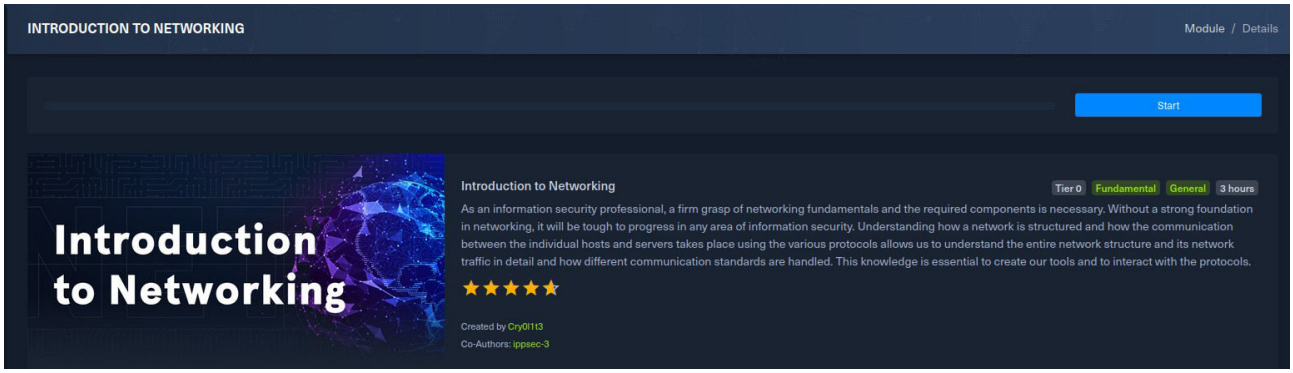
Eric Mwenda

Introduction to Networking

https://academy.hackthebox.com/achievement/596337/34



Networking Overview

In this module we began by explaining why a network is important and we all agree that for two computers to communicate with each other there must be a network that enables them to do so.

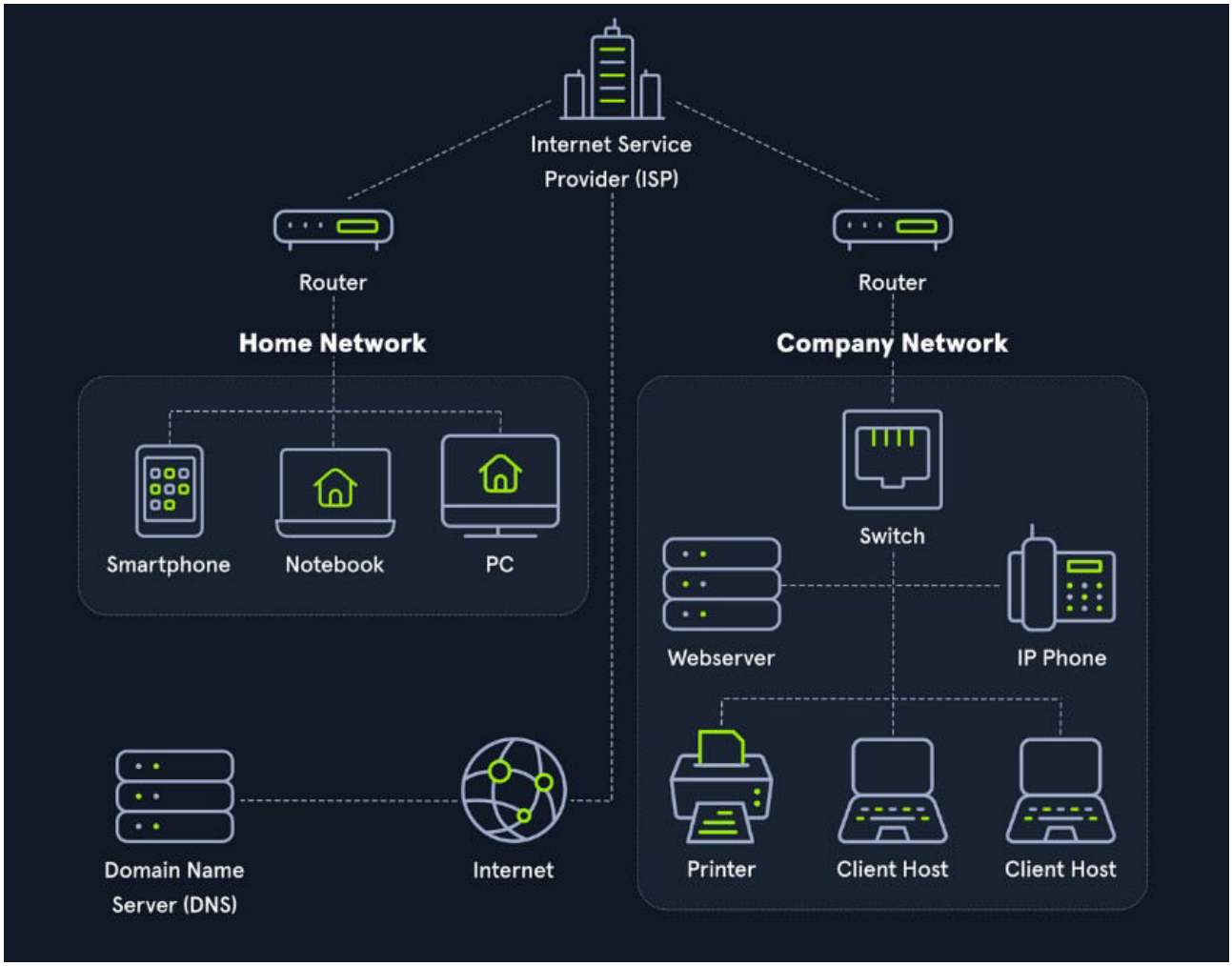
A network is composed of a wind array of topologies some of them include the mesh, tree, star and the ring, mediums may include ethernet, fiber, coax andwireless and protocols may include TCP, UDP, IPX that can be used to facilitate the network

Story Time - A Pentesters Oversight

Most networks use a /24 subnet, so much so that many Penetration Testers will set this subnet mask (255.255.255.0) without checking.

The /24 network allows computers to talk to each other as long as the first three octets of an IP Address are the same (ex: 192.168.1.xxx)

Basic Information



In the above figure we looked at a scenario that we want to visit a company's website from our "Home Network." In that case, we exchange data with the company's website located in their "Company Network." As with sending mail or packets, we know the address where the packets should go.

Another name for the **website address or Uniform Resource Locator (URL)** which we enter into our browser is **Fully Qualified Domain Name (FQDN).**

What is the difference between URLs and FQDN ?

A FQDN only specifies the address of the "building" ie (www.hackthebox.eu) while a URL specifies the "floor," "office," "mailbox" and the corresponding "employee" for whom the package is intended. Ie (https://www.hackthebox.eu/example?floor=2&office=dev&employee=17)

Assessments made from the diagram above on what the company network should consist of:-

- HTB suggests there should be 5 separate networks.

1. The Web Server should be in a DMZ (Demilitarized Zone) because clients on the internet can initiate communications with the website, making it more likely to become compromised. Placing it in a separate network allows the administrators to put networking protections between the web server and other devices.

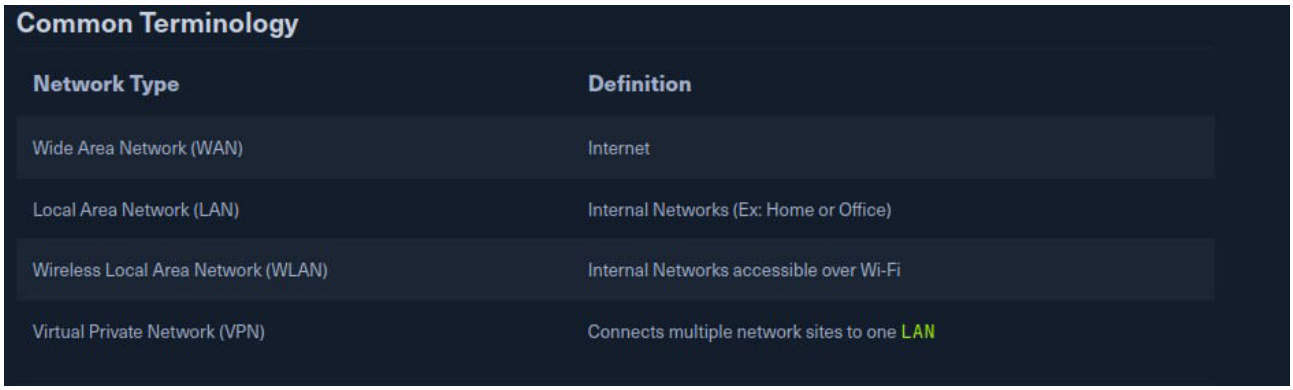
2. Workstations should be on their own network, and in a perfect world, each workstation should have a Host-Based Firewall rule preventing it from talking to other workstations. If a Workstation is on the same network as a Server, networking attacks like spoofing or man in the middle become much more of an issue.

3. The Switch and Router should be on an "Administration Network." This prevents workstations from snooping in on any communication between these devices. I have often performed a Penetration Test and saw OSPF (Open Shortest Path First) advertisements. Since the router did not have a trusted network, anyone on the internal network could have sent a malicious advertisement and performed a man in the middle attack against any network.

4. IP Phones should be on their own network. Security-wise this is to prevent computers from being able to eavesdrop on communication. In addition to security, phones are unique in the sense that latency/lag is significant. Placing them on their own network can allow network administrators to prioritize their traffic to prevent high latency more easily.

5. Printers should be on their own network. This may sound weird, but it is next to impossible to secure a printer. Due to how Windows works, if a printer tells a computer authentication is required during a print job, that computer will attempt an NTLMv2 authentication, which can lead to passwords being stolen. Additionally, these devices are great for persistence and, in general, have tons of sensitive information sent to them.

Network Types



There are various types of networks, this networks include:-

1. WAN – Wide Area Network.

2. LAN – Local Area Network.

3. WLAN – Wireless Local Area Network.

4. VPN – Virtual Private Network.

WAN (Wide Area Network)

This is commonly referred to as the **Internet.**

WAN is a large number of LANs joined together. This network coveres broader geographical space and can cover a city, cities, county or countries.

This network also can be used in large companies or government agencies. This companies can have an "Internal WAN" (also called Intranet, Airgap Network, etc.).

WAN networks can be identified using a WAN Specific routing protocol such as BGP or observing if the IP Schema in use is within RFC 1918 (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) if not, then it is a WAN.

LAN / WLAN

LANs (Local Area Network) and WLANs (Wireless Local Area Network) will typically assign IP Addresses designated for local use (RFC 1918, 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16).

LAN/WLAN covers a smaller geographical range than the WAN. Areas of use:- Colleges, Hospitals, Hotels etc.

The only diffrence between a LAN and WLAN is that WLAN's introduce the ability to transmit data without cables. It is mainly a security designation.

VPN (Virtual Private Networks)

We have three types of Virtual Private Networks (VPNs) tho all the three have one goal of making the user feel as if they were plugged into a different network. This VPNs are:-

1. Site-To-Site Vpn.

2. Remote Access VPN

3. SSL VPN

Site-To-Site VPN

In this type of VPN both the client and server are Network Devices, typically either Routers or Firewalls, and share entire network ranges. This is most commonly used to join company networks together over the Internet, allowing multiple locations to communicate over the Internet as if they were local.

Remote Access VPN

This VPN enables the client's computer creating a virtual interface that behaves as if it is on a client's network.

A good example was the VPNs we connect to in the HTB and TRYHACKME.

When analyzing these VPNs, an important piece to consider is the routing table that is created when joining the VPN. If the VPN only creates routes for specific networks like 10.10.10.0/24, this is called a Split-Tunnel VPN, meaning the Internet connection is not going out of the VPN.

Split-tunnel is most appropriate in the case privacy concern and of monitoring your internet connection is not necessary, However, for a company, split-tunnel VPN's are typically not ideal because if the machine is infected with malware, network-based detection methods will most likely not work as that traffic goes out the Internet.

SSL VPN

This is a VPN that is done within our web browser which is becoming increasingly common in web browsers.

Typically these will stream applications or entire desktop sessions to your web browser.

Other Terms Include:-

Network Type	Definition
Global Area Network (GAN)	Global network (the Internet)
Metropolitan Area Network (MAN)	Regional network (multiple LANs)
Wireless Personal Area Network (WPAN)	Personal network (Bluetooth)

GAN (Global Area Network)

A worldwide network such as the Internet is known as a Global Area Network (GAN). However, the Internet is not the only computer network of this kind. Internationally active companies also maintain isolated networks that span several WANs and connect company computers worldwide. GANs use the glass fibers infrastructure of wide-area networks and interconnect them by international undersea cables or satellite transmission.

MAN (Metropolitan Area Network)

Metropolitan Area Network (MAN) is a broadband telecommunications network that connects several LANs in geographical proximity. As a rule, these are individual branches of a company connected to a MAN via leased lines. High-performance routers and high-performance connections based on glass fibers are used, which enable a significantly higher data throughput than the Internet. The transmission speed between two remote nodes is comparable to communication within a LAN.

PAN / WPAN

Modern end devices such as smartphones, tablets, laptops, or desktop computers can be connected ad hoc to form a network to enable data exchange. This can be done by cable in the form of a Personal Area Network (PAN).

The wireless variant Wireless Personal Area Network (WPAN) is based on Bluetooth or Wireless USB technologies. A wireless personal area network that is established via Bluetooth is called Piconet. PANs and WPANs usually extend only a few meters and are therefore not suitable for connecting devices in separate rooms or even buildings.

Networking Topologies

A network topology is the arrangement, physical or logical connection of devices in a network.

The network topology determines the components to be used and the access methods to the transmission media. The transmission medium layout used to connect devices is the physical topology of the network. For conductive or glass fiber media, this refers to the cabling plan, the positions of the nodes, and the connections between the nodes and the cabling

We can divide the entire network topology area into three areas:

1. Connections	
Wired connections	Wireless connections
Coaxial cabling	Wi-Fi
Glass fiber cabling	Cellular
Twisted-pair cabling	Satellite

The network has various nodes connected to it, this are:-

Repeaters	Hubs	Bridges	Switches
Router/Modem	Gateways	Firewalls	

Network nodes are the transmission medium's connection points to transmitters and receivers of electrical, optical, or radio signals in the medium. A node may be connected to a computer, but certain types may have only one microcontroller on a node or may have no programmable device at all.

Classifications

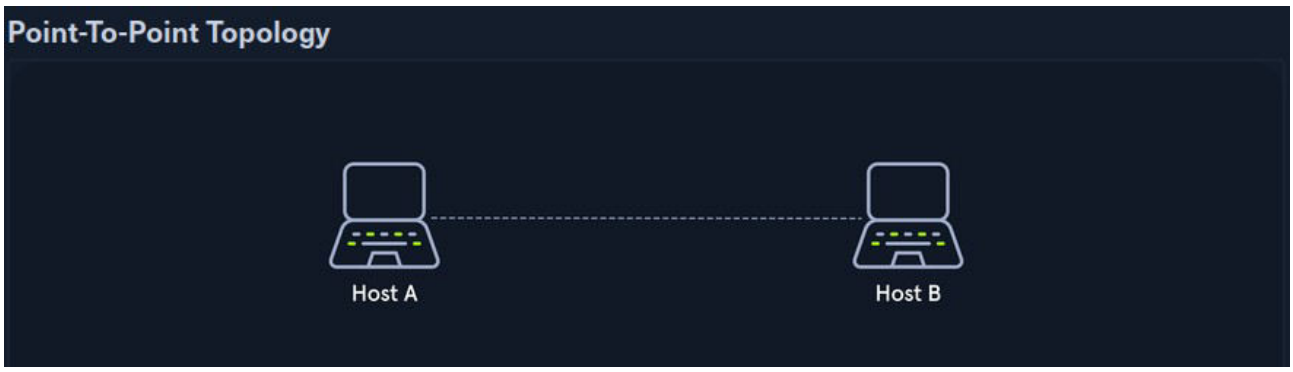
This is the structure of a network or the topology. Topologies can be either physical or logical.

Network topologies are divided into the following eight basic types this are:

Point-to-Point	Bus
Star	Ring
Mesh	Tree
Hybrid	Daisy Chain

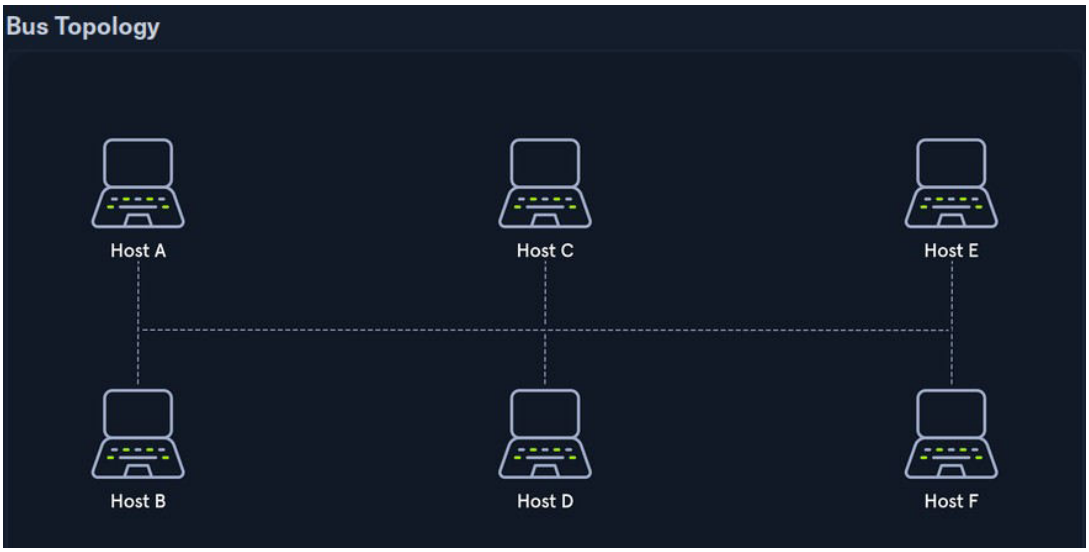
Point-to-Point

This is the simplest network topology with a dedicated connection between two hosts there is a direct and straightforward physical link existing only between the two hosts



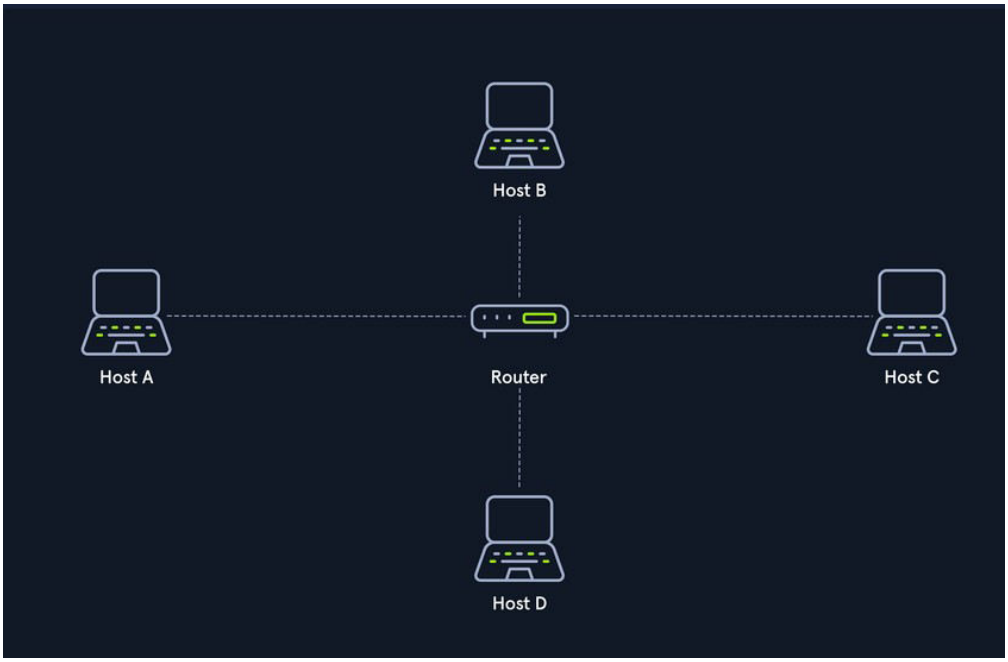
Bus

In this kind o topology all hosts are connected via a transmission medium in the bus topology. Every host has access to the transmission medium and the signals that are transmitted over it. There is no central network component that controls the processes on it.



Star

The star topology is a network component that maintains a connection to all hosts. Each host is connected to the central network component using separate links.

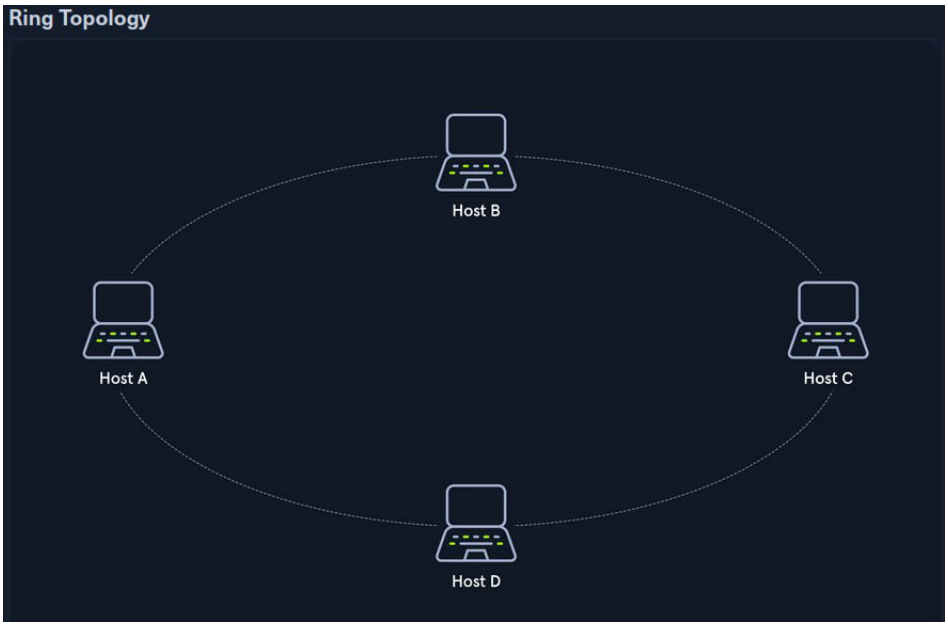


Ring

In a **physical topology** each host or node is connected to the ring with two cables. One for the incoming signals and the another for the outgoing one

For a **logical ring topology** it is based on a physical star topology, where a distributor at the node simulates the ring by forwarding from one port to the next.

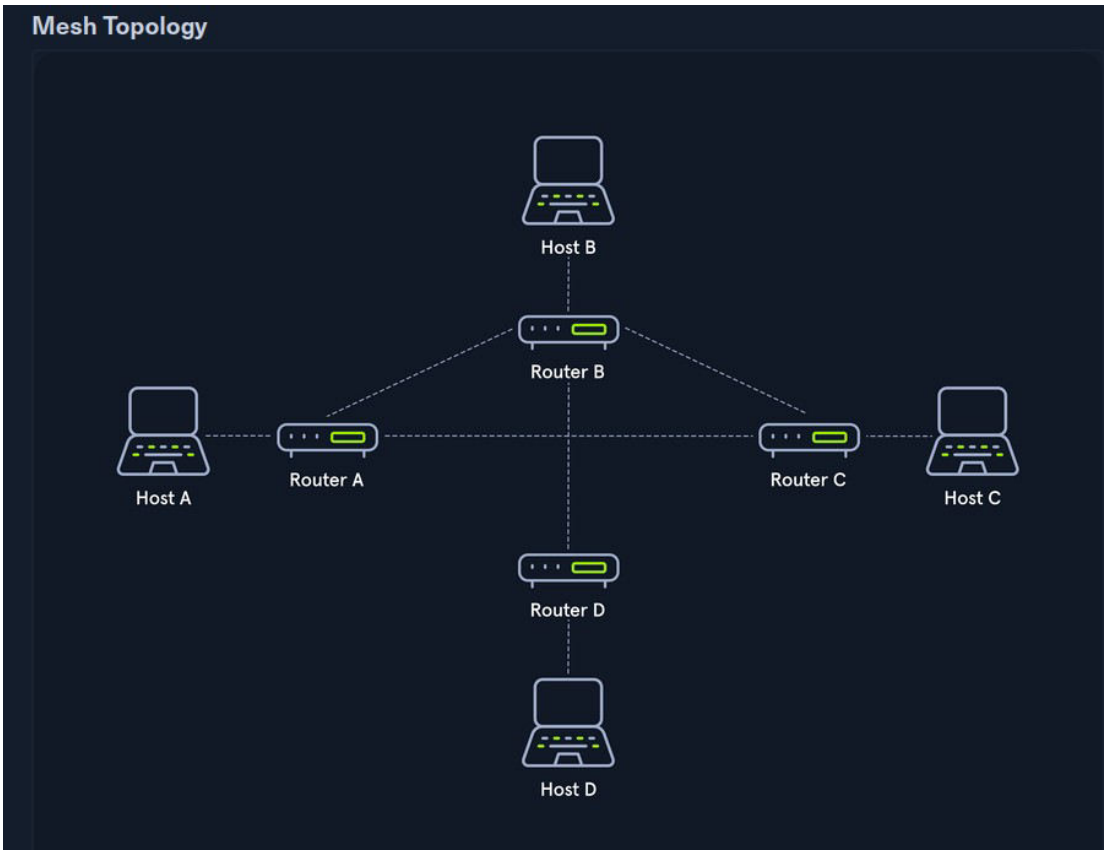
Typically, the transmission medium is accessed sequentially from station to station using a retrieval system from the central station or a token. A token is a bit pattern that continually passes through a ring network in one direction, which works according to the claim token process.



Mesh

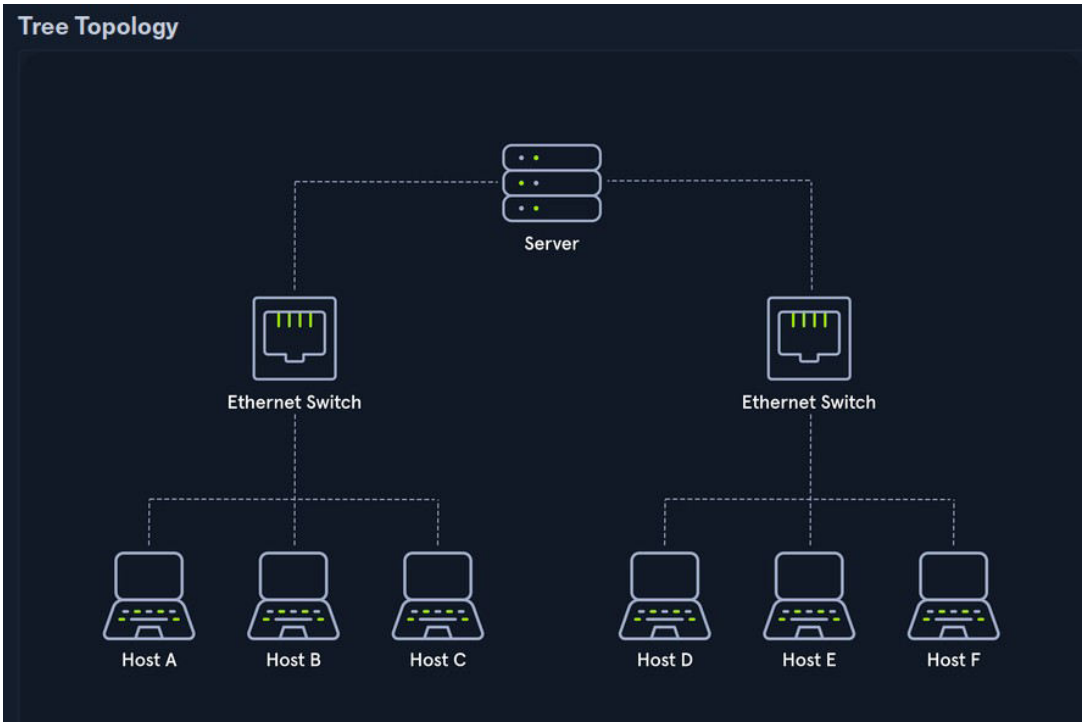
Meshed structures have no fixed topology. There are two basic structures from the basic concept: the fully meshed and the partially meshed structure.

Each host is connected to every other host in the network in a fully meshed structure. This means that the hosts are meshed with each other. This technique is primarily used in WAN or MAN to ensure high reliability and bandwidth.



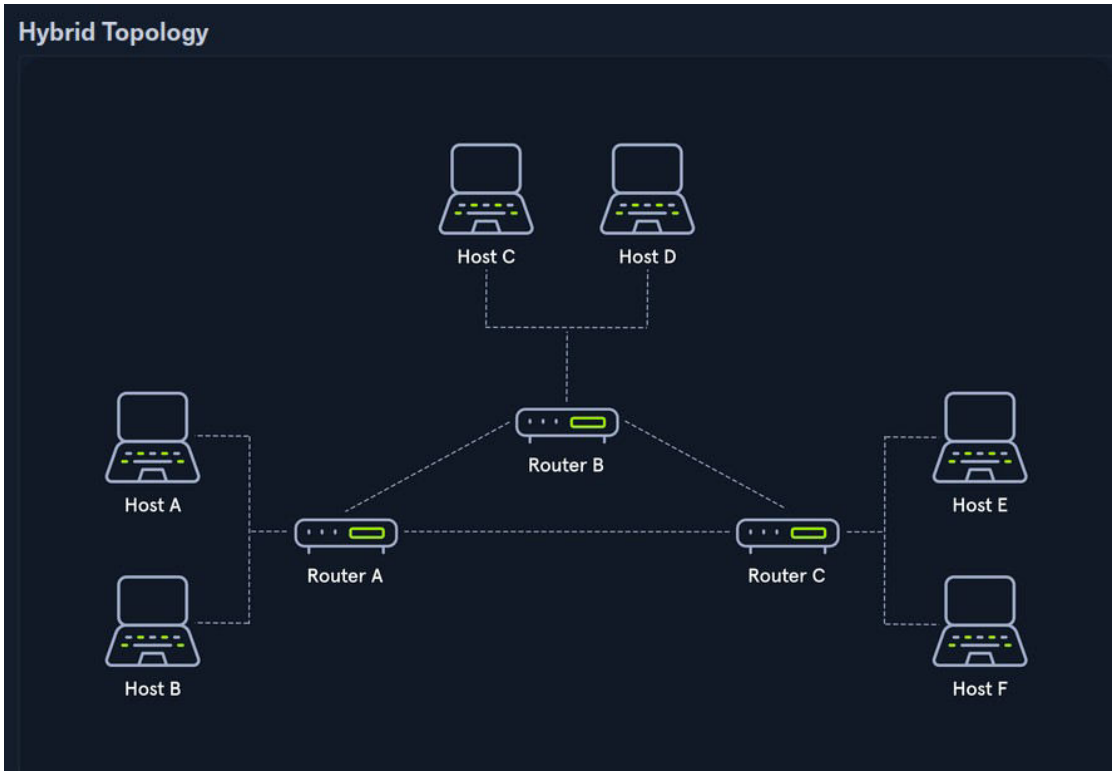
Tree

The tree topology is an extended star topology that more extensive local networks have in this structure. This is especially useful when several topologies are combined. This topology is often used, for example, in larger company buildings.



Hybrid

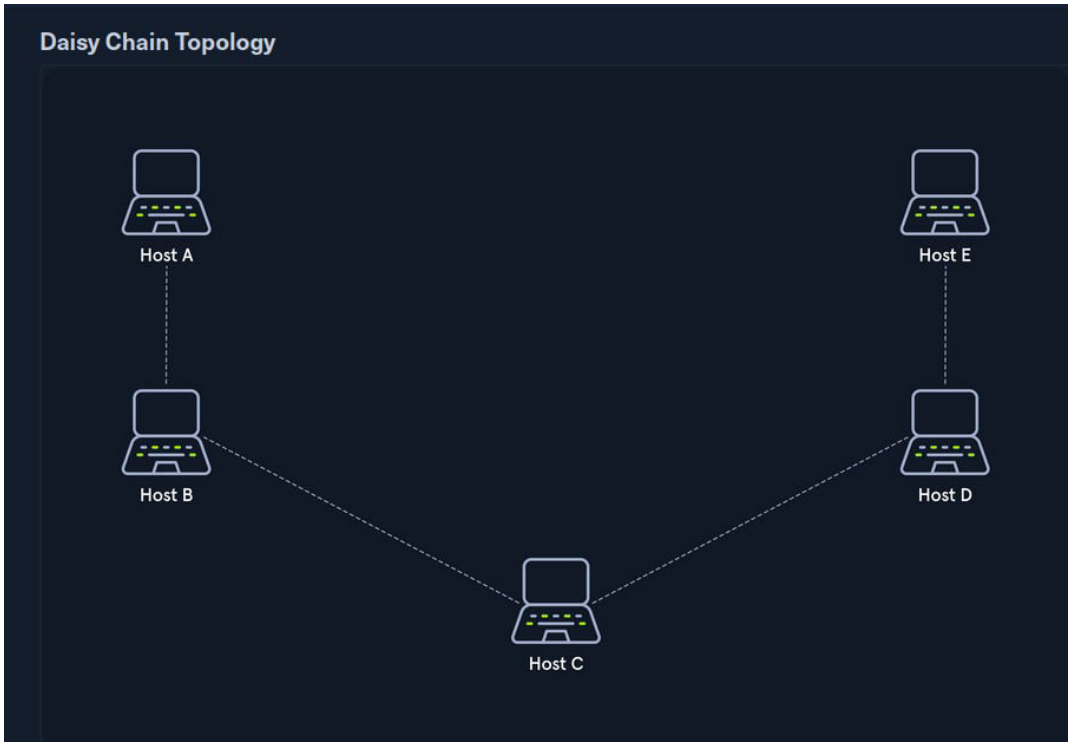
Hybrid networks combine two or more topologies so that the resulting network does not present any standard topologies. For example, a tree network can represent a hybrid topology in which star networks are connected via interconnected bus networks



Daisy Chain

In this topology, multiple hosts are connected by placing a cable from one node to another.

Daisy chain is also known as a **daisy-chain configuration** in which multiple hardware components are connected in a series. This type of networking is often found in automation technology (CAN).



Proxies

There are different opinions on what a proxy is.

Here are some of this opinions:-

- Security Professionals jump to HTTP Proxies (BurpSuite) or pivoting with a SOCKS/SSH Proxy (Chisel, ptunnel, sshuttle).

- Web Developers use proxies like Cloudflare or ModSecurity to block malicious traffic.

- Average people may think a proxy is used to obfuscate your location and access another country's Netflix catalog.

- Law Enforcement often attributes proxies to illegal activity.

A proxy is when a device or service sits in the middle of a connection and acts as a mediator. The mediator is the critical piece of information because it means the device in the middle must be able to inspect the contents of the traffic. Without the ability to be a mediator, the device is technically a gateway, not a proxy.

Proxies will almost always operate at Layer 7 of the OSI Model. There are many types of proxy services, but the key ones are:

- Dedicated Proxy / Forward Proxy

- Reverse Proxy

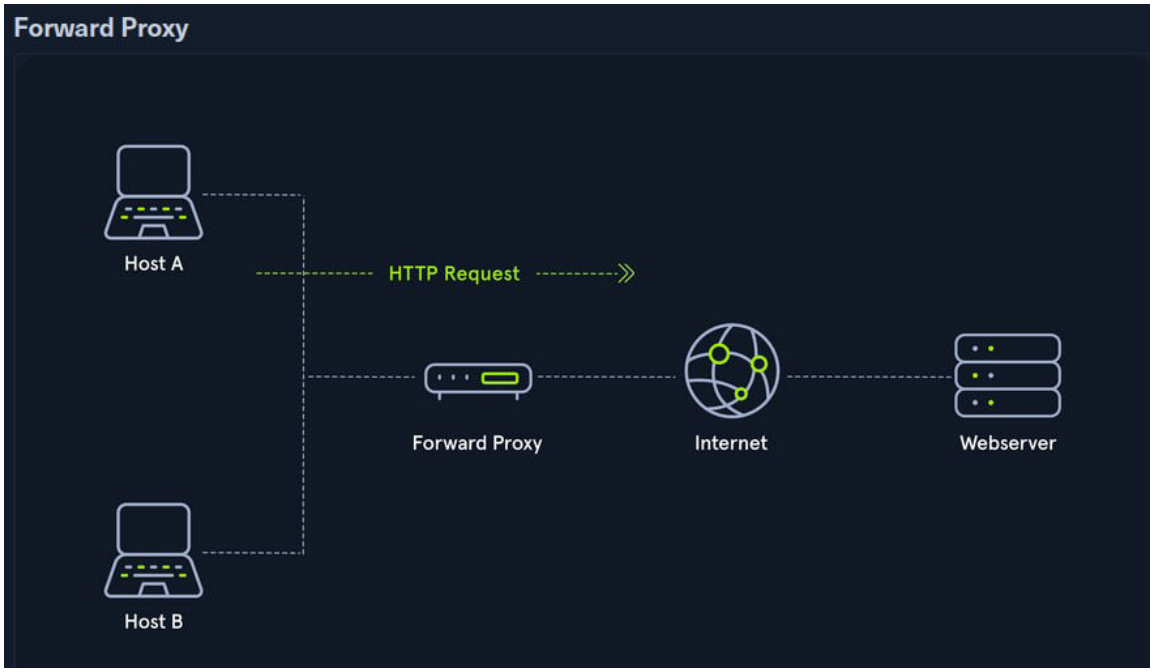
- Transparent Proxy

Dedicated Proxy / Forward Proxy

A Forward Proxy is when a client makes a request to a computer, and that computer carries out the request.

A good example explained was:-

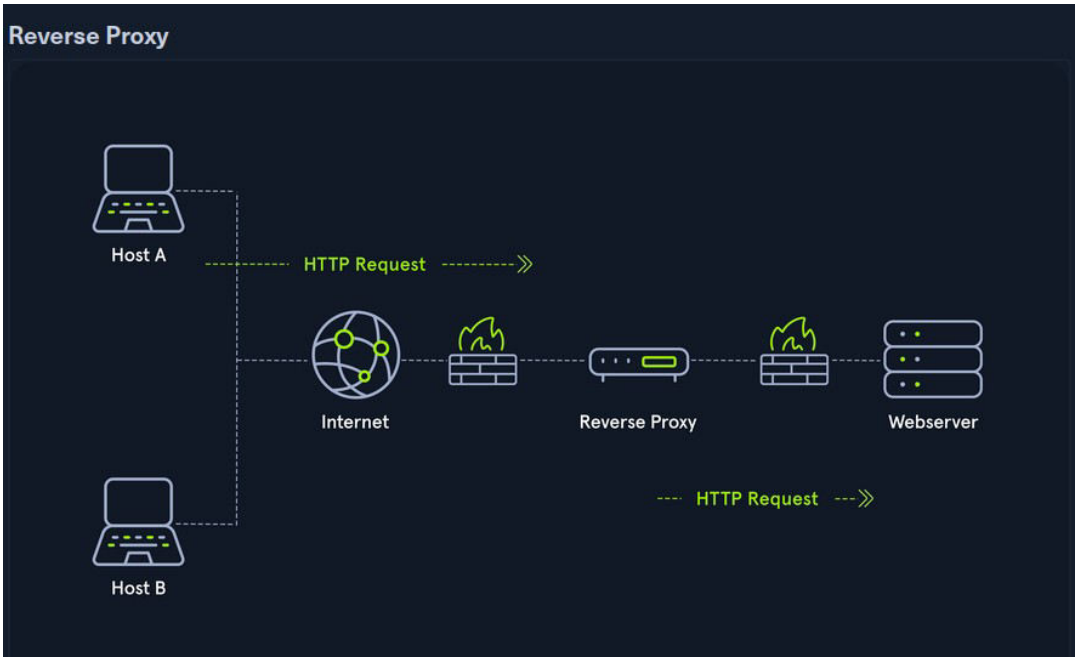
In the example where a corporate network, sensitive computers may not have direct access to the Internet. To access a website, they must go through a proxy (or web filter). This can be an incredibly powerful line of defense against malware, as not only does it need to bypass the web filter, but it would also need to be proxy aware or use a non-traditional C2 (a way for malware to receive tasking information).



Reverse Proxy

A reverse proxy, is the reverse of a Forward Proxy. Instead of being designed to filter outgoing requests, it filters incoming ones. The most common goal with a Reverse Proxy, is to listen on an address and forward it to a closed-off network.

In this section I learnt that many organizations use CloudFlare as they have a robust network that can withstand most DDOS Attacks. By using Cloudflare, organizations have a way to filter the amount (and type) of traffic that gets sent to their webservers.



(Non-) Transparent Proxy

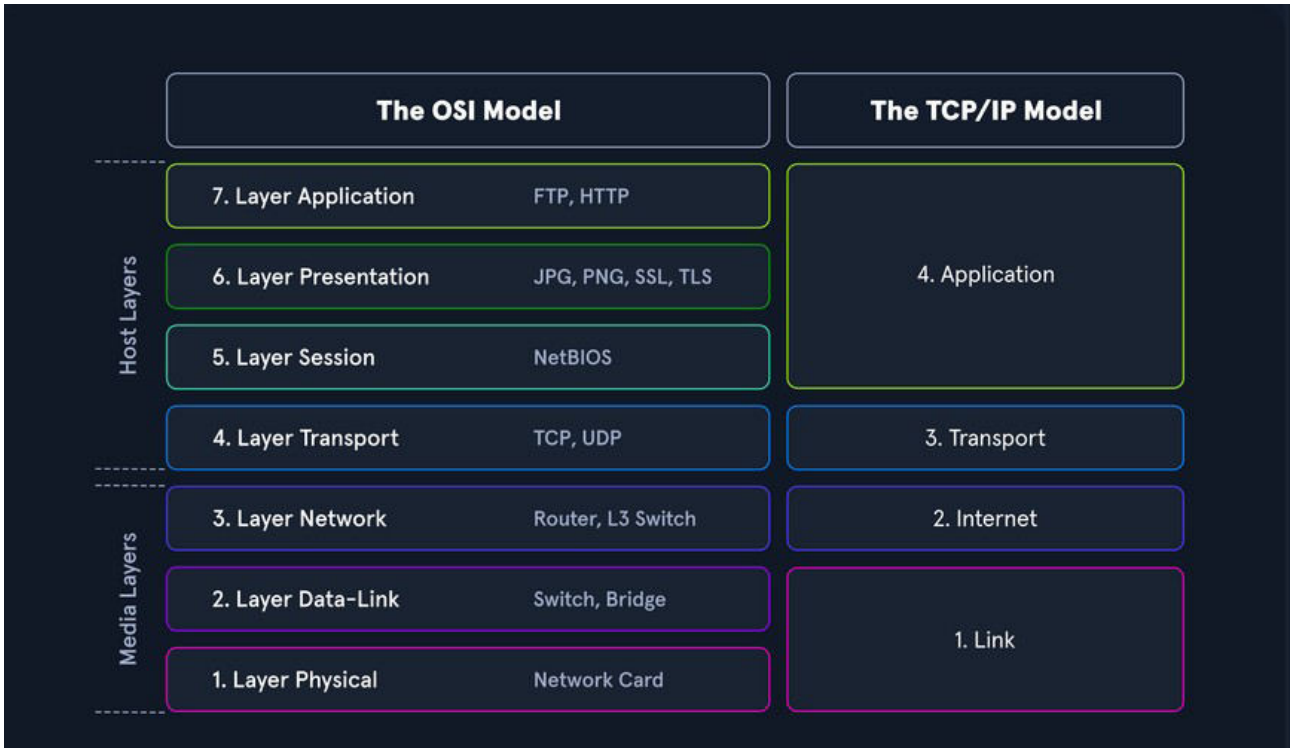
We have transparent and non-transparent proxies.

With a transparent proxy, the client doesn't know about its existence. The transparent proxy intercepts the client's communication requests to the Internet and acts as a substitute instance.

With a non-transparent proxy, we must be informed about its existence or the client has to know of its existence. For this purpose, we and the software we want to use are given a special proxy configuration that ensures that traffic to the Internet is first addressed to the proxy. If this configuration does not exist, we cannot communicate via the proxy.

Networking Models

In this section we discussed two major networking models this are the **ISO/OSI model** and the **TCP/IP model.**



The OSI Model

The OSI model, often referred to as ISO/OSI layer model, is a reference model that can be used to describe and define the communication between systems. The reference model has seven individual layers, each with clearly separated tasks.

The TCP/IP Model

TCP/IP (Transmission Control Protocol/Internet Protocol) is a generic term for many network protocols. The protocols are responsible for the switching and transport of data packets on the Internet. The Internet is entirely based on the TCP/IP protocol family. However, TCP/IP does not only refer to these two protocols but is usually used as a generic term for an entire protocol family.

ISO/OSI vs. TCP/IP

TCP/IP is a communication protocol that allows hosts to connect to the Internet. It refers to the Transmission Control Protocol used in and by applications on the Internet. In contrast to OSI, it allows a lightening of the rules that must be followed, provided that general guidelines are followed.

The OSI Model

The goal in defining the ISO/OSI standard was to create a reference model that enables the communication of different technical systems via various devices and technologies and provides compatibility. The OSI model uses seven different layers, this layers are:-

Layer 1

Physical Layer – This layer covers the transmission techniques used are, for example, electrical signals, optical signals, or electromagnetic waves. Through layer 1, the transmission takes place on wired or wireless transmission lines.

Layer 2

Data Link Layer - The central task of layer 2 is to enable reliable and error-free transmissions on the respective medium. For this purpose, the bitstreams from layer 1 are divided into blocks or frames.

Layer 3

Network Layer - On the networking layer, connections are established in circuit-switched networks, and data packets are forwarded in packet-switched networks. Data is transmitted over the entire network from the sender to the receiver.

Layer 4

Transport Layer – This layer is used for end-to-end control of the transferred data. The Transport Layer can detect and avoid congestion situations and segment data streams.

Layer 5

Session Layer - The session layer controls the logical connection between two systems and prevents, for example, connection breakdowns or other problems.

Layer 6

Presentation Layer - The presentation layer's task is to transfer the system-dependent presentation of data into a form independent of the application.

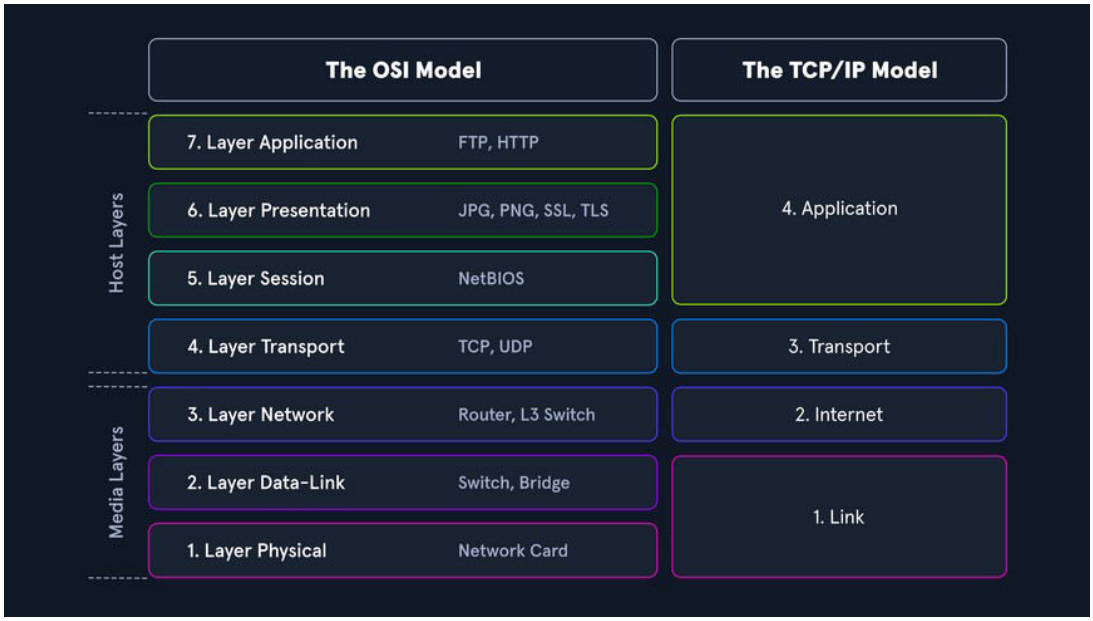
Layer 7

Application Layer – This is the last layer which controls the input and output of data and provides the application functions.

The TCP/IP Model

The TCP/IP model is also a layered reference model, often referred to as the Internet Protocol Suite.

The main difference between TCP/IP and OSI is the number of layers, some of which have been combined.



This model has 4 layers which are:-

1. Link Layer – This layer is responsible for placing the TCP/IP packets on the network medium and receiving corresponding packets from the network medium. TCP/IP is designed to work independently of the network access method, frame format, and medium.

2. Internet Layer is responsible for host addressing, packaging, and routing functions.

3. Transport Layer is responsible for providing (TCP) session and (UDP) datagram services for the Application Layer.

4. Application Layer allows applications to access the other layers' services and defines the protocols applications use to exchange data.

The most important tasks of TCP/IP are:-

1. Logical Addressing.

2. Routing.

3. Error and Control Flow.

4, Application Support.

5. Name Resolution.

IP Addresses

Every device has a **MAC (Media Access Control**) address for communications only in one network but If the remote host is located in another network, knowledge of the MAC address is not enough to establish a connection. Addressing on the Internet is done via the **IPv4 and/or IPv6** address, which is made up of the network address and the host address.

IPv4 / IPv6 - describes the unique postal address and district of the receiver's building.

MAC - describes the exact floor and apartment of the receiver.

IPv4 Structure

IPv4 is the most common method of assigning IP addresses.

IPv4 consists of a 32-bit binary number combined into 4 bytes consisting of 8-bit groups (octets) ranging from 0-255.

Thus an IPv4 address can look like this:

Notation	Presentation
Binary	0111 1111.0000 0000.0000 0000.0000 0001
Decimal	127.0.0.1

The IPv4 format allows 4,294,967,296 unique addresses. The IP address is divided into a host part and a network part. The router assigns the host part of the IP address at home or by an administrator. The respective network administrator assigns the network part.

The IP network blocks were divided into classes A - E. The different classes differed in the host and network shares' respective lengths. This classes are:-

Class	Network Address	First Address	Last Address	Subnetmask	CIDR	Subnets	IPs
A	1.0.0.0	1.0.0.1	127.255.255.255	255.0.0.0	/8	127	16,777,214 + 2
B	128.0.0.0	128.0.0.1	191.255.255.255	255.255.0.0	/16	16,384	65,534 + 2
C	192.0.0.0	192.0.0.1	223.255.255.255	255.255.255.0	/24	2,097,152	254 + 2
D	224.0.0.0	224.0.0.1	239.255.255.255	Multicast	Multicast	Multicast	Multicast
E	240.0.0.0	240.0.0.1	255.255.255.255	reserved	reserved	reserved	reserved

Subnet Mask

Subnettings helps to further separate the classes into small networks. This separation is done using the netmasks, which is as long as an IPv4 address. As with classes, it describes which bit positions within the IP address act as network part or host part.

Class	Network Address	First Address	Last Address	Subnetmask	CIDR	Subnets	IPs
A	1.0.0.0	1.0.0.1	127.255.255.255	255.0.0.0	/8	127	16,777,214 + 2
B	128.0.0.0	128.0.0.1	191.255.255.255	255.255.0.0	/16	16,384	65,534 + 2
C	192.0.0.0	192.0.0.1	223.255.255.255	255.255.255.0	/24	2,097,152	254 + 2
D	224.0.0.0	224.0.0.1	239.255.255.255	Multicast	Multicast	Multicast	Multicast
E	240.0.0.0	240.0.0.1	255.255.255.255	reserved	reserved	reserved	reserved

Broadcast Address

The broadcast IP address's task is to connect all devices in a network with each other. Broadcast in a network is a message that is transmitted to all participants of a network and does not require any response. In this way, a host sends a data packet to all other participants of the network simultaneously and, in doing so, communicates its IP address, which the receivers can use to contact it. This is the last IPv4 address that is used for the broadcast.

Class	Network Address	First Address	Last Address	Subnetmask	CIDR	Subnets	IPs
A	1.0.0.0	1.0.0.1	127.255.255.255	255.0.0.0	/8	127	16,777,214 + 2
B	128.0.0.0	128.0.0.1	191.255.255.255	255.255.0.0	/16	16,384	65,534 + 2
C	192.0.0.0	192.0.0.1	223.255.255.255	255.255.255.0	/24	2,097,152	254 + 2
D	224.0.0.0	224.0.0.1	239.255.255.255	Multicast	Multicast	Multicast	Multicast
E	240.0.0.0	240.0.0.1	255.255.255.255	reserved	reserved	reserved	reserved

Binary system

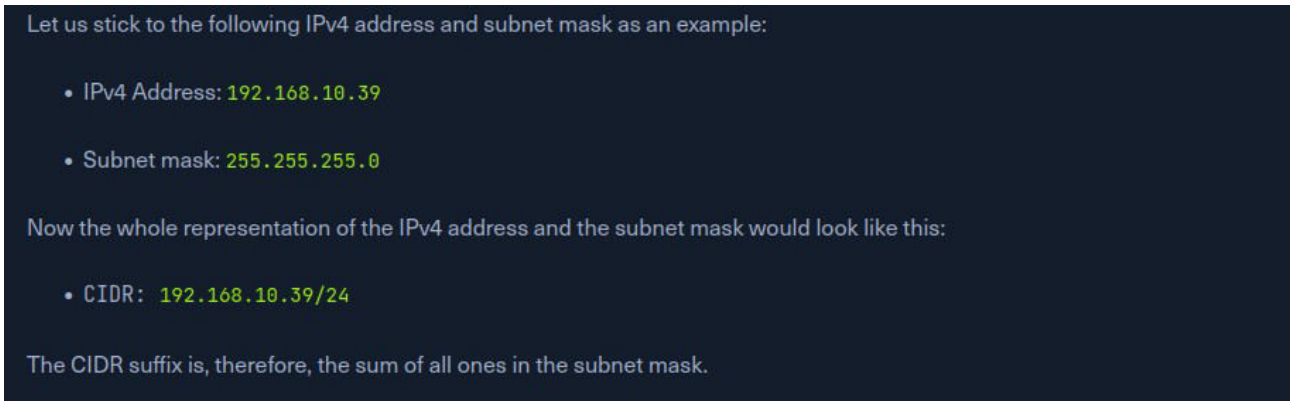
The binary system is a number system that uses only two different states that are represented into two numbers (0 and 1) opposite to the decimal-system (0 to 9).

An IPv4 address is divided into 4 octets, as we have already seen. Each octet consists of 8 bits. Each position of a bit in an octet has a specific decimal value.

IPv4 Address Example is:- 192.168.10.42

CIDR

CIDR is an abbreviation for **Classless Inter-Domain Routing** which is a method of representation and replaces the fixed assignment between IPv4 address and network classes (A, B, C, D, E). The division is based on the subnet mask or the so-called CIDR suffix, which allows the bitwise division of the IPv4 address space and thus into subnets of any size. The CIDR suffix indicates how many bits from the beginning of the IPv4 address belong to the network.



Subnetting

Subnetting is the division of an address range of IPv4 addresses into several smaller address ranges. A subnet is a logical segment of a network that uses IP addresses with the same network address.

With the help of subnetting, we can create a specific subnet by ourselves or find out the following outline of the respective network:

- Network address

- Broadcast address

- First host

- Last host

- Number of hosts

Questions

Submit the decimal representation of the subnet mask from the following CIDR: 10.200.20.0/27

ANS: 255.255.255.224

Submit the broadcast address of the following CIDR: 10.200.20.0/27

ANS: 10.200.20.31

Split the network 10.200.20.0/27 into 4 subnets and submit the network address of the 3rd subnet as the answer.

ANS: 10.200.20.16

Split the network 10.200.20.0/27 into 4 subnets and submit the broadcast address of the 2nd subnet as the answer.

ANS: 10.200.20.15

MAC Addresses

Every host in a network has its own 48-bit (6 octets) Media Access Control (MAC) address, represented in hexadecimal format. MAC is the physical address for our network interfaces. There are several different standards for the MAC address:

- Ethernet (IEEE 802.3)

- Bluetooth (IEEE 802.15)

- WLAN (IEEE 802.11)

How mac addresses look like:-

- DE:AD:BE:EF:13:37
- DE-AD-BE-EF-13-37
- DEAD.BEEF.1337

There exist several attack vectors that can potentially be exploited through the use of MAC addresses:

1. MAC spoofing -This involves altering the MAC address of a device to match that of another device, typically to gain unauthorized access to a network.

2. MAC flooding - This involves sending many packets with different MAC addresses to a network switch, causing it to reach its MAC address table capacity and effectively preventing it from functioning correctly.

3. MAC address filtering - Some networks may be configured only to allow access to devices with specific MAC addresses that we could potentially exploit by attempting to gain access to the network using a spoofed MAC address.

Address Resolution Protocol

ARP is an important part of the network communication process because it allows devices to send and receive data using MAC addresses rather than IP addresses, which can be more efficient.

There are two types of request messages can be used:-

- ARP Request.

- ARP Reply.

ARP Request

When a device wants to communicate with another device on a LAN, it sends an ARP request to resolve the destination device's IP address to its MAC address. The request is broadcast to all devices on the LAN and contains the IP address of the destination device. The device with the matching IP address responds with its MAC address.

ARP Reply

When a device receives an ARP request, it sends an ARP reply to the requesting device with its MAC address. The reply message contains the IP and MAC addresses of both the requesting and the responding devices.

In this section I learnt of a few tools that is Ettercap or Cain & Abel which can send an attack called

ARP spoofing which is also refered to as ARP cache poisoning or ARP poison routing by sending falsified ARP messages over a LAN with the goal to associate our MAC address with the IP address of a legitimate device on the company's network, effectively allowing us to intercept traffic intended for the legitimate device.

IPv6 Addresses

IPv6 is the successor of IPv4 which In contrast to IPv4, the IPv6 address is 128 bit long.

IPv6 consistently follows the end-to-end principle and provides publicly accessible IP addresses for any end devices without the need for NAT.

IPv6 is a protocol with many new features, which also has many other advantages over IPv4:

- Larger address space

- Address self-configuration (SLAAC)

- Multiple IPv6 addresses per interface

- Faster routing

- End-to-end encryption (IPsec)

- Data packages up to 4 GByte

Features	IPv4	IPv6
Bit length	32-bit	128 bit
OSI layer	Network Layer	Network Layer
Adressing range	~ 4.3 billion	~ 340 undecillion
Representation	Binary	Hexadecimal
Prefix notation	10.10.10.0/24	fe80::dd80:b1a9:6687:2d3b/64
Dynamic addressing	DHCP	SLAAC / DHCPv6
IPsec	Optional	Mandatory

There are four different types of IPv6 addresses:

1. Unicast - Addresses for a single interface.

2. Anycast - Addresses for multiple interfaces, where only one of them receives the packet.

3. Multicast - Addresses for multiple interfaces, where all receive the same packet.

4. Broadcast - Do not exist and is realized with multicast addresses.

An IPv6 address consists of 16 bytes and is represented in a hexadecimal notation. Therefore the 128 bits are divided into 8 blocks multiplied by 16 bits (or 4 hex numbers).

How an IPv6 looks like in full and in short form.

An IPv6 address can look like this:

- Full IPv6: `fe80:0000:0000:0000:dd80:b1a9:6687:2d3b/64`
- Short IPv6: `fe80::dd80:b1a9:6687:2d3b/64`

Networking Key Terminology

In this section we looked at various protocols that are used in the field of information technology, some I already had come through but to some this was the first time to come across them, such as:-

- TKIP (Temporal Key Integrity Protocol) which is a security protocol used in wireless networks but less secure.

- PGP (Pretty Good Privacy) which is an encryption program that is used to secure emails, files, and other types of data.

- EIGRP (Enhanced Interior Gateway Routing Protocol) which is an advanced distance-vector routing protocol that is used to route IP traffic within a network.

- MBSA (Microsoft Baseline Security Analyzer) which is a free security tool from Microsoft that is used to detect potential security vulnerabilities in Windows computers, networks, and systems.

Among many other protocols.

Protocol	Acronym	Description
Wired Equivalent Privacy	WEP	WEP is a type of security protocol that was commonly used to secure wireless networks.
Secure Shell	SSH	A secure network protocol used to log into and execute commands on a remote system
File Transfer Protocol	FTP	A network protocol used to transfer files from one system to another
Simple Mail Transfer Protocol	SMTP	A protocol used to send and receive emails
Hypertext Transfer Protocol	HTTP	A client-server protocol used to send and receive data over the internet

Common Protocols

The two main types of connections or protocols used on networks are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

Transmission Control Protocol

TCP is a connection-oriented protocol that establishes a virtual connection between two devices before transmitting data by using a Three-Way-Handshake. This connection is maintained until the data transfer is complete, and the devices can continue to send data back and forth as long as the connection is active.

TCP connections between the browser and the web server and maintained until the data transfer is complete. As a result, TCP is reliable but slower than UDP because it requires additional overhead for establishing and maintaining the connection.

Protocol	Acronym	Port	Description
Telnet	Telnet	23	Remote login service
Secure Shell	SSH	22	Secure remote login service
Simple Network Management Protocol	SNMP	161-162	Manage network devices
Hyper Text Transfer Protocol	HTTP	80	Used to transfer webpages
Hyper Text Transfer Protocol Secure	HTTPS	443	Used to transfer secure webpages
Domain Name System	DNS	53	Lookup domain names
File Transfer Protocol	FTP	20-21	Used to transfer files
Trivial File Transfer Protocol	TFTP	69	Used to transfer files
Network Time Protocol	NTP	123	Synchronize computer clocks
Simple Mail Transfer Protocol	SMTP	25	Used for email transfer
Post Office Protocol	POP3	110	Used to retrieve emails
Internet Message Access Protocol	IMAP	143	Used to access emails
Server Message Block	SMB	445	Used to transfer files
Network File System	NFS	111, 2049	Used to mount remote systems
Bootstrap Protocol	BOOTP	67, 68	Used to bootstrap computers

User Datagram Protocol

UDP is a connectionless protocol, which means it does not establish a virtual connection before transmitting data. Instead, it sends the data packets to the destination without checking to see if they were received.

UDP is faster than TCP but less reliable because there is no guarantee that the packets will reach their destination.

Protocol	Acronym	Port	Description
Domain Name System	DNS	53	It is a protocol to resolve domain names to IP addresses.
Trivial File Transfer Protocol	TFTP	69	It is used to transfer files between systems.
Network Time Protocol	NTP	123	It synchronizes computer clocks in a network.
Simple Network Management Protocol	SNMP	161	It monitors and manages network devices remotely.
Routing Information Protocol	RIP	520	It is used to exchange routing information between routers.
Internet Key Exchange	IKE	500	Internet Key Exchange
Bootstrap Protocol	BOOTP	68	It is used to bootstrap hosts in a network.
Dynamic Host Configuration Protocol	DHCP	67	It is used to assign IP addresses to devices in a network dynamically.
Telnet	TELNET	23	It is a text-based remote access communication protocol.
MySQL	MySQL	3306	It is an open-source database management system.
Terminal Server	TS	3389	It is a remote access protocol used for Microsoft Windows Terminal Services by default.
NetBIOS Name	netbios-ns	137	It is used in Windows operating systems to resolve NetBIOS names to IP addresses on a LAN.

Wireless Networks

Wireless networks are computer networks that use wireless data connections between network nodes. These networks allow devices such as laptops, smartphones, and tablets to communicate with each other and the Internet without needing physical connections such as cables.

Wireless networks use radio frequency (RF) technology to transmit data between devices.

A good example for a wireless Network is the WIFI (Wireless Fidelity)

Although WIFI is very convenient it has some security concerns as well.

To solve some of those security concerns, this are some of the security features used:-

- Encryption of data

- Access Control and Monitoring

- Firewall utilization.

Encryption

The most common encryption algorithms in WiFi networks are Wired Equivalent Privacy (WEP), WiFi Protected Access 2 (WPA2), and WiFi Protected Access 3 (WPA3).

Access Control

WiFi networks by default are configured to allow authorized devices to join the network using specific authentication methods. However, these methods can be changed by requiring a password or a unique identifier (such as a MAC address) to identify authorized devices.

Firewall

A firewall is a security system that controls incoming and outgoing network traffic based on predetermined security rules. For example, WiFi routers often have built-in firewalls that can block incoming traffic from the Internet and protect against various types of cyber threats.

Encryption Protocols

Wired Equivalent Privacy (WEP) and WiFi Protected Access (WPA) are encryption protocols that secure data transmitted over a WiFi network.

The longer the key used in encryption, the more the protocol is termed to be secure.

WEP uses a 40-bit or 104-bit key to encrypt data, while WPA using AES uses a 128-bit key.

WEP

WEP uses a shared key for authentication, which means the same key is used for encryption and authentication. There are two versions of the WEP protocol which are:-

- WEP-40/WEP-64

- WEP-104

Protocol	IV	Secret Key
WEP-40/WEP-64	24-bit	40-bit
WEP-104	24-bit	80-bit

WPA

WPA provides the highest level of security and is not susceptible to the same types of attacks as WEP. In addition, WPA uses more secure authentication methods, such as a Pre-Shared Key (PSK) or an 802.1X authentication server, which provide stronger protection against unauthorized access.

WPA provides strong encryption and authentication for wireless communications, helping protect against unauthorized network access and sensitive data interception. WPA includes two main versions:

- WPA-Personal

- WPA-Enterprise

WPA-Personal, are designed for home and small business networks, while WPA-Enterprise, are designed for larger organizations and uses a centralized authentication server such as RADIUS or TACACS+ to verify the identity of clients.

Virtual Private Networks

A Virtual Private Network (VPN) is a technology that allows a secure and encrypted connection between a private network and a remote device. This allows the remote machine to access the private network directly, providing secure and confidential access to the network's resources and services.

There are several components and requirements that are necessary for a VPN to work, this components are:-

Requirement	Description
VPN Client	This is installed on the remote device and is used to establish and maintain a VPN connection with the VPN server. For example, this could be an OpenVPN client.
VPN Server	This is a computer or network device responsible for accepting VPN connections from VPN clients and routing traffic between the VPN clients and the private network.
Encryption	VPN connections are encrypted using a variety of encryption algorithms and protocols, such as AES and IPsec, to secure the connection and protect the transmitted data.
Authentication	The VPN server and client must authenticate each other using a shared secret, certificate, or another authentication method to establish a secure connection.

Key Exchange Mechanisms

Key exchange methods are used to exchange cryptographic keys between two parties securely.

We then proceeded to look at some of the key exchange used:-

Diffie-Hellman (Diffie-Hellman key exchange)

This is one of the common key exchange methods which allows two parties to agree on a shared secret key without any prior communication or shared private information. It is based on the concept of two parties generating a shared secret key that can be used to encrypt and decrypt messages between them.

This key is often used as the basis for establishing secure communication channels, such as in the Transport Layer Security (TLS) protocol that is used to protect web traffic.

Limitations:

1. Vulnerable to MITM or Man In The Middle attacks - MITM attack, we intercept the communication between the two parties and pretend to be one of the parties, generating a different secret key and tricking both parties into using it. This allows the attacker to read and modify the messages sent between the parties.

2. **Large CPU power utilization** to generate shared secret key.

RSA

Another key exchange method is the Rivest–Shamir–Adleman (RSA) algorithm, which uses the properties of large prime numbers to generate a shared secret key.

This key is widely used in many application and protocols that require secure communication and data protection, they can be used in protecting data in transit over networks, such as in the Secure Socket Layer (SSL) and TLS protocols, encrypting and signing messages to provide confidentiality and authentication among many other various applications.

ECDH

Elliptic curve Diffie-Hellman (ECDH) is a variant of Diffie-Hellman key exchange that uses elliptic curve cryptography to generate the shared secret key.

ECDH has the advantage of being more efficient and secure than the original Diffie-Hellman algorithm.

ECDSA

The Elliptic Curve Digital Signature Algorithm (ECDSA) uses elliptic curve cryptography to generate digital signatures that can authenticate the parties involved in the key exchange.

Internet Key Exchange

Internet Key Exchange (IKE) is a protocol used to establish and maintain secure communication sessions, such as those used in VPNs. It uses a combination of the Diffie-Hellman key exchange algorithm and other cryptographic techniques to securely exchange keys and negotiate security parameters.

This key is a major component to many VPN solutions.

Pre-Shared Keys

A Pre-Shared Key (PSK) is a secret value shared between the two parties involved in the key exchange. This key is used to authenticate the parties and establish a shared secret that encrypts subsequent communication

Authentication Protocols

There are a number of authentication protocols in Information Technologies which are used in different systems. These protocols are essential because they provide a secure and standardized way of verifying the identity of users, devices, and other entities in a network. Without authentication protocols, it would be difficult to securely and reliably identify entities in a network, making it easy for attackers to gain unauthorized access and potentially compromise the network.

In this section we looked at a number of authentication protocols, here are some of them:-

Protocol	Description
Kerberos	Key Distribution Center (KDC) based authentication protocol that uses tickets in domain environments.
SRP	This is a password-based authentication protocol that uses cryptography to protect against eavesdropping and man-in-the-middle attacks.
SSL	A cryptographic protocol used for secure communication over a computer network.
TLS	TLS is a cryptographic protocol that provides communication security over the internet. It is the successor to SSL.
OAuth	An open standard for authorization that allows users to grant third-party access to their web resources without sharing their passwords.
OpenID	OpenID is a decentralized authentication protocol that allows users to use a single identity to sign in to multiple websites.
SAML	Security Assertion Markup Language is an XML-based standard for securely exchanging authentication and authorization data between parties.
2FA	An authentication method that uses a combination of two different factors to verify a user's identity.
FIDO	The Fast IDentity Online Alliance is a consortium of companies working to develop open standards for strong authentication.
PKI	PKI is a system for securely exchanging information based on the use of public and private keys for encryption and digital signatures.
SSO	An authentication method that allows a user to use a single set of credentials to access multiple applications.
MFA	MFA is an authentication method that uses multiple factors, such as something the user knows (a password), something the user has (a phone), or something the user is (biometric data), to verify their identity.
PAP	A simple authentication protocol that sends a user's password in clear text over the network.

Although all this authentication protocols are used I think the most common is the HTTPS, SSL, SSH and Kerberos maybe.

TCP/UDP Connections

TCP

As disussed earlier TCP is a connection-oriented protocol that establishes a virtual connection between two devices before transmitting data by using a Three-Way-Handshake. This connection is maintained until the data transfer is complete, and the devices can continue to send data back and forth as long as the connection is active.

TCP reliable and slower than UDP because more time is required for transmission and error recovery.

UDP

UDP is a connectionless protocol, which means it does not establish a virtual connection before transmitting data. Instead, it sends the data packets to the destination without checking to see if they were received.

UDP is faster than TCP but less reliable because there is no guarantee that the packets will reach their destination.

IP Packet

An IP packet is the data area used by the network layer of the Open Systems Interconnection (OSI) model to transmit data from one computer to another.

IP Packet consists of a header and the payload, the actual payload data.

IP header of an IP packet contains several fields that have important information. This information includes:-

Field	Description
Version	Indicates which version of the IP protocol is being used
Internet Header Length	Indicates the size of the header in 32-bit words
Class of Service	Means how important the transmission of the data is
Total length	Specifies the total length of the packet in bytes
Identification (ID)	Is used to identify fragments of the packet when fragmented into smaller parts
Flags	Used to indicate fragmentation
Fragment Offset	Indicates where the current fragment is placed in the packet
Time to Live	Specifies how long the packet may remain on the network
Protocol	Specifies which protocol is used to transmit the data, such as TCP or UDP
Checksum	Is used to detect errors in the header
Source/Destination	Indicate where the packet was sent from and where it is being sent to
Options	Contain optional information for routing
Padding	Pads the packet to a full word length

Cryptography

This was the very last section we looked in this module about cryptography which is the process of hiding or coding information so that only the person a message was intended for can read it.

During the transmission of data on the internet such as payment information, e-mails or personal data, encryption of this data is required which is done using various cryptographic algorithms based on mathematical operations.

We have Digital keys in **symmetric or asymmetric** encryption processes being used for encryption.

Symmetric Encryption

Symmetric encryption, also known as secret key encryption, is a method that uses the same key to encrypt and decrypt the data. This means the sender and the receiver must have the same key to decrypt the data correctly.

Asymmetric Encryption

Asymmetric encryption, also known as public-key encryption, is a method of encryption that uses two different keys:

- A public key

- A private key

In this case the public key is used to encrypt the data, while the private key is used to decrypt the data. This means anyone can use a public key to encrypt data for someone, but only the recipient with the associated private key can decrypt the data.

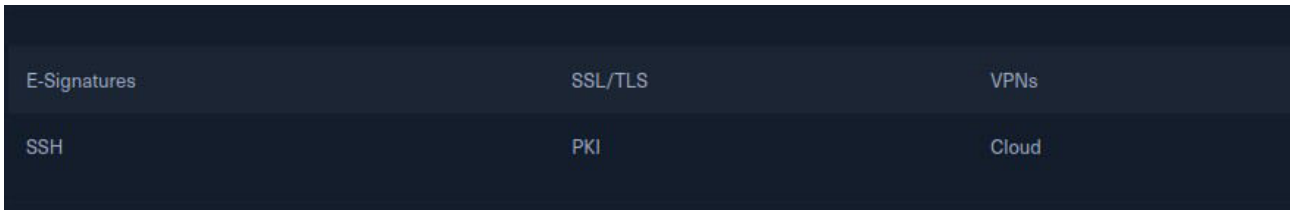
Asymmetric encryption methods are used in various areas such as:-

- Rivest–Shamir–Adleman (RSA)

- Pretty Good Privacy (PGP)

- Elliptic Curve Cryptography (ECC)

Other areas of application:-



Public-Key Encryption

public keys can be accessible to everyone, there is no need to exchange keys secretly.

Data Encryption Standard

DES is a symmetric-key block cipher, and its encryption works as a combination of the one-time pad, permutation, and substitution ciphers applied to bit sequences. It uses the same key in both encrypting and decrypting data.

The key consists of 64 bits, with 8 bits used as a checksum. Therefore, the actual key length of DES is only 56 bits.

Triple DES / 3DES – This is an extension of DES which encrypts data more securely. It consists of three keys, with the first key being used to encrypt the data, the second to decrypt the data, and the third to encrypt the data again.

Cipher Modes

This refers to how a block cipher encrypts plain text messages.

A block cipher algorithm will encrypt data, each using fixed-size blocks of data usually 64 or 128 bits while a cipher mode defines how these blocks are processed and combined to encrypt a message of any length.

common cipher modes include:-

Cipher Mode	Description
Electronic Code Book (ECB) mode	ECB mode is generally not recommended for use due to its susceptibility to certain types of attacks. Furthermore, it does not hide data patterns efficiently. As a result, statistical analysis can reveal elements of clear-text messages, for example, in web applications.
Cipher Block Chaining (CBC) mode	CBC mode is generally used to encrypt messages like disk encryption and e-mail communication. This is the default mode for AES and is also used in software like TrueCrypt, VeraCrypt, TLS, and SSL.
Cipher Feedback (CFB) mode	CFB mode is well suited for real-time encryption of a data stream, e.g., network communication encryption or encryption/decryption of files in transit like Public-Key Cryptography Standards (PKCS) and Microsoft's BitLocker.
Output Feedback (OFB) mode	OFB mode is also used to encrypt a data stream, e.g., to encrypt real-time communication. However, this mode is considered better for the data stream because of how the key stream is generated. We can find this mode in PKCS but also in the SSH protocol.
Counter (CTR) mode	CTR mode encrypts real-time data streams AES uses, e.g., network communication, disk encryption, and other real-time scenarios where data is processed. An example of this would be IPsec or Microsoft's BitLocker.
Galois/Counter (GCM) mode	GCM is used in cases where confidentiality and integrity need to be protected together, such as wireless communications, VPNs, and other secure communication protocols.

In conclusion to this section we are told the chose on which encryption mode to use depends on the application's requirements and the security objectives to be achieved and that every mode has its characteristics which is more suitable for certain use cases depending on others.

Conclusions

Introduction to Networking in depth course work has laid out the whole topology or the overview of how the Networking environment looks like and how it functions. I belief its a necessary foundation to anyone with the interest to be a security analyst.

This module has highlighted a few security benefits in some network protocols and also their attached limitations, giving me an overview of the networks I should suggest to a client in the case I get the opportunity to advice one, I have learnt a few benefits and limitations to some of those protocols.

This module has also introduced new terms that I did not know before but I belief with the foundational knowledge I have gained, as I continue to interact with networking, this terms will not be so new to me again.

In my conclusion I a grateful to Hack The Box team for compiling such informative information to us as students and also to the Cyber Shujaa program for referencing me to this resources I have gained a lot.

Thank You.