lease time is a time period where the host will need to renew its address, otherwise it

will return back to the available pool of addresses ready to be dished out to other hosts. This stop ip addresses being wasted any time you throw a computer out or just unplug it.



Networking Devices and LAN Topologies

Hub:

- A HUB is a **physical layer networking device** that is **used to connect multiple devices in a network.** They are generally **used to connect computers in a LAN.**
- HUB is a **dumb device.**
- HUB is a **broadcasting device (It broadcasts the data packet to all the devices connected to the hub by ethernet)**
- Network hubs are best suited for small, simple local area network (LAN) environments.
- **Data Transmission form is an Electrical signal or bits**
- HUB's cost is l**ess than switches. (**only advantage over switch)

Switch:

- A switch is a **data link layer networking device** which c**onnects devices in a network and uses packet switching to send and receive data over the network.**
- Switch is a **smart device**
- The switch **performs MAC address filtering (It stores the MAC address of the devices in the CAM table that are connected to the switch and sends data only to the device for which it is intended)**
- **Data Transmission form is Frame (L2 Switch) Frame & Packet (L3 switch)**

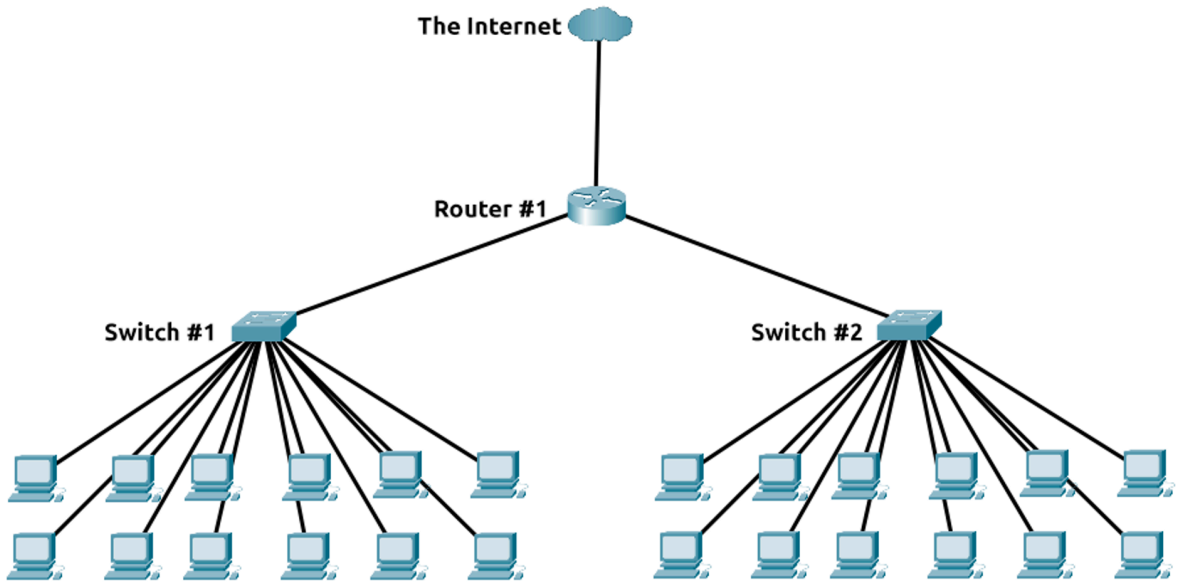
Router:

- **A router is a Network layer device(since it deals with the IP addresses)**
- **To exchange data outside their own network, a device needs to be able to read IP addresses.**
- **A router is used to connect a network to another network or connect a network to the internet**

- There are 2 types of Port, LAN and WAN (LAN is used to connect devices inside the network and WAN port is used the connect devices inside the network to the Internet or outside networks)

What is the use of traceroute?

What is traceroute used for? Running traceroute is helpful for **figuring out the routing hops data has to go through, as well as response delays as it travels across nodes**, which are what send the data toward its destination. Traceroute also enables you to locate points of failure.



Difference Between Hub, Switch and Router

1. Hubs & Switches are used to create networks. Routers are used to connect networks.
2. Hubs and Switches are used to exchange data within a local area network.
3. Hubs and Switches are not used to exchange data outside their own network.

4. To exchange data outside their own network, a device needs to be able to read IP addresses. Router is used to connect a network to another network or connect a network to the internet

Gateway:

- A default gateway is a device that forwards data from one network to another. And most of the time, this will be a router.
- A default gateway lets devices from one network, communicate with devices on another network.
- If you want to communicate with a device that is not on your network your communication happens through the gateway IP address
- It is also called a protocol converter because it helps to connect two different networks using different protocols
- Gateway is network layer device (Layer 3)

Repeater:

- A repeater is an electronic device that receives a signal and retransmits it at a higher level or higher power so that the signal can cover longer distances without degradation. or onto the other side of an obstruction
- It is mainly used in wireless communication (used in both wireless and wired but mainly for wireless)
- Repeater is a physical layer device (Layer 1)

Modem:

- Modem (from modulator-demodulator)

- It converts **digital data (1's and 0's) to analog data (sounds)** so that it can be transmitted through a telephone line and to the receiver side it converts it back to digital data

Bridge:

A bridge is a repeater with additional functionality of reading a mac address. It is a layer 2 (data link layer) device. It is used for interconnecting 2 lans on same protocol.

NIC (Network Interface Controller Card):

- A network interface card (NIC) is a computer hardware component designed to allow computers to communicate over a computer network. It is both an OSI layer 1 and layer 2 device
- NIC **i**s equipped with a unique identifier known as the Media Access Control (MAC) address. This address can be used by routers and switches to control access to a network
- RG45 connecter

Wireless Access Point (WAP):

A wireless access point (WAP or AP): is a device that allows wireless communication devices to connect to a wireless network using Wi-Fi, Bluetooth, or related standards. The WAP usually connects to a wired network and can relay data between the wireless devices (such as computers or printers) and wired devices on the network.

Simplex, Half-Duplex, Full-Duplex:

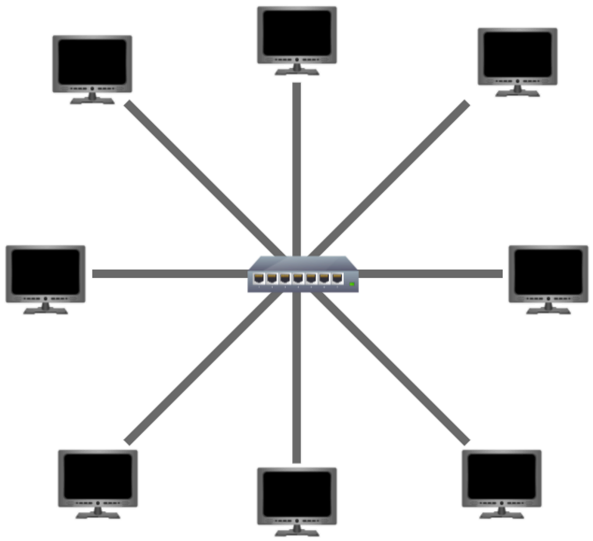
- **Simplex Mode** supports a UniDirectional flow of data.
- **Half-Duplex Mode** supports a Bi-directional flow of data but in one direction at a time.
- **Full-Duplex Mode** supports a Bi-directional flow of data in both directions at the same time (simultaneous flow).

Network Topology:

A network topology is the physical and logical arrangement of nodes and connections in a network.

1. Star Topology:

- In star topology the the devices are connected via a central networking device such as Hub or Switch
- Any information sent to a device in this topology is sent via the central device to which it connects.
- if the centralised hardware that connects devices fails, these devices will no longer be able to send or receive data. Thankfully, these centralised hardware devices are often robust.
- Because more cabling & the purchase of dedicated networking equipment is required for this topology, it is more expensive than any of the other topologies.
- This topology is much more scalable in nature, which means that it is very easy to add more devices as the demand for the network increases.



2. Bus Topology:

- In Bus topology all devices are connected to a single cable called a "bus." which is known as a backbone cable
- devices are connected to the bus using drop lines or taps, which are connected to the main cable.
- typically a coaxial cable or a twisted pair cable is used
- all data destined for each device travels along the same cable, it is very quickly prone to becoming slow and bottlenecked
- It is cost effective
- If this cable were to break, devices can no longer receive or transmit data along the bus.

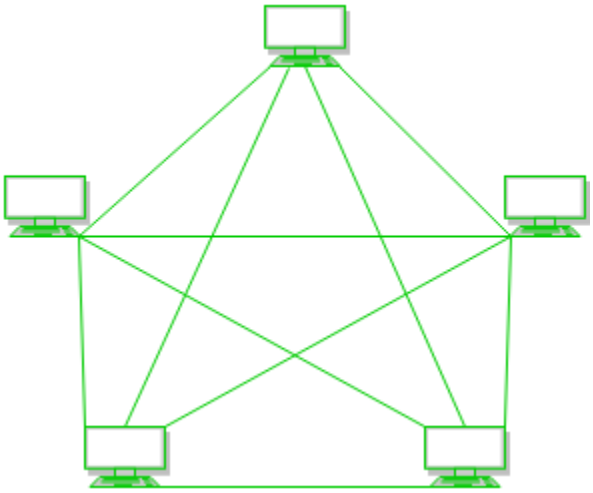
3. Ring Topology:

- The ring topology (also known as token topology)
- In this topology Devices are connected directly to each other to form a loop,
- A ring topology works by sending data across the loop until it reaches the destined device, using other devices along the loop to forward the data

- Because there is only one direction for data to travel across this topology, it is fairly easy to troubleshoot any faults that arise.
- a fault such as cut cable, or broken device will result in the entire networking breaking.

4. Mesh Topology

In a mesh topology, every device is connected to another device via a particular channel. In Mesh Topology, the protocols used are AHCP (Ad Hoc Configuration Protocols), DHCP (Dynamic Host Configuration Protocol), etc.



5. Tree Topology:

- This topology is the variation of the Star topology. This topology has a hierarchical flow of data. In Tree Topology, protocols like DHCP and SAC (Standard Automatic Configuration) are used
- In a tree topology, there is one central node (the “trunk”), and each node is connected to the central node through a single path. Nodes can be thought of as branches coming off of the trunk. (Parent node and Child node)

6. Hybrid Topology:

This topological technology is the combination of all the various types of topologies

.

MAC Address:

- **Media Access Control address**. Also known as **physical address**
- MAC Address is the **unique address used to identify each host and is associated with its NIC (Network Interface Card).**
- **The MAC address is the physical or hardware address burned into each NIC at the time of manufacturing.**
- Everything that uses a NIC (Network Interface Controller) is gonna have a MAC address
- L**ayer 2 Protocol (Data Link layer)**
- It is **48 bits of address**

NIC (Network Interface Card):

- A network interface card (NIC) is a computer hardware component that **allows computers to communicate over a computer network**. It is both an **OSI layer 1 and layer 2 device**
- NIC **i**s equipped with a unique identifier known as the Media Access Control (MAC) address. This address can be used by routers and switches to control access to a network
- RG45 connecter

ARP (Address resolution protocol)

- It binds MAC address with IP address
- It maps IP addresses to MAC addresses. ARP requests only happen in layer 2 (data link layer) networks.

arp -a

this command shows us the arp table which shows us the internet address (ip address), physical address (mac address), and type (this shows us if the mac address was learnt by arp, or if it's a static entry).

RARP (Reverse address resolution protocol)

It maps MAC addresses to IP addresses.

Ping:

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.

What is TTL in connection?

Time to live (TTL) refers to **the amount of time or "hops" that a packet is set to exist inside a network before being discarded by a router**. (a hop is a router in the network).

Protocol

Protocol is a set of rules that determine how data is transmitted between different devices in the same network.

Port:

A port can be referred to as a logical channel through which data can be sent/received to an application. Any host may have multiple applications running, and each of these applications is identified using the port number on which they are running.

TCP, UDP, and Three-Way Handshake

TCP	UDP
Transmission Control Protocol	**User Datagram Protocol**
Connection-oriented protocol (Secure):	**Connectionless protocol** (Unsecure):

This means connection should be established before transmitting of the data. It uses a 3-way handshake to establish a connection	This means that it sends the data without checking whether the system is ready to receive or not.
Retransmission of lost data packets is possible. It is a reliable protocol	**Retransmission of lost data packets is not possible** It is an unreliable protocol
It is **slower** than UDP	It is **faster** than TCP
Used in **Websites**:(HTTP/HTTPS, DNS, SSH, FTP, SMTP)	Used in **Streaming service,** videos, Voice calls, gaming (DNS, DHCP, TFTP. SNMP.....)
TCP is a **Transport layer protocol (Layer 4)**	UDP is a **Transport layer protocol (Layer 4)**
TCP is a communications standard that enables application programs and computing devices to exchange messages over a network. It is designed to send packets across the internet and ensure the successful delivery of data and messages over networks.	UDP is a communications protocol that is primarily used to establish low-latency and loss-tolerating connections between applications on the internet. UDP speeds up transmissions by enabling the transfer of data before an agreement is provided by the receiving party.

Three-way Handshake

- TCP works on a 3-way handshake
- (because it is a connection-oriented protocol you need to establish a reliable connection before communicating with other devices

- **Step 1 (SYN):**

In the first step, the client wants to establish a connection with a server, so it sends **SYN** (**synchronize sequence number)** data packet. which informs the server that the client wants to establish a connection

- **Step 2 (SYN + ACK):**

The server acknowledges the client request and allows to establish a connection with the client by sending an **SYN/ACK** (**acknowledgment sequence number**) data packet to the client.

- **Step 3 (ACK):**

In the last step client acknowledges the response of the server by sending the ACK(**acknowledgment sequence number)** data packet and a reliable connection is established for a secure data transfer

Tcp/ip (transmission control protocol/internet protocol) model

It is a practical model and comprises of the following layers:

Network layer

This consists of the physical and the data link layer of the osi model.

Internet layer

This consists of the network layer of the osi model.

Transport layer

This consists of the transport layer of the osi model.

Application layer

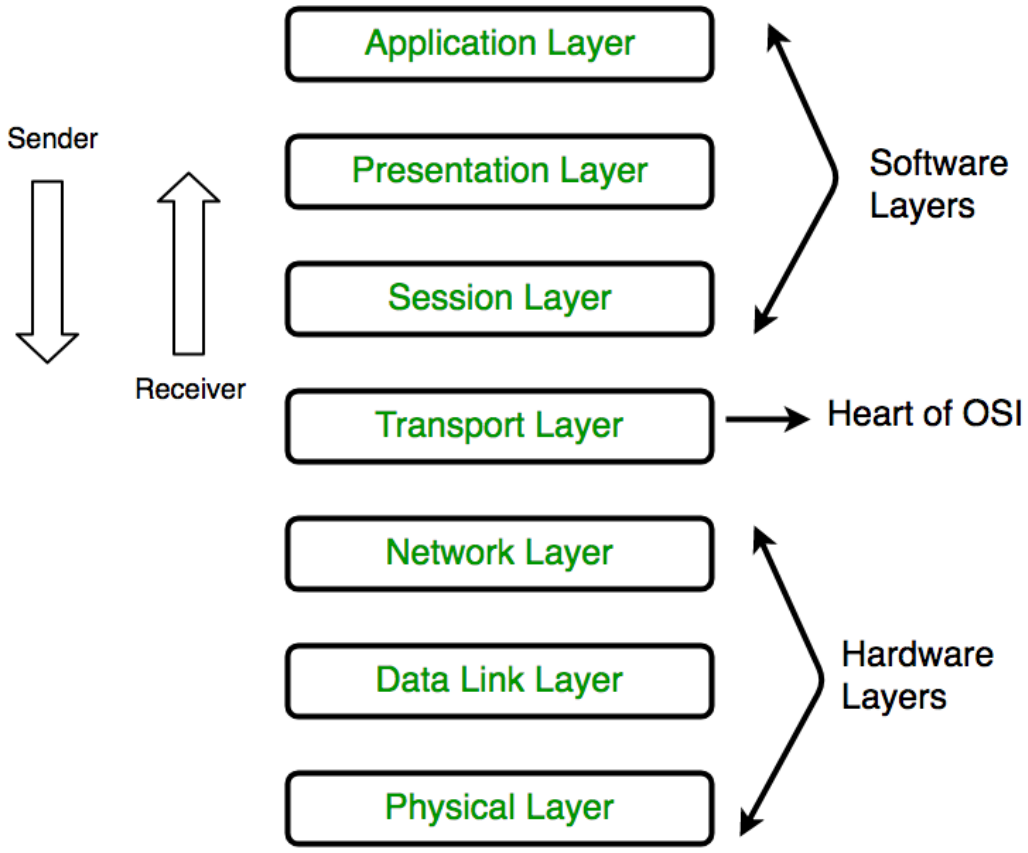
This consists of the session, presentation, and the application layer of the osi model.

OSI Model

Open Systems Interconnection Model

1. it's a **conceptual** model.
2. It **describes how data travels across a network**
3. There are **7 layers** in the OSI model,

4. when data/traffic passes through these layers specific processes take place, and pieces of information are added to this data. this process is called encapsulation



PDNTSPA

Layer 1 - The Physical Layer:

- The Physical layer is responsible for maintaining the communication between the hardware and the network
- The physical layer Controls how the data is transferred over the physical medium
- It is responsible for the actual physical connection between the devices. Such as:

    - **Hardware**: The type of media used on the network, such as type of cable, type of connector, and pinout format for cables.
    - **Topology:** The physical layer identifies the topology to be used in the network. Common topologies include ring, mesh, star, bus, and hybrid
- It converts frames received from the data link layer into bits(1's and 0's) and transmits over a network
- Hub, Repeater, modem, cables are physical layer device

Layer 2 - Data Link Layer: (physical addressing, Mac address, Frame)

- The data link layer is also responsible for error detection, error correction, and hardware addressing.
- The data link layer assigns the MAC address of the sender and receiver to each data packet (received from the network layer) to form a frame this is called physical addressing
- **The MAC address is the physical or hardware address burned into each NIC at the time of manufacturing.**
- A network interface card (NIC) i a computer hardware component that **allows computers to communicate over a computer network**.
- Switch, NIC and bridge is a Data link layer device
- The data in this layer is represented as a frame

Layer 3 - The Network Layer: (logical addressing, Routing, Packet)

- The network layer **transmits the received data segments from one computer to another computer that is located in a different network.**

- The network layer **assigns an IP header to each segment which includes the sender and receiver's IP address to each segment to form an IP packet this is called Logical Addressing**
- It is also called the **routing layer,** It **routes the data packets from source to destination through the shortest path available**
- Protocols used are I**P, IPV4, IPV6, and ICMP,**
- A **router** is a network layer device.
- Data in this layer is represented as **packet**

Layer 4 - Transport Layer: **(TCP/UDP, Segmentation, Port and Sequence number, Segment)**

- This layer **describes how data is being delivered and where it is being delivered into a system.**
- It uses two protocols to transport data: **TCP and UDP**
  - **TCP (Transmission Control Protocol):** Connection-oriented transmission (makes a connection between sender and receiver with the help of a TCP handshake before sending the data) Retransmission of lost data packets is possible
  - **UDP (User Datagram Protocol):** Connectionless transmission
- **Data segmentation is performed, where data is divided into small segments**
- Each segment will **contain source and destination port numbers and the sequence number of the segment, which reassembles the segment in the correct order at the receiver side**
- It is responsible for **Flow control** means it controls the amount of data that is being transported
- It is responsible for **Error control** means if data transmission fails it will re-transmit the failed data segments again
- **A firewall** is a transport layer device.
- Data in this layer is represented as a **Segment**

Layer 5 - Session Layer: (Session management, Authentication and authorization)

- The session layer **creates a connection between the sender and the receiver**
- The session layer is r**esponsible for Creating, managing, and terminating the connection/session between one Sender and receiver**
- **It enables the sending and receiving of data**
- **Authentication and authorization** take place at this layer
    - **Authentication:** Checking the identity of user by asking username and password
    - **Authorization**: Checking if user has the permission to access the resource or data it is trying to access
- **Gateway** is a session layer device

Layer 6 - Presentation Layer: (Translator, SSL/TLS, Encryption/Decryption, Compression)

- Presentation layers **ensure that the data is in usable format**
- It is **often combined with the Application Layer**
- This layer **acts as a translator for data to and from the application layer**
- **Data encryption and decryption occur at this layer.** (SSL/TLS) So that the data is only accessed by authorized users
- **Encodes and Decodes the Data** (Converting password into a hash) (Encoding is part of encryption)
- It **uses data Compression so it is easier to transport**
- **Protocol used in this layer: SSL (TLS)**
- Example: ASCII (American Standard Code for Information Interchange) to EBCDIC (extended binary-coded decimal interchange code**)**, JPEG, JPG, ...

Layer 7 - Application Layer: (GUI, Protocols)

- **The application layer is what we see**
- In the application layer, the **user interacts with the data through GUI**
- The **application layer takes requests and data from the users and passes them to the lower layers of the OSI model.**
- Application layers use **Protocols that determine how users should interact and handle data**
- Protocols used in this layer are **HTTP, FTP, SMTP, DNS, DHCP, Telnet, and POP3**
- Example: Everyday applications such as email clients, browsers, or file server browsing provide a friendly, Graphical User Interface (GUI) **(BROWSER)**

Common Ports, Services, and Protocols

Protocol:

Protocol is a set of rules that determine how data is transmitted between different devices in the network and how users should interact and handle data

Port:

- **A port can be referred to as a logical channel through which data can be sent/received to an application.** Any host may have multiple applications running, and each of these applications is identified using the port number on which they are running.
- **A port number is a 16-bit integer,** hence, we have 2^16 ports available which are categorized as shown below:
    - Total Numbers of Ports: 65,536
    - Range: 0 – 65535
    - “Well-known” & Reserved Ports : 0 to 1023
    - Registered Ports: 1024 – 49151
    - Dynamic ports: 49152 to 65536

Dynamic ports are used to randomly generate unique port numbers for that local a computer that it can use as its source port.

TCP	Description
FTP (21)	**File Transfer Protocol** : Transfer files between systems. Authenticates with username and password
SSH (22)	**Secure Shell:** The ability to log into the machine remotely. SSH is an encrypted version of Telnet
Telnet (23)	**Telnet:** The ability to log into the machine remotely (Console access). Telnet is clear text and not encrypted
SMTP (25)	**Simple Mail Transfer Protocol** : Server to Server mail transfer. (most common way to send email message over the internet)
DNS (53)	**Domain Name System**: Translates domain name to IP Address

HTTP (80) / HTTPS (443)	**Hyper Text Transfer Protocol /Secure:** HTTP/S is the set of rules used for communicating with web servers for the transmitting of webpage data
POP3 (110)	**Post Office Protocol v3** : Basic mail transfer functionality
SMB (139 +445)	**Server Message Block:** file share
IMAP (143)	**Internet Message Access Protocol** : mail transfer functionality. provides more options than POPv3 for managing mail
ICMP	**Internet control message protocol:** It is an error-reporting protocol that network devices such as routers use to generate error messages to the source IP address when network problems prevent the delivery of IP packets.
ARP	**Address resolution protocol:** It maps IP addresses to MAC addresses. ARP requests only happen in layer 2 (data link layer) networks.
RARP	**Reverse address resolution protocol**: It maps mac addresses to ip addresses.

UDP	Description
DNS (53)	**Domain Name System**: Translates domain name into IP Address
DHCP (67, 68)	**Dynamic Host Control Protocol:** It associates you with random IP Address for a specific amount of time
TFTP (69)	**Trivial File Transfer Protocol** : Same as FTP work on UDP instead of TCP , No authentication

SNMP (161)	**Simple Network Management Protocol** is a networking protocol used for the management and monitoring of network-connected devices in Internet Protocol network.

Cryptography: Symmetric and Asymmetric Encryption, Keys and Algorithm

Cryptography

Process of converting plain text into cipher text and vice versa using an encryption algorithm, decryption algorithm, and key

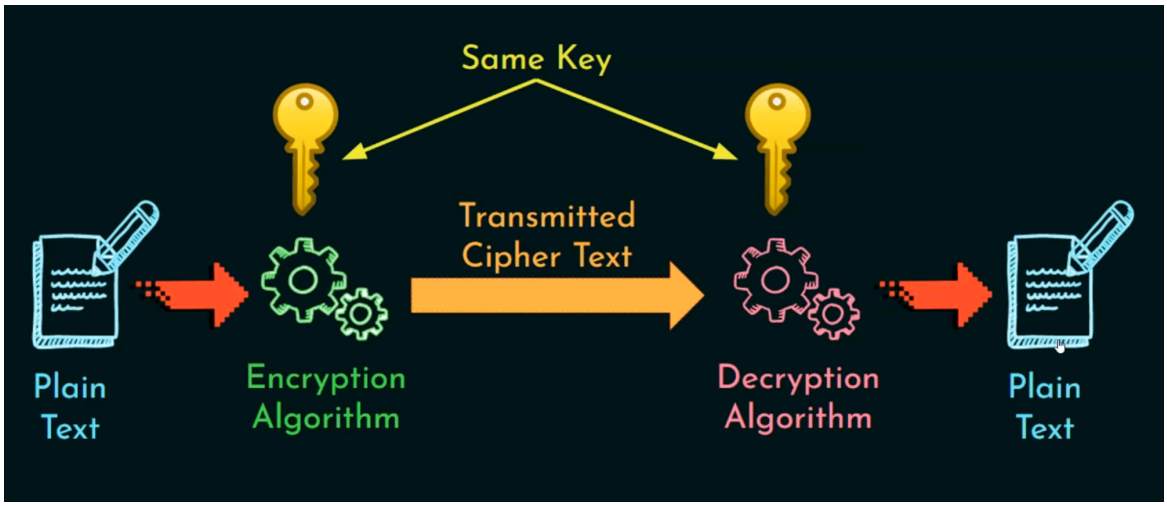
Types of cryptography

1. Symmetric Cryptography (Private Key Cryptography)

2. Asymmetric Cryptography (Public Key Cryptography)

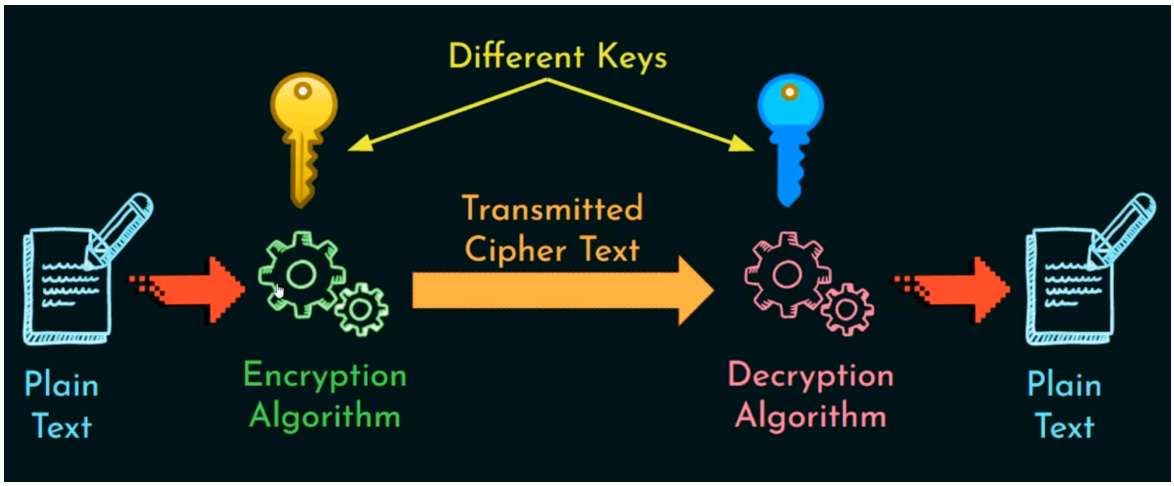
1. Symmetric Cryptography (Private Key Cryptography)

- In this cryptography, only one key is used
- sender and receiver use the same key to encrypt and decrypt the message (Private Key)
- Example: AES and DES



2. Asymmetric Cryptography (Public Key Cryptography)

- In this cryptography, two keys are used
- The Sender uses a different key to encrypt the message(Public key) and the receiver uses a different key to decrypt the data (Private key)
- The Sender uses the receiver's public key to encrypt the message
- The receiver uses his own private key to decrypt the message
- Example: RSA, Diffie-Hellman



Cipher:
They’re encryption algorithms used in cryptography. They are publically known.

Hashing:
The process of converting passwords to cipher text using a hashing algorithm

Eg: MD5, SHA-1, 256

Salting:
The process of **adding a series of random characters to a password before it goes through a hashing process.** This increases the length of the hash and makes it more secure

Digital signature
It is a mathematical technique to validate the authenticity and integrity of a message, software, or digital document.

CA Certificate:

A certificate authority (CA) is a trusted entity that issues Secure Sockets Layer (SSL) certificates.
Web browsers use them to authenticate content sent from web servers, ensuring trust in content delivered online.

DOS (denial of service)
Making a system or a network unavailable to its intended users by sending multiple requests to the victim

DDOS (distributed denial of service)
When multiple systems perform a dos attack to a single target, it is called as ddos. The target is attacked from many locations at once. This makes it difficult to detect the location of the attack.

Malware:

Malware is malicious software designed to harm or exploit computer systems, networks, or applications to gain unauthorized access to information or systems

Types of Malware:

1. **Virus:**

A virus is a computer code that attaches itself to an executable file. It affects a system when the user opens the executable file. A virus cannot be transferred from one PC to another automatically, it needs a medium, and it can be transferred by USB drive, E-mail, etc.

2. **Worms:**
   Worms are malicious programs that replicate themselves to fill the storage and spread across networks without requiring a host file. They often exploit vulnerabilities in network protocols to infect multiple systems rapidly.

3. **Keylogger**
   Keyloggers record the keystrokes entered by a user from a keyboard on a pc infected by a kelogger.

4. **Trojan Horses (Trojans):**
   Trojans disguise themselves as legitimate software to deceive users into installing them. Once activated, Trojans can perform various malicious activities, such as stealing sensitive information or providing backdoor access to attackers.

5. **Ransomware:**
   Ransomware encrypts a user's files and demands a ransom payment in exchange for the decryption key. It can severely impact individuals, businesses, and organizations, rendering data inaccessible until the ransom is paid.

6. **Spyware:**
   Spyware is designed to spy on a user's activities without their knowledge. It can capture sensitive information, such as login credentials, browsing habits, or keystrokes, and send this data to malicious actors.

7. **Botnets**:
   Botnets are networks of compromised computers controlled by a single entity, often for malicious purposes. The infected computers, known as bots, can be used to carry out coordinated attacks, send spam, or participate in distributed denial-of-service (DDoS) attacks.

8. **Rootkits:**
   Rootkits are designed to hide the presence of other malicious software on a system. They often manipulate system functions to conceal their activities, making them difficult to detect and remove.

Social engineering

Manipulating users into giving sensitive information or making them perform tasks is called as social engineering.

Phishing:

Phishing involves sending spoofed email addresses and links to trick people into providing login credentials, credit card numbers, or other personal information. Variations of phishing attacks include:

Baiting:

Baiting is a type of social engineering attack that lures victims into providing sensitive information or credentials by promising something of value for free. For example, the victim receives an email that promises a free gift card if they click a link to take a survey. The link might redirect them to a spoofed Office 365 login page that captures their email address and password and sends them to a malicious actor.

Tailgating (Piggybacking):

Tailgating occurs when an unauthorized person follows an authorized person into a secured area. This physical form of social engineering exploits the natural tendency to be courteous and hold doors open for others.

Firewall, IDS and IPS

PARAMETER	FIREWALL	IDS	IPS
Abbreviation for	-	Intrusion Detection System	Intrusion Prevention System
Definition	**A firewall is a network security device that Monitors/filters incoming and outgoing network traffic based on predetermined rules**	**Intrusion detection system (IDS) is a device or software application that monitors traffic for monitors network traffic for suspicious activity and alerts when such activity is discovered.**	**An Intrusion Prevention System (IPS) is a device or a software application that monitors network traffic for suspicious activity and then detects it, classifies it, and then takes action to prevent it, including reporting, blocking, or dropping it, when it does occur.**
Principle of working	Filters traffic based on **IP address and port numbers**	Monitors the traffic based on **patterns or signatures of attack and then generates alerts**	Monitors the traffic based on p**atterns or signatures of attack and then prevents the attacks on detection**
Placement	**Placement is at the perimeter of the**	**Placement is through port span or via tap.**	**Placement is generally after the**

	network. Should be 1st Line of defense.	**Should be placed after the firewall**	**firewall. Should be placed after the Firewall device in network**
OSI layer	**Layer 3 (Network) Since it deals with IP address it is Network layer device**	**Layer 3 and 4 (Network and Transport)**	**From Layer 2 to Layer 7**
Configuration mode	Layer 3 mode or transparent mode	Inline or as end host (via span) for monitoring and detection	Inline mode , generally being in layer 2
Traffic patterns	Not analyzed	Analyzed	Analyzed
Placement wrt each other	Should be 1st Line of defense	Should be placed after firewall	Should be placed after the Firewall device in network
Action on unauthorized traffic detection	Block the traffic	Alerts/alarms on detection of anomaly	Preventing the traffic on Detection of anomaly
Related terminologies	> Stateful packet filtering> permits and blocks traffic by port/protocol rules	> Anomaly based detection> Signature detection> Zero day attacks> Monitoring> Alarm	> Anomaly based detection> Signature detection> Zero day attacks> Blocking the attack

IDS and IPS: Signature based blocking

Firewall: IP Based blocking

Firewall: Parameter-Based Monitoring

IDS and IPS: Signature-based monitoring

What are signature-based attacks?

Signature-based ID systems **detect intrusions by observing events and identifying patterns that match the signatures of known attacks**. An attack signature defines the essential events required to perform the attack and the order in which they must be performed.

SPAN: A SPAN port (sometimes called a mirror port) is a software feature built into a switch or router that creates a copy of selected packets passing through the device and sends them to a designated SPAN port

Firewall:

- A firewall is a network security device that Monitors/filters incoming and outgoing network traffic based on predetermined rules.
- It filters the traffic based on IP Address, Ports, Protocols, Domain name, etc.
- These rules are also known as the access control list, these rules are customizable.
- These rules are determined by the network administrator.
- The firewall comes in as a standalone device which is mainly used in a large organization or they come as a built-in component in the router.
- **Placement is at the perimeter of the network. Should be 1st Line of defense.**

Types of Firewalls:

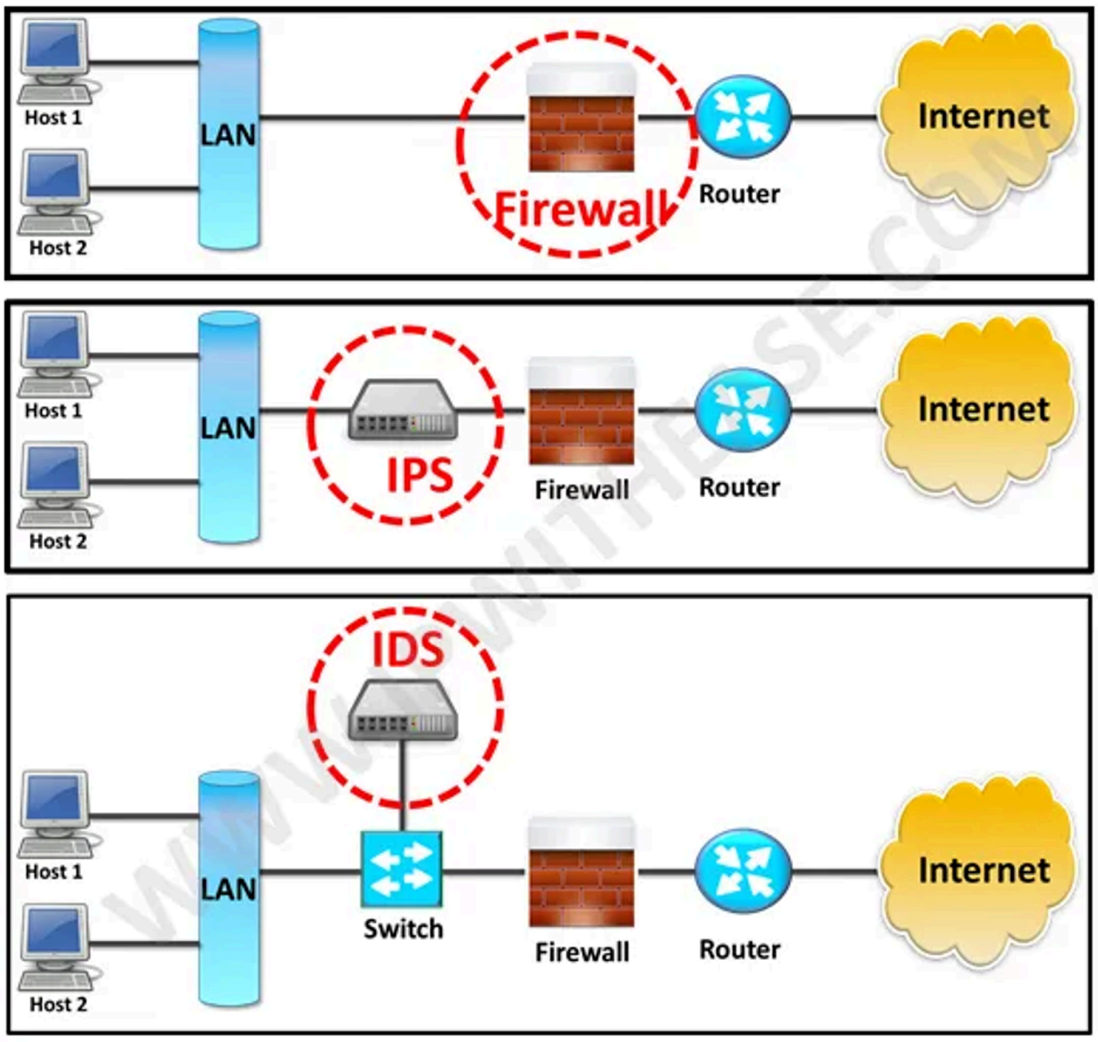
1. **Host-Based Firewall:**
   It is a software firewall installed on the devices or computer connected inside a private network and it protects that computer only
   Eg: The newer version of Windows comes with a pre-installed host-based firewall

2. **Network-Based Firewalls:**

It is a combination of hardware and software and is placed between a private network and the public internet

A network-based firewall protects the entire private network from the public internet unlike a host-based firewall which protects only a single computer or device

it operates at the network layer



Network scanning
Detecting all active hosts (devices) on a network and mapping them to their ip addresses is called as network scanning.

Port scanning
Process of sending packets to specific ports on a host and analyzing the responses to learn details about its running services or locate potential vulnerabilities is called as port scanning.

Sniffing
Intercepting and monitoring traffic on a network is called as sniffing.

Passive sniffing
In passive sniffing, the attacker doesn't interact with the target. Sniffing is carried out through hub. The attacker captures packets transmitted and received by the network or exchanged between two machines. For example, hub based networks or wireless networks.

Active sniffing
In active sniffing, the attacker directly interacts with the target by sending packets and receiving responses. Sniffing is carried out through switch.

The attacker poisons the switch by sending spoofed mac address. For example, mac flooding, arp spoofing, etc.

DOS (denial of service)
Making a system or a network unavailable to its intended users by sending multiple requests to the victim

DDOS (distributed denial of service)
When multiple systems perform a dos attack to a single target, it is called as ddos. The target is attacked from many locations at once. This makes it difficult to detect the location of the attack.

Vulnerability
Flaws or weaknesses in the code through which an attacker can gain access to a system/network is called as vulnerability.

Threat
When you exploit vulnerabilities in a system/network, it is called as a threat.

Risk
The probability of threat and damage to a system/network is called as risk

Exploit

Exploit is a tool that can be used to take advantage of a vulnerability, and what delivers the payload (Exploits give you the ability to pop a shell/run your payload code).

Payload
It is a malicious program or a piece of code placed by an exploit.

Zero-day vulnerability
A zero-day vulnerability is a vulnerability that has not yet been discovered by the system vendor or security researchers.

Application:

It is a type of software that is built for specific tasks. For example, web browsers, media players, etc.

Framework:

It is a software used by developers to develop other software.

Advisory:

Provides list of vulnerable IP, domains, hashes which we can put inside the IDS and Firewall rules to block it

Kernel

It is a computer program that has complete control over everything in the system. It handles the interactions between hardware and software.

Cybersecurity:

- Cybersecurity or Information security refers to the security of computer systems, networks, applications, data or infrastructure from digital threats, attacks, unauthorized access
- The goal is to maintain the Confidentiality, Integrity, and Availability of the data

Vulnerability Assessment

- VA **identifies the vulnerability and issues in the system/application or network**
- A vulnerability assessment is the **process of defining, identifying, classifying, and prioritizing vulnerabilities** in computer **systems, applications, and network infrastructures.**

- The goal of a vulnerability assessment is to evaluate the security posture of an organization and identify potential weaknesses that could be exploited by attackers.

Penetration testing

- The process of testing a computer system/network/web application with permission from the owner or organization for vulnerabilities and loopholes that an attacker could exploit is called penetration testing.
- It can be automated or performed manually.

VAPT:

VA identifies the vulnerability and issues in the system/application or network and In PT the tester exploits the vulnerability found in VA to verify and check the impact of the vulnerability that an attacker could exploit

Types of pentesting:

1. White box pentesting:

In white box pentesting, the **tester has been provided with the whole range of information about systems/networks like schema, source code, internal design, data structure, os details, IP address, etc.** It is also known as structural, glass box, clear box, and open box.

2. Black box pentesting:

In black box pentesting, the **tester has no knowledge about the target system/network. He must gather information about the target system/network.**

3. Grey box testing:

In grey box testing, the **tester is provided with partial information about the internal details of the system.**

Steps for VA:

1. Define scope

Clearly define the scope of the assessment, including the systems, networks, and applications to be evaluated.

(**Define what part of the application needs to be tested and what part is out of scope**)

2. Identify Assets

Identifying the asset that needs to be scanned

3. Prioritization Assets

It isn’t possible to scan every asset of the company without considering the budget of the company. Vendors often charge per asset. Assets like Internet-facing (Assets that are exposed publicly to the Internet and accessible through one or several ports are classified as Internet-facing) servers, and employee laptops should be at the highest priority.

Prioritize assets based on their criticality to the organization's operations and potential impact if compromised.

4. Vulnerability Scanning (using automated tools)

The scanner looks for open ports and services, software versions, and configuration settings. Based on this **the scanner identifies known vulnerabilities and weak security settings.**

5. Risk Assessment:

Evaluate the risk of the vulnerability based on the impact

6. Reporting and remediation

Prepare comprehensive reports that document the findings, including a **detailed description of each vulnerability, its risk level, and recommended remediation steps.**

Steps for PT:

1. Gather Information (Reconnaissance):

- Conduct information gathering to gather intelligence about the target environment. This may include DNS enumeration, WHOIS lookups, and other methods to identify potential entry points.

2. Scanning (Enumeration):

- Use automated scanning tools to identify open ports and services, the scanner identifies known vulnerabilities and weak security settings.

3. Exploitation:

- Attempt to exploit identified vulnerabilities to assess the impact of a successful attack. This may include exploiting weak credentials, injection attacks, or misconfigurations.

4. Post-Exploitation:

- conduct post-exploitation activities to understand the extent of the compromise. This may involve lateral movement, privilege escalation, and data exfiltration.

5. Reporting and Remediation

- Prepare a comprehensive report that includes a detailed summary of findings, risk assessments, and recommended remediation steps. The report should be tailored for both technical and non-technical audiences.

Phases of Hacking

Rise and **Shine Good Morning Chips**

1. **Reconnaissance (Information Gathering): Active and Passive**

Gathering info about target like ip range, network, dns records, etc. through active or passive recon

2. **Scanning: Nmap, Nessus, Nikto, etc**

Scanning the system/network or application with the help of automated tools to find open ports and know vulnerabilities and weak security settings

3. **Gaining Access (Exploitation):**

The hacker uses the information gathered in the first and the second phase to gain access into the system by exploiting this information.

4. **Maintaining Access:**

In this phase, the hacker must maintain the access gained. The system can be used as a base to launch additional attacks in the future.

5. **Clearing Tracks**

In this phase, the hacker tries to delete his presence from the target system. This is achieved by deleting the sent mails, clearing server logs, clearing temp files, etc. Also prior to the attack, the hacker changes his mac address and uses vpn to attack the target system.

Red, Blue and Purple Team

Red team

These are a group of people **hack or exploit the application with the permission of the organization to find vulnerabilities** in the system, application, or network

Blue team

These are a group of peopleprotecting the organization against cyberattcks. They **assess an organization's security and take actions to remediate any vulnerabilities. The Blue Team defends against such attacks**

Purple team

This combines the skills of both the red team and the blue team. A purple team can be one member of a red team and one of a blue team working together.

Reporting:

Prepare a comprehensive report that includes a detailed summary of findings, risk assessments, and recommended remediation steps.

The report should be tailored for both technical and non-technical audiences.

Executive Summary (Client)

1. Summary of the report- overview of findings in chart or graph format including vulnerabilities found organized according to severity, a classification
2. Which vulnerabilities should be prioritized
3. How to remediate these vulnerabilities

Technical Report

1. Detailed test breakdown: How the test was performed, what were the findings, and the impact of vulnerabilities
2. Evidence of Exploitation: Screenshots
3. Remediation information for developers
4. Hardening information for system administrators
1.

Report Parameters:

2. **Description**
3. **POC**
4. **Payload**
5. **Severity**
6. **Reference**
7. **Impact**
8. **Solution/ Remediation**

SIEM Tools: (SOC analyst Monitoring tools)

1. Qradar- IBM
2. Ark site- HP
3. Splunk
4. OSSIM- Alien Vault

Wifi (wireless fidelity):

It is a technology that allows devices to connect a network wirelessly.

Wifi hacking

iwconfig (to check the name of the network adapter)

ifconfig wlan0 down (to disable an interface (wlan0))

airmon-ng check kill (this checks and kills the processes that might interfere with the aircrack-ng suite)

iwconfig wlan0 mode monitor (this enables the monitor mode)

ifconfig wlan0 up (to enable an interface (wlan0))

iwconfig (check if the interface (wlan0) is in monitor mode)

airodump-ng wlan0 (to show all the networks in your area)

airodump-ng -d “bssid (mac address) of the target network” -c “channel of the network” -w “name for the handshake file (.cap file)” wlan0

aireplay-ng –deauth “number of deauthentication packets sent to the target” -a “bssid (mac address) of the target network” wlan0

now create a wordlist

nano “name of the wordlist with the extension as .txt”

Identification:

- Identification involves the **process of presenting an identity or credentials to the system.**
- **Eg: Providing username and password**

Authentication:

- It is a **mechanism used to verify the user's identity** and confirm that they are who they say they are
- It is the ability to verify a user's identity

Session:

A session is a **series of interactions, or transactions, between a user and a system that occurs during a specific period of time**

Session Management:

- After authentication, **a session is created, and the server generates Cookie that is tied to the username** which **acts as a short-lived password**.
- **This cookie verify the identity of user every time the user sends a request to server**

Cookie:

- cookie is a small piece of data that allows the web application to remember information about the client/user.
- Cookies are saved when the client receives a "Set-Cookie" header in the response from the web server.

Session ID:

- A session ID is a unique identifier assigned to a user's session on a web server.
- It is typically generated by the server when a user first visits a website and is used to track the user's interactions during that session.
- The session ID is often stored on the server, and a corresponding reference to it may be stored on the client side, usually in the form of a cookie.

Access Control:

It **determines whether the user is allowed to carry out the action that they are attempting to perform.**

Reverse Shell:

- A reverse shell is a **type of shell in which the target machine initiates a connection to the attacker's machine, allowing the attacker to execute commands on the target machine remotely.**
- Reverse shells are commonly used in penetration testing and other security-related tasks, as they allow an attacker to gain remote access to a system without the need for any user interaction or network configuration.

Meterpreter:

A Meterpreter session is a component of the Metasploit framework, d**esigned for post-exploitation tasks**. It **allows an attacker to interact with a compromised system, providing a powerful interface to manipulate and gather information.**

Questions asked in Interview

1. OSI model
2. TCP/IP model
3. Firewall and types of firewall
4. Encryption and types of encryption
5. What is a Vulnerability assessment and the steps of VA
6. Difference between encryption and encoding
7. OWASP Top 10 any vulnerability - SQL injection
8. Python - tuples and list
9. HTML basic
10. Metasploit- what is meterpreter? And how exactly do you exploit to gain access (what is this called?)
11. Burpsuite- tabs, intruder tab and how would you perform brute force