Contents

[CHAPTER 1 3](#_Toc151295419)

[NETWORK TOPOLOGIES 3](#_Toc151295420)

[HALF-DUPLEX VS FULL-DUPLEX 4](#_Toc151295421)

[DIFFERENT NETWORK TYPES 4](#_Toc151295422)

[VLAN 5](#_Toc151295423)

[BROADBAND CABLE VS DSL VS FIBER INTERNET 6](#_Toc151295424)

[CHAPTER 2 7](#_Toc151295425)

[HDMI, DISPLAYPORT, DVI, VGA, THUNDERBOLT - VIDEO PORT COMPARISON 7](#_Toc151295426)

[USB PORTS, CABLES, TYPES, & CONNECTORS 8](#_Toc151295427)

[ETHERNET CABLES, UTP VS STP, STRAIGHT VS CROSSOVER, CAT 5,5E,6,7,8 9](#_Toc151295428)

[NETWORK CONNECTORS 10](#_Toc151295429)

[NETWORKING TOOLS 12](#_Toc151295430)

[CHAPTER 3 14](#_Toc151295431)

[PUBLIC VS PRIVATE IP 14](#_Toc151295432)

[IPV4 VS IPV6 16](#_Toc151295433)

[SUBNET MASK 17](#_Toc151295434)

[NAT 17](#_Toc151295435)

[DHCP 18](#_Toc151295436)

[APIPA 19](#_Toc151295437)

[DNS 20](#_Toc151295438)

[DDNS - DYNAMIC DNS EXPLAINED 21](#_Toc151295439)

[CHAPTER 4 22](#_Toc151295440)

[MAC ADDRESS 22](#_Toc151295441)

[NETWORK PORTS 23](#_Toc151295442)

[PORT FORWARDING 24](#_Toc151295443)

[CHAPTER 5 25](#_Toc151295444)

[NETWORK DEVICES: HUBS, SWITCHES, AND ROUTERS 25](#_Toc151295445)

[BLUETOOTH VS WIFI 25](#_Toc151295446)

[HOTSPOT 26](#_Toc151295447)

[DEFAULT GATEWAY 28](#_Toc151295448)

[WIRELESS ACCESS POINT VS WI-FI ROUTER 28](#_Toc151295449)

[MESH WIFI EXPLAINED 30](#_Toc151295450)

[GUEST NETWORK 31](#_Toc151295451)

[2.4 GHZ VS 5 GHZ WIFI 31](#_Toc151295452)

[WIFI PASSWORD SECURITY 32](#_Toc151295453)

[POWER OVER ETHERNET (POE) 33](#_Toc151295454)

[CHAPTER 6 34](#_Toc151295455)

[WHAT IS A SERVER? 34](#_Toc151295456)

[TELNET VS SSH 35](#_Toc151295457)

[RAID 36](#_Toc151295458)

[FULL VS INCREMENTAL VS DIFFERENTIAL BACKUP 37](#_Toc151295459)

[PATCH PANELS 38](#_Toc151295460)

[PROXY SERVERS 38](#_Toc151295461)

[PROXY VS REVERSE PROXY 39](#_Toc151295462)

[VPN 40](#_Toc151295463)

[FIREWALL 41](#_Toc151295464)

[DMZ 41](#_Toc151295465)

[VIRTUALIZATION EXPLAINED 42](#_Toc151295466)

[VIRTUAL MACHINES VS CONTAINERS 43](#_Toc151295467)

[CLOUD COMPUTING 44](#_Toc151295468)

[NAS VS SAN - NETWORK ATTACHED STORAGE VS STORAGE AREA NETWORK 45](#_Toc151295469)

[CHAPTER 7 46](#_Toc151295470)

[ARP (ADDRESS RESOLUTION PROTOCOL) EXPLAINED 46](#_Toc151295471)

[TCP VS UDP 46](#_Toc151295472)

[HTTP, HTTPS & SSL 47](#_Toc151295473)

[FTP, SFTP, AND TFTP Protocols 48](#_Toc151295474)

[SMTP - SIMPLE MAIL TRANSFER PROTOCOL 49](#_Toc151295475)

[POP3 VS. IMAP 50](#_Toc151295476)

[DDOS ATTACK 51](#_Toc151295477)

[RANDOM 52](#_Toc151295478)

# CHAPTER 1

## NETWORK TOPOLOGIES

Now a topology is the layout of how a network communicates with different devices.

I. WIRED TOPOLOGIES:

1. STAR TOPOLOGY:

Computers connected to a central point (hub or switch).

Individual cable connections for each computer.

Advantages: Fault isolation for individual computers.

Disadvantages: Single point of failure if the central hub/switch fails.

2. RING TOPOLOGY:

Computers connected in a closed loop or ring.

Easy installation and troubleshooting.

Disadvantages: Disruption if a computer or cable fails.

3. BUS TOPOLOGY:

Computers and devices share a single cable or backbone.

Cheap and easy to implement.

Requires terminators to prevent signal reflection and disruptions.

4. MESH TOPOLOGY:

Every computer connected to every other computer.

High redundancy, handles failures well.

Expensive, mainly used in wide area networks (e.g., the internet).

II. WIRELESS TOPOLOGIES:

1. INFRASTRUCTURE TOPOLOGY:

Combination of wired and wireless devices.

Wired devices connected to a switch, wireless devices connect through access points.

Enables wireless communication while maintaining a wired backbone.

2. AD HOC TOPOLOGY:

Simple peer-to-peer wireless network.

No reliance on infrastructure, each device responsible for security.

Quick setup for sharing data without an existing network.

3. WIRELESS MESH TOPOLOGY:

Devices wirelessly interconnected.

Multiple access points communicate to create a seamless internet connection.

Redundant, as data can be rerouted even if some access points fail.

## HALF-DUPLEX VS FULL-DUPLEX

HALF-DUPLEX NETWORKING

In a half-duplex network, two devices are connected using a point-to-point system.

Communication can occur in both directions but only one at a time.

The analogy of walkie-talkies is used to illustrate the concept, emphasizing the need to take turns in transmitting and receiving data.

Data flows in one direction at a time.

Waiting periods between transmissions, akin to pressing a button on a walkie-talkie.

The comparison is drawn to cars on a single-lane highway, where collisions may occur, necessitating a "traffic cop" known as CSMA/CD (Carrier Sense Multiple Access with Collision Detection).

FULL-DUPLEX NETWORKING

In a full-duplex network, devices can communicate in both directions simultaneously.

Double the bandwidth compared to half-duplex.

The analogy of a telephone conversation is used, where talking and listening happen concurrently.

Described as a two-lane highway where each lane is dedicated to a specific direction, eliminating the need for a "traffic cop."

Full-duplex networks are the standard in modern networking, offering simultaneous bidirectional communication and higher bandwidth.

Half-duplex networks are associated with older legacy equipment and are less commonly used in contemporary networking.

## DIFFERENT NETWORK TYPES

1. Personal Area Network (PAN)

Definition: A PAN, or Personal Area Network, is a small-scale network for personal devices like smartphones and laptops.

Connectivity: PANs utilize wireless technologies (Bluetooth, infrared, NFC) and may employ wired connections like USB cables.

Purpose: Primarily used for transferring small files (e.g., music, photos, calendar appointments).

2. Local Area Network (LAN)

Definition: A LAN, or Local Area Network, involves devices like computers and printers within the same building or close proximity.

Common Type: Ethernet LAN, where devices connect via Ethernet cables and a switch.

Wireless Alternative: WLAN (Wireless LAN) replaces wired communication with wireless, typically facilitated by a Wi-Fi router.

3. Campus Area Network (CAN)

Definition: CAN, or Campus Area Network, connects multiple LANs within a limited area, like different departments in a university.

Structure: Buildings with individual LANs are interconnected to form a larger campus area network.

4. Metropolitan Area Network (MAN)

Definition: A MAN, or Metropolitan Area Network, spans multiple buildings in a city or town.

Connectivity: MANs use high-speed connections like fiber optic cables.

Purpose: Enables sharing of data and resources within a city or town.

5. Storage Area Network (SAN)

Definition: A SAN, or Storage Area Network, is a high-speed network dedicated to storing and providing access to large amounts of data.

Components: Includes disk arrays, switches, and servers.

Advantages: SANs are isolated from local area networks, avoiding traffic-related issues.

6. Wide Area Network (WAN)

Definition: The WAN, or Wide Area Network, is the largest network type, encompassing multiple LANs, CANs, and MANs.

Geographical Scale: Spans large areas, such as countries, continents, or the entire globe.

Example: The internet serves as a prime example of a wide area network.

## VLAN

VLAN stands for Virtual Local Area Network.

It is a logical network where devices are connected regardless of physical location.

VLANs are created to enhance security, traffic management, and simplify network architecture.

In a scenario with multiple departments on the same floor, all connected to a switch, network broadcast traffic is mixed.

Different departments can see each other's network traffic, posing security and management challenges.

VLANs provide a solution without physically relocating devices.

They logically group devices into separate virtual networks for each department.

Example: Three-story office building with accounting, shipping, and support departments.

VLANs are created for each department to isolate network broadcast traffic.

VLANs are implemented on VLAN-capable switches.

Specific ports on the switch are designated for each department and assigned to corresponding VLANs.

Computers from the same department are connected to the designated ports.

VLANs isolate traffic between departments, enhancing security and reducing congestion.

VLANs are crucial for traffic management as local area networks expand with more devices.

VLANs offer an efficient solution to segregate network traffic logically.

They address security concerns, simplify network management, and manage broadcast traffic effectively in growing local area networks.

## BROADBAND CABLE VS DSL VS FIBER INTERNET

I. Broadband Cable

Broadband cable is a high-speed technology using a cable modem and coaxial cable.

Provided by cable TV providers, leveraging existing infrastructure, especially in the United States.

Various speed packages offered by providers, with examples from Xfinity.

Cable internet involves receiving a modem or gateway for connecting multiple devices.

Downside: Shared bandwidth in the neighborhood can lead to slowdowns during peak hours.

II. DSL (Digital Subscriber Line)

DSL carries voice and data simultaneously over phone lines, distinct from slow dial-up connections.

DSL modem connects to common telephone lines, offering high-speed internet.

Cost-effective compared to cable, with dedicated connections, avoiding neighborhood bandwidth sharing.

Different types of DSL: ADSL (asymmetric), SDSL (symmetric), and VDSL (very high bit) for varying needs.

DSL uses copper wire for short distances; VDSL can also use fiber optic cable for longer distances.

III. Fiber Internet

Fiber offers the fastest internet speeds, reaching 1000 Mbits/s for both download and upload.

Uses light to transmit data through fiber optic cable, the backbone of the internet.

Advantages include faster speed, longer transmission distances, and resistance to electromagnetic interference.

Fiber is relatively new, more expensive, and may not be widely available due to developing infrastructure.

# CHAPTER 2

## HDMI, DISPLAYPORT, DVI, VGA, THUNDERBOLT - VIDEO PORT COMPARISON

1. VGA Port (Video Graphics Array)

Description: Introduced in 1987, VGA is an older port with 15 pins carrying analog data.

Characteristics: Found in CRT monitors but still present in some LCD monitors; being phased out for modern designs.

Limitations: Degrades video quality at higher resolutions and longer cable lengths; end adapter is typically blue.

2. DVI Port (Digital Visual Interface)

Overview: Developed in 1999, succeeding VGA for high-quality video on LCD monitors.

Types: DVI-A (analog), DVI-D (digital), and DVI-I (integrated for both analog and digital signals).

Links: Single-link and dual-link options; dual-link supports higher resolutions (2560 x 1600).

Adapter Color: Typically, white.

3. HDMI (High-Definition Multimedia Interface)

Significance: Dominant video port developed in 2002 for transmitting uncompressed video and audio through a single cable.

Evolution: HDMI 1.4 (2009) added an Ethernet channel; HDMI 2.1 (2017) supports higher resolutions (4K at 120Hz, 8K at 60Hz).

Features: Crystal-clear video and audio; supports up to 10K resolution for specialized uses.

4. DisplayPort

Introduction: Debuted in 2006, designed by VESA to replace VGA and DVI interfaces.

Capabilities: High-performance interface for video; can carry USB and audio data.

Advantages Over HDMI: Multi-monitor capabilities through daisy-chaining; locking mechanism for secure connections; royalty-free product.

Latest Version: DisplayPort 1.4 (2016) supports a max resolution of 8K at 60Hz.

5. Thunderbolt

Definition: High-speed technology interface released in 2011, combining PCI Express and DisplayPort signals.

Usage: Not only for video but also for connecting external peripherals; supports daisy-chaining up to six devices.

Versions: Thunderbolt 1 & 2 use mini-DisplayPort connectors; Thunderbolt 3 uses USB type-C connectors.

## USB PORTS, CABLES, TYPES, & CONNECTORS

Universal Serial Bus (USB) is the standard for connecting peripherals to computers, widely used due to its universality.

USB connects various devices like keyboards, mice, cameras, printers, and can handle networking and charging.

USB development aimed to simplify device connection by creating a universal connector.

Emphasis on easy device configuration and fast transfer rates.

USB is hot-swappable, allowing device connections without turning off the computer.

Evolution of USB Versions:

1. USB 1.0 (1996): 1.5 Mbps.

2. USB 1.1 (1998): 12 Mbps.

3. USB 2.0 (2000): 480 Mbps.

4. USB 3.0 (2008): 5 Gbps.

5. USB 3.1 (2013): 10 Gbps.

6. USB 3.2 (20 Gbps) and USB 4 (40 Gbps, 2019).

Types of USB Connectors:

Type A: Rectangular host connector on computers.

Type B: Square design used on printers, external hard drives, etc.

Mini B: Smaller version used on older smartphones, digital cameras.

Micro B: Thinner and smaller, replacing Mini B for modern devices.

USB 3.0 Type B: Larger, with nine pins for higher transfer speeds and power supply.

USB 3.0 Micro B: Wider than 2.0 version, used for modern external hard drives.

USB C (2014): Thin, rounded edges, 24 pins, reversible, used in modern devices, including laptops.

USB cables generally have different connectors on each end, e.g., Type A on one end and B or C on the other.

USB C cables are an exception, featuring the same connector on both ends.

## ETHERNET CABLES, UTP VS STP, STRAIGHT VS CROSSOVER, CAT 5,5E,6,7,8

Ethernet cables used in local area networks (LANs) are twisted pair cables.

Connect computers to routers or modems for internet access.

Two types of twisted pair cables: Unshielded Twisted Pair (UTP) and Shielded Twisted Pair (STP).

Types of Twisted Pair Cables:

1. Unshielded Twisted Pair (UTP):

Most common type.

Four pairs of color-coded wires twisted to prevent interference.

Commonly used in homes and businesses.

2. Shielded Twisted Pair (STP):

Similar to UTP but with a foil shield for extra protection against interference.

Mainly used for industrial purposes.

Creating Custom Cables:

For DIY cables, use bulk twisted pair cable.

Use a cable stripper to remove outer sheathing.

Wire crimper is used to attach RJ45 connectors.

Wiring Standards:

Two standards: 568A and 568B.

Colors determine the wiring order.

568A: White green, green, white orange, blue, white blue, orange, white brown, brown.

568B: White orange, orange, white green, blue, white blue, green, white brown, brown.

No functional difference; B standard more common in the U.S.

Cable Types

1. Straight Cable (Patch Cable):

Both ends wired using the same standard.

Connects dissimilar devices (computers to hubs, switches, routers, or modems).

2. Crossover Cable:

Both ends wired using different standards.

Connects similar devices directly (computer to computer, hub to hub, or switch to switch).

Categories of Twisted Pair Cables:

CAT 3, CAT 5, CAT 6, CAT 7, CAT 8.

Categories represent the maximum speed without crosstalk.

Speed ranges from 10 Mbps (CAT 3) to 40 Gbps (CAT 8).

CAT 5e commonly used for gigabit speeds; CAT 3 and CAT 5 obsolete.

CAT 7 backward compatible; shielded version of CAT 6a.

CAT 8 is the latest version with a speed of 40 Gbps up to 30 meters.

To enhance your comprehensions,

Both Unshielded Twisted Pair (UTP) and Shielded Twisted Pair (STP) cables are types of Ethernet cables commonly used in networking.

Both Straight Cables and Crossover Cables can be either Unshielded Twisted Pair (UTP) or Shielded Twisted Pair (STP) cables. The classification into UTP or STP pertains to the construction of the cable and whether it has a shield to protect against electromagnetic interference (EMI).

## NETWORK CONNECTORS

Different types of connectors used in networking.

Variability based on network type and cable.

RJ-45 Connector:

Most common network connector.

Eight-pin connector for connecting computers and network devices.

Used with unshielded twisted pair (UTP) cable.

Crimped on both ends using a wire crimper.

Single locking tab for secure connection.

UTP Coupler:

Not a connector but used to connect UTP cables with RJ-45 connectors.

Extends network cables by joining two cables together.

RJ-48 Connector:

Similar to RJ-45 but used with shielded twisted pair cable.

Primarily used with T1 lines.

RJ-11 Connector:

Four-wire connector for telephone equipment.

Used to connect computers to a local area network through a modem.

Single locking tab, smaller than RJ-45.

BNC Connector:

Used with coaxial cable.

Bayonet Neill–Concelman connector.

Common in older networks.

Types include BNC-T connector, BNC coupler, and BNC terminator.

F-type Connector:

Threaded connector used on coaxial cables.

Commonly used by cable providers for cable modems.

Also used in satellite internet.

USB Connector:

Common on desktops and laptops.

Universal use, including networking.

Examples include USB wireless adapters and wired network adapters.

Fiber Optic Connectors

Used in fiber optic networks.

Utilize pulses of light for data transmission.

SC Connector

Standard square connector.

Push-pull connection.

Common between floors in a building.

MRTJ Connector:

Mechanical transfer register jack.

Latched push-pull connection.

Small form factor, replacing SC connector.

LC Connector:

Local or Lucent connector.

Competes with SC connector.

Half the size of SC, suitable for populated racks.

ST Connector:

Straight tip connector.

Half twist bayonet lock.

Larger size, declining in usage.

Fiber Couplers:

Used to join two of the same fiber optic connectors.

Different from fiber adapters, which join different connectors.

UPC vs. APC End Faces:

UPC (Ultra Physical Contact) reflects light directly back, causing signal loss.

APC (Angled Physical Contact) reduces signal loss by reflecting light at an angle into the cable wall.

## NETWORKING TOOLS

Cable Stripper:

Removal of outer plastic shielding from cable ends.

Insert the cable into the cable stripper.

Squeeze, twist, and pull to remove the outer plastic shielding.

Essential for preparing cables before attaching connectors.

Wire Crimper:

Crimping connectors (e.g., RJ45) to twisted pair cables.

Arrange wires in the correct order.

Insert the wires into the RJ45 connector.

Place the connector into the wire crimper and squeeze for a secure connection.

Ensures a reliable and secure connection for data transmission.

Cable Tester:

Verification of continuity and correct wire arrangement in cables.

Connect both ends of the cable to the tester.

The tester cycles through all pins to ensure proper wiring.

Ensures cables are properly wired before installation, preventing connectivity issues.

Tone Generator

Tracing cables from one end to the other in complex setups.

Connect the tone generator at one end of the cable to be isolated.

Generates a tone through the cable to the other end.

Use a probe to jump from cable to cable on the patch panel until the desired cable is found.

Facilitates cable identification in scenarios with multiple interconnected cables.

Time Domain Reflectometer (TDR):

Electronic equipment for testing twisted pair and coaxial cables.

Transmits a signal through the cable.

Analyzes the reflected signal to pinpoint cable issues (e.g., conductors, loose connectors).

Provides detailed insights into cable integrity, aiding in troubleshooting.

Optical Time Domain Reflectometer (OTDR):

Similar to TDR but used for fiber optic cables.

Transmits light through the fiber optic cable.

Analyzes the reflected light to detect any problems.

Specifically designed for the characteristics of fiber optic cables.

Light Meter:

Measures the amount of light passing through fiber optic cables.

Light source at one end sends light through the cable.

A light meter at the other end measures the amount of transmitted light.

Provides a basic indication of the functionality of fiber optic cables.

RJ45 Ethernet Loopback Adapter:

Performs loopback tests to identify network port or connection issues.

Wires in the network cable arranged in a specific way into an RJ45 connector.

Causes output signals to loop back into the input signals, forming a complete circuit.

Quick and easy method to test network connections and identify potential issues.

Butt Set:

Resembles a telephone, used by telephone technicians.

Hooks up to telephone lines to monitor conversations and identify issues.

Allows technicians to listen to conversations and detect problems in telephone lines.

Punch Down Tool and Block:

Connects wires to a punch down block without stripping the cable first.

Insert wires using a punch down tool.

Excess wire is automatically cut off during the punching down process.

Simplifies the process of connecting wires in telephone equipment.

Multimeter:

Tests electrical circuits and measures voltage.

Measures voltage in network devices.

Checks for voltage in power outlets.

Verifies continuity in network cables.

Available in both analog and digital versions.

Versatile tool for various trades, including networking, providing essential electrical measurements.

# CHAPTER 3

## PUBLIC VS PRIVATE IP

The first thing we have to know is what is an IP address? Well, an IP address is a numeric address.

It's an identifier for a computer or device on a network.

Every device has to have an IP address for communication purposes.

There are two different types of IP addresses: public and private.

Let's first talk about public IP addresses.

When you order internet service from an internet service provider, they are going to assign your modem or your router in your home or business a public IP address.

This public IP address is registered on the internet, it's what gives you access to the world wide web. So, if you don't have a public IP, you cannot access the internet.

Public IP addresses are also unique, there are no duplicates anywhere in the world of public IP addresses.

Now when IP addresses were created, engineers didn't realize how big the internet would become

So, in order to prevent a shortage of public IPv4 addresses, engineers developed private IP addresses.

Now private IP addresses are not publicly registered on the internet. So, you can't access the internet using a private IP address.

However, if your device does have a private IP address and you want to access the internet, your private IP has to be converted into a public IP address before you can access the internet. And this is because private IP addresses are only used internally such as inside a home or business.

A service that's inside your router called DHCP is what assigns your internal devices a private IP. So as an example, most homes are not going to have just one device that needs access to the internet, chances are they're going to have multiple devices that need internet access. So, all of those devices need a public IP address if they want to access the internet.

When these devices need to access the internet their private IP address will be translated to the one public IP address that we have been given. And the service that translates this is called NAT or network address translation and it's a service that's built into our router.

It not only does it translate private to public but it also translates public to private.

Now private IP addresses have three different classes and these classes have different ranges.

|  |  |  |
| --- | --- | --- |
| CLASS | IP ADDRESSES RANGE | DEFAULT SUBNET MASK |
| A | 10.0.0.0 – 10.255.255.255 | 255.0.0.0 |
| B | 172.16.0.0 – 172.31.255.255 | 255.255.0.0 |
| C | 192.168.0.0 – 192.168.255.255 | 255.255.255.0 |

Class A is typically used for large organizations.

Class B is typically used in medium-sized organizations.

Class C start with 192 and is used in small organizations or homes.

Class C is the most popular range of private IP addresses that's used. So don't be surprised if you happen to check your IP addresses on your devices in your home and you see them starting with 192.168, because like I said it's the class that's mostly used.

So, to summarize,

|  |  |
| --- | --- |
| PUBLIC IP | PRIVATE IP |
| Public IP addresses are unique | private ip addresses are non-unique because the same private ip addresses can be used in other private networks |
| Public IPs are publicly registered so they are able to access the internet | Private IPs are not publicly registered, so they cannot access the internet directly |
| Public IPs are used externally on the internet | Private IPs are used internally on local networks |
| Public IPs are assigned by your internet service provider | Private IPs are assigned by your router |
| Public IPs are not free, you have to pay for them | Private IPs are free |

Now even though private IPs are used internally, they still have to be translated to a public IP when you want to go on the internet. Which means your public IP is exposed on the internet.

So, in order to make a public IP more secure you have to add security measures such as using a proxy or VPN, which hides your public IP address.

## IPV4 VS IPV6

An IP address is a numeric identifier for devices on a network.

It comprises two parts: network address and host address.

IP VERSION 4 (IPV4)

Current version with a 32-bit numeric address.

Written as four numbers separated by periods (octets).

Each octet's value ranges from 0 to 255.

Binary representation used by computers; 1s and 0s determine the value.

Each octet consists of eight binary bits.

Bits have values: 128, 64, 32, ..., down to 1.

1s under relevant values give the binary representation.

Example: Converting 66 to binary results in 01000010.

IPv4, thought to be sufficient, provides over 4 billion addresses.

Limitations emerged with the internet's growth.

IP VERSION 6 (IPV6)

Next-generation with a 128-bit hexadecimal address.

Hexadecimal includes numbers and alphabets.

Can produce an immense 340 undecillion IP addresses (340 with 36 digits).

128-bit address comprises 8 sets of 16 bits.

Sets separated by colons.

## SUBNET MASK

A subnet mask is a 32-bit number that divides an IP address into two parts: the network address and the host address. The network address identifies the network to which a device belongs, while the host address identifies the specific device on that network. Subnetting is the process of dividing a large network into smaller subnetworks. This is done to improve network performance and security.

An IP address is a 32-bit numeric address, written as four numbers, separated by periods.

The binary number for an IP address and subnet mask is used to determine the network and host portions of the IP address.

Subnet masks are typically written in decimal format, but computers and networks only understand them in binary format.

The 1s in the subnet mask indicate the network address and the 0s indicate the host addresses.

Default subnet masks are simple to use, but custom subnet masks can be used to create more complex network configurations.

Subnet masks are an essential part of IP networking. They play a critical role in routing traffic and ensuring that devices can communicate effectively. Understanding subnet masks is essential for anyone who wants to work with computer networks.

## NAT

NAT stands for network address translation and this is a service that is used in routers.

The purpose of NAT is to translate private IP addresses to public IP address and public IP addresses to private IP addresses.

and the reason for having the NAT service is to help preserve the Limited amount of IP version 4 public IP addresses that we have available around the world When the IP version 4 address was created engineers didn't realize how big the internet will become

However, we won't need NAT or private IP addresses in the future and this is because of the new generation of an IP address called IP version 6

With IP version 6 every single device in the world will have its own public IP address. So, there is no need for IP address translation.

This is because IP version 6 is able to produce over 340 undecillion IP addresses, so that's the number 340 with 36 digits after it.

340,282,366,920,938,463,463,374,607,431,768,211,456

With a number that huge we will never run out of IP addresses.

## DHCP

Before diving into DHCP we must understand that dynamic host configuration protocol is just a service that runs on a server. For instance, this could be a Microsoft server or a Linux server. Moreover, it's also a service that runs on many routers. Whether the router is a business router or a small office/home office router. These routers will have a DHCP service built into them.

Most importantly remember that IP addresses assigned by DHCP will be private IP addresses.

Every computer or device on a network has to have an IP address for communication purposes as we saw before.

An IP address is an identifier for a computer or device on a network.

There are two ways that a computer can be assigned an IP address. 1> Using a static IP 2> Using dynamic IP

A static IP is where a user assigns a computer or device with an IP address manually. This was the original method that was done in the beginning of networking. So, for each computer on a network you had to open up the computer's network configuration page and manually type in an IP address.

But in addition to an IP address, you also have to type in a subnet mask, default gateway, and a DNS server. And anytime that you wanted to add another computer or device to the network, you had to do the same thing. So, as you might have guessed this could be a lot of work especially if you are dealing with a large network that has a lot of computers.

And you also have to make sure that all the IP addresses are unique because if you assign the same IP address twice it would cause an IP conflict and would cause those computers to not have access to the network

But there is a better and easier way to assign a computer an IP address and this is called a dynamic IP.

A dynamic IP is where a computer gets an IP address automatically from a DHCP server.

A DHCP server automatically assigns a computer with an IP address. And in addition to an IP address it can also assign a subnet mask, default gateway, and a DNS server.

A DHCP server assigns IP addresses to computers on a network from its scope. And a scope is a range of IP addresses that a DHCP server can hand out.

Now when computers obtain an IP address from a DHCP server, the server assigns the IP address as a lease. So, the computer doesn't actually own the IP address, it's actually a lease. And a lease is the amount of time an IP address is assigned to a computer.

Now the reason for the lease is to help make sure that the DHCP server does not run out of IP addresses in its scope.

Now if you wanted a computer or device on your network to have a specific IP address all the time, in other words you never want that IP address to change, then you can create a reservation on the DHCP server.

A reservation ensures that a specific computer or device, identified by its MAC address, will always be given the same IP address when that computer or device requests an IP address from the DHCP server.

Now, reservations are not typically given to regular computers. They are typically given to special devices or computers such as network printers, servers, routers, etc. Because devices like these should be given the same IP address constantly.

## APIPA

As we all know by now, every computer has to have an IP address to communicate on a network.

When a computer is set to automatically obtain an IP address, it gets the IP from a DHCP server.

But what happens if the computer can't reach the server? What happens if a DHCP server goes down or if the communication to the server is lost.

If this happens, the computers that are running Microsoft Windows, the computers themselves will self-assign their own IP address and these IP addresses will be in the 169.254.0.0 to 169.254.255.255.

This type of self-assigned IP addressing is what's called automatic private IP addressing. And in addition, they were also assigned themselves a 16-bit subnet mask.

Now the reason why computers do this, is that even though they cannot get an IP address from a DHCP server, they will still be able to communicate with other computers on the same local network, or to be specific, on the same subnet that also have self-assigned IP addresses.

However, the computers will not be able to access the internet or access other devices on a different subnet with this type of IP address. Which also means the router will not be able to convert these private IP addresses to public IP address.

Let's say in an office we have three computers and they're all connected to the switch that's connected to the DHCP server.

And let's say for example that the DHCP server cannot be reached. Whether it's due to a malfunction or disconnected cable or maybe even the server caught on fire?

So, when we turn on these computers, they are going to ask the DHCP server for an IP address. However, since the server cannot be reached because it's on fire, the computers are going to have to self-assign their own IP address from this range of IP addresses.

But IP addresses have to be unique for each computer.

So, in order to ensure that the computers don't pick the same IP address, the computers will broadcast an ARP message on the network to make sure that no other computer picks the same IP address. Then once they have all their IP addresses, they will then be able to communicate with each other on the same subnet.

Now every few minutes the computers will check to see if they can contact a DHCP server, hopefully one that's not on fire, and if it detects one, the computer will replace the self-assigned IP address with the one obtained from the DHCP server.

## DNS

In the world of networking, computers don't go by names like humans do, they go by numbers, such as IP addresses.

Humans on the other hand are accustomed to using names instead of numbers.

So, in order to bridge the communication gap between computers and humans and make the communication a lot easier, networking engineers developed DNS, and DNS stands for a domain name system.

DNS resolves names to numbers, to be more specific it resolves domain names to IP addresses.

So, if you type in a web address in your web browser, DNS will resolve the name to a number because the only thing computers know are numbers!

For example, if you wanted to go to a certain website you would open up your web browser and type in the domain name of that website, so for example let's use yahoo.com.

Now technically you really don't have to type in yahoo.com to retrieve the Yahoo web page, you can just type in the IP address instead if you already knew what the IP address was, but since we are not accustomed to memorizing and dealing with numbers, especially when there are millions of websites on the internet, we can just type in the domain name instead and let DNS convert it to an IP address for us.

So back to our example, when you type in yahoo.com in your web browser, the DNS server search through its database to find a matching IP address for that domain name, and when it finds it it will resolve that domain name to the IP address of the Yahoo web site, and once that is done then your computer is able to communicate with a Yahoo web server and retrieve the webpage.

DNS basically works like a phone book, when you want to find a number, you don't look up the number first, you look up the name first, then it will give you the number.

To break this down into further detail let's examine the steps that DNS takes.

When you type in yahoo.com in your web browser and if your web browser or operating system can't find the IP address in its own cache memory, it will send the query to the next level to what is called the resolver server.

The resolver server is basically your ISP, so when the resolver receives the query, it will check its own cache memory to find an IP address for yahoo.com, and if it can't find it it will send the query to the next level which is the root server.

The root servers are the top or the root of a DNS hierarchy. There are 13 sets of these root servers and they are strategically placed around the world, and they are operated by 12 different organizations and each set of these root servers has their own unique IP address.

When the root server receives the query for the IP address for yahoo.com, the root server is not going to know what the IP address is, but the root server does know where to send the resolver to help it find the IP address. The root server will direct the resolver to the TLD or top level domain server for the dot com domain.

The resolver will now ask the TLD server for the IP address for yahoo.com but TLD server is not going to know what the IP addresses for yahoo.com. So the TLD will direct the resolver to the next and final level, which are the authoritative name servers.

So once again the resolver will now ask the authoritative name server for the IP address for yahoo.com. They are the final authority. So, when the authoritative name server receives the query from the resolver, the name server will respond with the IP address for yahoo.com.

And finally, the resolver will tell your computer the IP address for yahoo.com and then your computer can now retrieve the Yahoo web page.

It's important to note that once the resolver receives the IP address, it will store it in its cache memory in case it receives another query for yahoo.com so it doesn't have to go through all those steps again.

## DDNS - DYNAMIC DNS EXPLAINED

Just as a refresher as to what DNS does, if you type in a web address in your web browser, DNS is what transforms that domain name to an IP address.

For example, when you type in youtube.com in your web browser, the DNS server will search through its database to find a matching IP address for that domain name, and when it finds the IP, it'll transform that domain name to the IP address of the YouTube web server.

In a DNS database, a domain name such as youtube.com, is mapped or joined to an IP address, and that IP address must not change. In other words, it must be a static IP.

If the IP address does change, DNS will update their database with the new IP address for youtube.com, so people can find YouTube. Now this may not sound like a big deal, however the problem is, is that it could take up to 24 hours for DNS to update their database with the new IP and that is a problem because that means that YouTube will lose up to 24 hours’ worth of business until DNS does the update.

This is the main reason why websites, organizations, and companies use static IP addresses and not dynamic IP addresses.

DNS is used with static IP addresses but dynamic DNS is used with dynamic IP addresses.

A dynamic IP address is where an IP address gets an IP from a DHCP server, therefore the IP address changes periodically.

Dynamic DNS is a service that allows you to access devices that are in your home, such as a computer, router, or security camera, and you can access them from anywhere in the world, even if your IP address changes.

Dynamic DNS is mainly used in homes because internet service that are used in homes are given a dynamic IP and not a static IP.

Let's say you're at work and then you wanted to access your home computer using Microsoft remote desktop. You would open up the remote desktop service from your work computer and then you would type in the IP address for your home and then you would type the password and then you're connected.

You already knew what the IP address was for your home because you either wrote it down or maybe you memorized it, however since you have a home account with your internet service provider, your IP address is dynamic and it will change periodically.

If it changes without you knowing about it, the next time that you want to remote access your home computer, you will not be able to because you're typing in your old IP address and not your updated one.

This is where dynamic DNS comes in. Dynamic DNS allows you to access your home computer even if your IP address changes.

It allows you to create a custom hostname, such as 'myhomepc.ddns.org' or whatever and then you can link that hostname to your computer.

So, if your home IP address does change, dynamic DNS will update the new IP address and map it to your custom hostname automatically.

Dynamic DNS will ensure that you will always have access to your home computer even if your IP address changes.

So, for example now let's say you wanted to access your home computer again, but instead of typing your home's IP address, you would type in your custom hostname that you created with dynamic DNS.

You would type in 'myhomepc.ddns.org' and then you'll be connected.

No matter how many times your IP address changes, it doesn't matter, because whenever you want to access a device in your home you will always use your custom hostname instead of the IP address. And dynamic DNS will always make sure that the correct IP address is mapped to your custom hostname.

# CHAPTER 4

## MAC ADDRESS

The MAC or media access control address is an identifier that every network device uses to uniquely identify itself on a network.

No 2 devices anywhere in the world will have the same MAC address.

The MAC address is made up of a 6-byte, hexadecimal number that is burned into every NIC by its manufacturer.

The MAC address can contain any number and it also contains alphabets from A – F.

The MAC address is broken up into 2 parts. The first 3 bytes identify the manufacturer of the NIC. The last 3 bytes are a unique number from the manufacturer that identifies each device on a network.

The MAC address is also referred to as the physical address or hardware address.

MAC addresses are formatted in different ways. On a windows computer, it will have dashes in between the digits. On Apple and Linux systems, it will have colons in between the digits. And Cisco will display the MAC address separated by periods.

So, what exactly is the purpose of the MAC address? The purpose of the MAC address is so network devices can communicate with each other.

Whenever a device wants to talk to another device, it's ultimately done using the MAC address. This is whether the devices are close to each other, or if they are thousands of miles apart on a different network. The bottom line is that devices communicate with each other using the MAC address.

Now you might be asking yourself, well if devices talk to each other using the MAC address. What is the purpose of an IP address? I mean aren't IP addresses also unique?

Well public IP addresses are unique. But public IP addresses can periodically change. So, you may have had a certain IP address for the past few months, but an internet service provider or a network administrator can change your IP address to a different one.

But MAC addresses don't change. They are permanent.

A networking device needs both an IP address and a MAC address. The IP and MAC addresses work together so devices can talk to each other.

The MAC address is used to identify a device, but an IP address is used to locate that device.

So, for example, in a typical neighborhood, you have houses and you have people living in those houses. Each house has a mailing address and the person living inside has a name. An IP address is like the mailing address of a house. The mailing address tells us what country, city, and the street of where the house is located. But it doesn't necessarily tell us who lives in the house. But a MAC address is like the name of the person. It tells us who lives in the house. So, an IP address tells us where a networking device is located. But a MAC address tells us specifically who the device is.

MUST WATCH VIDEO – <https://youtu.be/yDTC6sbYFFE?si=DMgKgmuqSe7nkNqV>

## NETWORK PORTS

A port is not a physical connection, it's a logical connection that is used by programs and services to exchange information.

It specifically determines which program or service on a computer or server that is going to be used.

Ports have a unique number that identifies them. The number ranges from 0 - 65535.

For example, some common ports are port 80 and 443 which are used for web pages. Port number 21 is used for FTP. And port number 25 is used for email.

A port number is always associated with an IP address. And an IP address and a port number work together to exchange data on a network.

So, for example if you want to connect to a server over the internet, the IP address is used to determine the geographical location of that server. Such as what continent, country, city, and so on. And a port number determines which service or program on that server it wants to use.

Now in simple terms, what does this all mean? let's take a very common port that just about everyone uses every day and that is port number 80.

Port 80 is associated with HTTP which is web pages. Whenever you visit a web page from your computer, you're using port 80 whether you know it or not.

So, let's say you’re sitting at your computer and you want to visit Google's web page. So you would open up a web browser and then you would type google.com in the address bar. But before your computer can bring up Google's web page, it has to do a couple of things first.

It has to convert the domain name of google.com into Google's IP address, and in addition since you're using a web browser which is using HTTP, your computer is going to add port 80 to the IP address. So now the IP address is going to be used to locate Google's web server. Then once the server is found, the IP address has done its job. So now it's the port number's turn.

And Google's web server will see the incoming request with port number 80 and will forward that request to its built-in web service. So, you can finally retrieve Google's web page.

## PORT FORWARDING

Port forwarding allows computers over the internet to connect to a specific computer or service within a private network. It's basically making your computer accessible over the internet, even though you're behind a router.

Let's say a friend of yours at their home wants to remotely control your computer at your home using a service such as remote desktop connection. Remote desktop connection is a service built into Microsoft Windows that enables you to connect to another computer running Microsoft Windows. And then once you're connected to the remote computer, you can use that computer's programs and files just as if you were sitting in front of it.

So now your friend is ready to connect to your computer. So, he starts up the remote desktop connection and sends the request to your public IP address with a specific port number. In this case remote desktop connection uses port 3389.

The request with the port number will make its way through the internet, to your router and once it reaches your router, your router needs to know where to forward the request for port 3389.

Because without any port forwarding configured, your friend will not be able to connect to your computer because your router does not know what to do with this request.

This is where port forwarding comes in. So now we're going to tell our router to send or forward any requests that come in with port 3389 and send the request to our computer here.

To do this we're going to log in to our router's configuration page by typing in the routers internal IP address using a web browser.

# CHAPTER 5

## NETWORK DEVICES: HUBS, SWITCHES, AND ROUTERS

Network devices play a crucial role in connecting computers and enabling communication within and across networks. Three common network devices are hubs, switches, and routers. While they share similarities, each device serves a distinct purpose in data transmission and network management.

A hub is a basic network device that operates at the physical layer of the OSI model. It functions as a central connection point for multiple devices, allowing them to share data. However, hubs lack intelligence and broadcast data packets to all connected devices, regardless of the intended recipient. This approach leads to network congestion and security concerns.

Switches, operating at the data link layer, are more sophisticated than hubs. They maintain a table of MAC addresses, the unique identifiers of network devices. When a data packet arrives, the switch identifies the intended recipient based on its MAC address and directs the packet only to that device. This selective forwarding reduces network traffic and enhances security.

Routers operate at the network layer and function as gateways between different networks. They analyze data packets based on their IP addresses, the logical addresses that identify devices across networks. Routers determine the optimal path for data packets to reach their destination across different networks, ensuring efficient data routing.

Hubs are primarily used in small, low-traffic networks due to their low cost. Switches are preferred for larger networks due to their ability to reduce network congestion and improve performance. Routers are essential for connecting networks, such as home networks to the internet or corporate networks to each other.

## BLUETOOTH VS WIFI

Both of these are radio frequency technologies that are used for wirelessly connecting electronic devices. And certain devices will have both Bluetooth and WIFI functionality built into them.

Let s first talk about Bluetooth. Now Bluetooth was created to get rid of the hassle of dealing with wires and cables.

Bluetooth is a low-power, wireless technology that uses a short-range radio that provides a way to connect nearby devices to each other.

Bluetooth devices will have a computer chip inside of them that will broadcast a signal so that other Bluetooth devices can connect to them, which is known as pairing. And when the devices are paired, they will then be able to exchange information between them.

The range of Bluetooth is approximately 30 feet or 10 meters.

Now let’s talk about WIFI. WIFI is a wireless technology that uses radio waves that allows devices such as desktop computers, laptops, tablets, and cell phones to be able to connect wirelessly to the internet.

The most common way that WIFI devices access the internet is by connecting to a WIFI router. WIFI routers will have a connection to an internet service provider that will broadcast a WIFI signal so that nearby devices can connect to the signal and grant them internet access.

In addition to internet access, these devices can be configured to exchange information between them by creating a network.

Depending upon the surrounding environment, WIFI has a range anywhere from 100 - 300 feet.

So, what are the differences between Bluetooth and WIFI? Well, the main difference is that Bluetooth is for connecting devices to each other to exchange data. And WIFI is used to connect devices to the internet.

And another difference is the range and speed. Bluetooth has a slower transfer rate and a shorter range WIFI on the other hand, is faster than Bluetooth and has an approximate 10x longer range.

Now both Bluetooth and WIFI operate at 2.4 GHz. But the thing is, a lot of other devices also operate at 2.4 GHz, such as microwaves and cordless phones and this could interfere with wireless signals.

But Bluetooth is less vulnerable to interference because it uses a technology called Frequency Hopping Spread Spectrum, which uses a method of transmitting signals in a pattern that only the transmitting and receiving devices know.

The signal hops between 79 different channels and changes channels 1,600 times per second. Which makes Bluetooth highly resistant to interference when compared to WIFI.

Bluetooth devices are also simpler to connect to because there's no password required.

## HOTSPOT

Hotspots are physical locations where people can access the internet wirelessly using their mobile devices, such as laptops, tablets, or smartphones. These hotspots can be either public or private.

Public hotspots are typically found in places like coffee shops, hotels, airports, and even airplanes. They are created using a Wi-Fi router or a wireless access point that is connected to an internet service provider. To connect to a public hotspot, you will need to select the network ID (SSID) and enter a password if one is required. Some public hotspots are free to use, while others may require payment.

Private hotspots are typically found in homes or offices. They are created using a Wi-Fi router that broadcasts a wireless signal so that anyone authorized to access the network can connect and use the internet. Another type of private hotspot is called tethering. Tethering is a feature that allows you to use your smartphone as a wireless access point, sharing its cellular data connection with other devices.

Mobile hotspots are portable devices that use cellular networks to connect wireless devices to the internet. They are available through cell phone carriers and come in two forms: standalone devices and smartphone features. Mobile hotspots are a convenient option for people who need internet access when they are away from home or a public hotspot.

Public hotspots pose some security risks because they are accessible to anyone. To protect yourself when using a public hotspot, you should take the following precautions:

Disable folder sharing or password protect your shared folders.

Install an antivirus program.

Enable your firewall.

Use a VPN to encrypt your data and prevent hackers from stealing it.  
MODEM VS ROUTER

A lot of people actually think that a modem and a router are the same thing but they are not.

If you want internet inside your home or business, you have to have a modem.

A modem is what brings the internet into your home or business.

A modem establishes and maintains a dedicated connection to your internet service provider to give you access to the internet.

Another reason why you need a modem is because of the two different types of signals out there.

A computer only reads digital signals, while signals out on the internet are analog.

As analog data comes in from the internet, the modem demodulates the incoming analog signals into a digital signal so that a computer can understand it.

And a modem also modulates outgoing digital signals from a computer into an analog signal as it goes out on the internet.

This is where we get the word 'modem'. The word modem means modulator demodulator which is exactly what a modem does.

It modulates outgoing data from a computer and demodulates incoming data from the internet

A router comes in after the modem.

Now a router is what routes or passes your internet connection to all of your devices in your home or business. It directs it to all of your computers, tablets, phones and so on so that those devices can access the internet

Now, technically you really don't need a router if you only want one of your devices to access the internet. You can just plug that device's network cable directly into the modem, and then you'll be able to access the internet.

However, like most homes and businesses you're going to have multiple devices that need access to the internet, and that's where you would need a router.

## DEFAULT GATEWAY

If you open up a command prompt and then you type in ipconfig and in the output, you'll see the IP address, subnet mask, and the default gateway that's been assigned to this computer.

So, you might be asking yourself, well what is a default gateway? Simply put, a default gateway is a device that forwards data from one network to another. And the majority of the time, this is going to be a router.

Let’s imagine a local area network with the router, switch, and the computers. On the other side of the router, we have the internet, which is another network. So, in order for these computers to access another network, such as a web page out on the internet, the data has to exit its own local network by going through the default gateway, which is the router. And then the router will forward the data to the internet.

Now this also works both ways. So if a device on the internet wanted to communicate with a computer on this network, it has to go through this network's default gateway and then to the computer. So, in a nutshell, that's what a default gateway is.

It lets devices from one network communicate with devices on another network.

And as I said before, this is typically going to be a router. A router is the gateway or doorway to every network.

The term default means that the designated device is the first option that's looked upon when data needs to exit the network.

## WIRELESS ACCESS POINT VS WI-FI ROUTER

A lot of people think that these two devices are the same thing. But even though they do look similar and they do similar things, they are in fact different.

Almost everyone who has an internet connection in their home would have a Wi-Fi router, whether that Wi-Fi router is a separate device or if it's built into their modem.

A Wi-Fi router is what allows multiple wired and wireless devices to join together in a local area network.

It'll broadcast a Wi-Fi signal so that wireless devices can connect to it and it'll also have a built-in switch with several network ports so that wired devices can connect to it using Ethernet cables.

A wireless AP connects directly to a router where the router is then connected directly to a modem. Which gives the wireless devices access to the internet.

Wireless access points are primarily used by medium to large organizations and typically an organization will have multiple access points to make sure it covers the entire building.

Let’s imagine we have a medium sized office. And this office has desktop computers, laptops, and tablets. So, the desktop computers will connect to the organization's router using Ethernet cables. But in order for the wireless laptops and tablets to connect to the network, this office is going to use wireless access points.

The access points are going to be placed in strategic places and each of them will connect to the router using an Ethernet cable.

Then once that is done, they will all broadcast a Wi-Fi signal so that the laptops and tablets can connect wirelessly and join this network so now all the desktop computers and wireless devices are joined together in one network.

That one network is managed by one single router and because wireless access points are managed by a single router, that is one of the main reasons why larger organizations use wireless access points instead of Wi-Fi routers.

Now in reality this office here can use Wi-Fi routers instead of wireless APs and it would work just fine. But the problem with using Wi-Fi routers instead of wireless APs is manageability.

If the network administrator wanted to manage this network and make certain changes, he would have to log into each Wi-Fi router to make that change. And that could be a hassle and time-consuming especially if there were a lot of Wi-Fi routers. But if this office was using wireless access points instead, then all the management and all the changes in the configuration would be done by this single router.

Another difference between these is how devices are able to connect to them. Wireless access points are strictly for wireless devices to connect to, whereas Wi-Fi routers are able to accept connections from both wireless devices and wired devices. Because in addition to having a Wi-Fi antenna Wi-Fi router will also have a built-in switch to accept Ethernet cable connections.

Another difference is a firewall. Wireless access points don't have a firewall, while Wi-Fi routers will have a firewall.

Wi-Fi routers will also have a built-in DHCP service. A DHCP service is what automatically assigns IP addresses to devices that are connected to it. So, when devices connect to a Wi-Fi router, its built-in DHCP service will directly assign those devices an IP address. But since Wireless APs don't have a DHCP service, the devices that are connected to it will get its IP address from the organization's router. So once a device connects to the wireless AP, the router will send the IP through the wireless access point and then to the device.

Another difference is that Wi-Fi routers will have a WAN port or internet port. A WAN or internet port is where you would plug in a network cable coming in from your modem. And this is what gives your Wi-Fi router an internet connection so it can pass it on to other devices, whereas a wireless access point doesn't have a WAN or internet port. So, it cannot directly connect to a modem. It has to connect directly to a router instead and then the router is what connects to a modem.

And on a final note, wireless access points are often used to further extend a network's existing wireless signal.

## MESH WIFI EXPLAINED

A lot of us use wireless internet in our homes. And the reason we use wireless internet is because we want the freedom of accessing the internet from anywhere in our home.

Whether it's in the kitchen, bedroom, or living room, Wi-Fi gives us the ability and freedom to do just that from all of our devices.

However sometimes the Wi-Fi signal can be a little spotty. For example, there might be areas in your home where the Wi-Fi signal is weak or it may be totally dead.

To remedy this problem a lot of times people would buy a Wi-Fi extender to extend the Wi-Fi signal.

Now even though Wi-Fi extenders do work, the problem is that Wi-Fi extenders create their own Wi-Fi network with their own separate SSID. So, you would have to connect to the Wi-Fi router or the Wi-Fi extender's network, depending on where you are in the home.

If you're closer to the router, then you would connect to the router. Or if you're closer to the extender, then you would connect to the extender. This can be a little extra work.

A better solution for this is a mesh Wi-Fi system. Mesh Wi-Fi is the latest technology to solve the issue of weak or dead spot issues with Wi-Fi.

A mesh Wi-Fi system is a group of routers or Wi-Fi points that are placed in different locations inside a home and it provides a blanket of Wi-Fi coverage all throughout the home. A great feature of mesh Wi-Fi systems is that the Wi-Fi points communicate with each other wirelessly to create one large Wi-Fi network.

So, for example, if you wanted to set up a mesh Wi-Fi system in your home, normally you would have a modem that brings the internet into your home and then you would attach one of the mesh Wi-Fi points to the modem using an ethernet cable.

And then you would place the other Wi-Fi points in different locations all throughout your home.

Then once this is done, the Wi-Fi points will all talk to each other to create a seamless internet connection that covers your entire home for all your wireless devices to connect to.

Now this system creates one large Wi-Fi network. So it's not like each Wi-Fi point is creating their own Wi-Fi network with its own SSID like an extender would. It's all one network with a single SSID.

If you have a wireless laptop that's connected to your mesh Wi-Fi, you can move from room to room seamlessly because as you move to different areas in your home, your laptop will always connect to the nearest Wi-Fi point. It will seamlessly disconnect from a Wi-Fi point and then reconnect to another one.

## GUEST NETWORK

In today's connected world, providing internet access to guests has become a common courtesy. However, sharing your primary Wi-Fi password poses security risks, as it grants access to your entire home network. This is where guest networks come into play.

A guest network is a separate Wi-Fi network that allows visitors to access the internet without compromising the security of your main network. It acts as a virtual partition, isolating your guest devices from your personal devices and files.

Benefits of Using a Guest Network:

By keeping guests on a separate network, you prevent them from accessing sensitive data stored on your personal devices or shared network drives.

If a guest's device is infected with malware, it cannot spread to your network, minimizing the risk of data breaches or system compromises.

By limiting guests to internet access only, you ensure that your personal devices have ample bandwidth for tasks like streaming or video conferencing.

Most modern Wi-Fi routers have a built-in guest network feature. To enable it, follow these steps:

Open a web browser and enter your router's IP address in the address bar.

Navigate to the router's settings page and look for a section labeled "Guest Network" or "Guest Wi-Fi."

Provide a name for the guest network, set a password (recommended), and choose whether to allow guests to access other devices on your network.

Once the settings are configured, enable the guest network and apply the changes.

When guests arrive, provide them with the guest network name and password. They can connect to the guest network just like they would connect to any other Wi-Fi network.

## 2.4 GHZ VS 5 GHZ WIFI

In the realm of wireless connectivity, two frequency bands, 2.4 GHz and 5 GHz, play a crucial role in Wi-Fi operations. While both serve the same purpose of transmitting data between devices, they differ in their characteristics, offering distinct advantages and disadvantages.

The 2.4 GHz band is the more established and widely used frequency for Wi-Fi routers. It boasts a longer range, enabling signals to travel farther and penetrate walls and other obstacles more effectively. However, this popularity comes with a drawback: increased susceptibility to interference. A plethora of devices, including microwave ovens, cordless phones, Bluetooth gadgets, and wireless cameras, utilize the 2.4 GHz band, causing congestion and potential signal disruption. This interference can manifest as slower Wi-Fi speeds and occasional connection drops.

The 5 GHz band, a newer addition to the Wi-Fi scene, offers a significant advantage in terms of speed. It can deliver data transfer rates up to six times faster than the 2.4 GHz band, making it ideal for high-bandwidth activities like streaming videos, gaming, and large file transfers. However, its higher frequency results in a shorter range. Signals in the 5 GHz band have a harder time penetrating walls and solid objects, limiting their reach compared to the 2.4 GHz band.

The decision between using the 2.4 GHz or 5 GHz band depends on your specific requirements and usage patterns. If you prioritize range and need a stable connection for devices located farther from the router, the 2.4 GHz band might be a suitable choice. However, if speed is paramount and you primarily use your devices in proximity to the router, the 5 GHz band offers a significant performance boost.

For those who seek the benefits of both bands without compromising, dual-band routers provide the optimal solution. These routers simultaneously broadcast signals on both the 2.4 GHz and 5 GHz bands, allowing devices to connect to the band that best suits their needs. This flexibility ensures seamless connectivity and optimal performance for a wide range of applications.

## WIFI PASSWORD SECURITY

Wi-Fi networks can be open (no password required) or secure (requiring a password for access).

WEP (Wired Equivalent Privacy):

Developed in 1999, WEP was the earliest wireless security protocol.

Used a 40-bit encryption key, making it vulnerable to hacking.

WEP is outdated and no longer used in modern Wi-Fi routers.

WPA (Wi-Fi Protected Access):

Developed as an improvement over WEP.

Utilizes TKIP (Temporal Key Integrity Protocol) for stronger encryption.

While more secure than WEP, WPA is considered outdated due to TKIP vulnerabilities.

WPA2 (Wi-Fi Protected Access 2):

Developed to provide stronger security than WPA.

Uses AES (Advanced Encryption Standard) for encryption, resistant to brute-force attacks.

Recommended for modern devices as it only uses AES, unlike the mixed option.

WPA3 (Wi-Fi Protected Access 3):

Introduced in 2018, WPA3 offers cutting-edge security protocols.

Enhances Wi-Fi security, simplifies authentication, and provides increased protection against password guessing.

WPS (Wi-Fi Protected Setup):

Designed for easy connection without typing a password.

Common method: Push button setup.

Some routers and Wi-Fi printers have physical WPS buttons.

WPS is the simplest way to join a wireless network.

Access Control/MAC Filter:

Another method for network security.

Controls access by allowing or blocking devices using their MAC addresses.

Adds an extra layer of security beyond Wi-Fi passwords.

## POWER OVER ETHERNET (POE)

Networking devices require electrical power, usually supplied through a separate power cable.

Some devices, however, utilize Power over Ethernet (PoE), receiving both power and data through the same Ethernet cable.

Ethernet cables contain four pairs of twisted wires, with earlier versions using only four wires for data transfer.

PoE technology leverages the unused wires to transmit power, eliminating the need for a separate power cable.

PoE-enabled devices require connection to Power Sourcing Equipment (PSE), such as a PoE switch.

Example with a PoE switch and PoE IP phone, where both data and power flow through the Ethernet cable.

If connected to a standard non-PoE switch, a PoE injector can be used to supply power to the IP phone without replacing the switch.

Benefits of PoE:

Streamlines the need for separate power cables.

Avoids the expense and effort of installing additional power outlets.

Devices can be placed in more optimal locations without proximity to electrical outlets.

Types of PoE:

Active PoE: Ensures compatibility and communicates with devices to deliver the correct amount of power.

Passive PoE: Constantly sends power without communication, requiring careful voltage matching to avoid equipment damage.

Evolution of PoE Standards:

Cisco pioneered PoE in 2000, initially for IP phones.

In 2003, the IEEE 802.3af standard (Type 1) was introduced, delivering 15.4 Watts.

2009 saw the release of IEEE 802.3at (Type 2 or PoE Plus), doubling power output to 30 watts.

In 2011, Cisco's proprietary standard doubled power again to 60 watts.

The IEEE 802.3bt standard (Type 3 or four-pair PoE) was released in 2018, providing up to 90 Watts, capable of powering laptops.

# CHAPTER 6

## WHAT IS A SERVER?

Now a server is basically a dedicated computer that provides services on behalf of clients, such as ordinary desktop.

It's a centralized machine where multiple clients connect to, either over the Internet or in a local area network, for a specific service.

For example, that service could be to retrieve a website, to access data, or email, and so on.

When people talk about a server generally, they are referring to a powerful centralized computer that clients connect to over a network, and they would be correct on that. However, a server is not just a physical computer.

A server is actually a role that a computer takes. Because any ordinary desktop computer can be set up as a server and it doesn't necessarily have to be a powerful computer.

For example, you can set up a network in your home where you can have an ordinary desktop computer serve as a file server. The computer would have those files in a shared folder and then other computers can connect to it to access those files.

However, desktop computers do have their limitations because they are not designed to handle a large workload and they can't handle a lot of incoming connections from users. This is not only because of their inferior hardware, but it's also because of software. Desktop operating systems are only able to handle a limited number of concurrent connections.

Now servers need to be up and running 24/7 because they are vital to an organization. And if a server does go down then that could jeopardize a business or an organization. This is why servers need to be more reliable. They need to be built with robust hardware that's able to run non-stop with little to no downtime.

A desktop would use a processor that's designed obviously for desktops, such as the Intel core series processors. A server would use a processor designed for servers such as the Intel Xeon processor. A server processor needs to be fast and had the ability to perform a lot of tasks simultaneously.

Now there are many different types of servers and when I mean types I'm talking about the type of service that the server provides.

For example, a web server. A web server is what hosts a website. Any website that you go to with your web browser, you are connecting over the Internet to that web server to pull up the web site you want. The web server will contain all of the website's data, including the HTML code and graphics and it will also be running the web server software.

Another type of server is an email server. An email server is what facilitates the sending and receiving of email and you would access the email using your web browser or you can use an email client such as Outlook or Thunderbird using email protocols such as IMAP,, POP, and SMTP.

Database server is another type of server. This type of server stores data on the backend and then it's retrieved from computers on the front end, for example using queries such as SQL. These are just a few examples of what servers do but there is a lot more.

## TELNET VS SSH

Telnet is a terminal emulation program used to access remote servers, running on various operating systems.

It allows users to send commands remotely to a server, managing and administering it as if physically present.

Telnet is a command-line tool with no graphical user interface, originally developed in 1969.

Users can run programs, create folders, delete files, transfer files, browse directories, and manage services remotely using telnet.

It is not limited to servers but also used for configuring network devices like routers and switches.

Telnet operates with text commands sent via a keyboard, making it fast but lacking encryption.

Telnet lacks encryption, sending all commands in clear text, making it vulnerable to eavesdropping.

Developed before internet security concerns, it is considered outdated and insecure for use over the public internet.

SSH (Secure Shell) is a modern alternative to telnet, providing secure data transfer over a network.

It encrypts data during transfer, protecting sensitive information such as usernames and passwords.

SSH offers additional features, including password and public key authentication.

SSH performs all telnet functions but adds a layer of security through encryption.

It is the preferred choice for secure communication, especially over the internet.

Telnet, despite its historical significance, is outdated and insecure due to the lack of encryption.

SSH, with its encryption capabilities, is the modern and secure choice for remote communication.

## RAID

Storage is a very important part of fault tolerance. If something were to happen to a company's data such as a disk failure that results in data loss, then that could have a serious impact on how the company performs.

That's why we need to make sure that if a disk does fail, that no data loss would occur.

one of the best ways to prevent data loss is RAID, RAID stands for redundant array of independent disks.

In a RAID setup, the data is copied on multiple disks. So that in the event of a disk failure, no data would be lost.

There are four common types of RAID. There is RAID 0, RAID 1, RAID 5, and RAID 10. N

RAID 0 is not fault tolerant. In fact, RAID 0 shouldn't even be called RAID because not only does it not provide fault-tolerance, it actually increases the chance for data loss. Because in a RAID 0, the data is not duplicated, but it's actually spread or striped across two separate disks. If one of these disks fails, or if you decide to destroy yourself with a hammer, then all the data will be lost. The only reason why you would want to use RAID 0 is speed. Because when you have 2 disk controllers working instead of 1, then accessing data is much faster.

Now RAID 1 is fault tolerant. In a RAID 1 set up the data is copied on more than one disk. Disk 2 will have the exact same copy of the data as disk 1. In the event of a single disk failure, such as getting destroyed by a laser beam, then no data loss would happen because the other disk would have a duplicate copy.

In order to use RAID 5 you need to have 3 or more disks. RAID 5 is probably the most common setup that is used because it's fast and it can store a large amount of data. In a RAID 5 setup, data is not duplicated, but its striped or spread across multiple disks. And in addition to the data, there is another very important piece of information that is being evenly spread across all the disks, and this information is called parity, and parity is used to rebuild the data in the event of a disk failure.

But there is a downside to RAID 5, because since the equivalent of an entire disk is used to store parity, it reduces the collective amount of data that can be stored in this array.

For example, if all 4 of these disks were 1 terabyte each, that totals 4 terabytes, but in a RAID 5 set up, the total amount that will be used for data storage would be 3 terabytes, because the equivalent of 1 entire disk would be used to store parity.

And finally, there is raid 10 and RAID 10 is basically what the name says, its combining RAID 1 and RAID 0 together, and you need to use a minimum of 4 disks. In a RAID 10 set up, a set of 2 disks are mirrored using a RAID 1 set up. Then both sets of the two disks are striped using RAID 0. RAID 10 benefits from the fault tolerance of RAID 1 and the speed of RAID 0.

But the downside in a RAID 10, is that you can only use 50% of the capacity for data storage. So, if you are using four disks in a RAID 10 setup, you can only use two of them for actual storage.

## FULL VS INCREMENTAL VS DIFFERENTIAL BACKUP

fault tolerance can be defined as the prevention of data loss if a component fails.

But in the event that fault tolerance fails, then disaster recovery would be our last option.

Disaster recovery is the process of rebuilding an organization's data after a disaster has happened, such as data loss. Even if we have fault tolerance measures, we still need to back up our data. There are three different types of backups: there's full, incremental, and differential.

A full backup is just like its name says, it's a full backup. It backs up all the data. For example, all the data is simply backed into one tape. This is the simplest form of backup to perform because only one tape is used.

However, if your organization has a large amount of data, then performing a full backup daily would not be efficient because the disadvantage of doing a full backup is that it takes the longest to perform. But full backups do have an advantage and that is during data restoration, because if you ever needed to restore the data, then the data can be restored in one session.

An incremental backup is much faster than a full back up because in an incremental backup, the only data that is backed up, is that data that has been changed since the last full or incremental backup. For example, let's say a company does a full back up on Monday and does incremental backups Tuesday through Friday. So again, the only data that is backed up is that data that has been changed since the last full or incremental backup. Tuesday will only backup Tuesday's data, Wednesday will only backup Wednesday's data, Thursday will only backup Thursday's data, and so on.

The advantage of an incremental backup is that it's the fastest backup compared to a full or differential backup. However, the disadvantage of an incremental backup is that it takes the longest when you have to restore the data, because when you have to restore the data after you've done an incremental backup, you have to restore the full back up along with the incremental backups, and you have to restore the incrementals in the same order as you backed them up.

A differential backup is faster than a full backup but it's not as fast as an incremental backup. Now in a differential backup, the data that is backed up is that data that has been changed since the last full backup.

Going back to our example, a company does a full back up on Monday and does differential backups Tuesday through Friday. So as data is being added to the database on those weekdays, the differential backup will back up the data that has been changed since Monday's full backup.

So Tuesday will backup Tuesday's data. Wednesday will backup Tuesday's and Wednesday's data. Thursday will backup Tuesday's, Wednesday's, and Thursday's data. And Friday will backup Tuesday's, Wednesday's, Thursday's, and Friday's data.

After a differential backup, if you ever needed to restore the data, you would only need the last full backup and the last differential backup to completely restore your data.

## PATCH PANELS

In the realm of networking, patch panels serve as crucial components for organizing and managing cable connections. They are commonly employed in server rooms and wiring closets to maintain a clean and structured network environment.

Patch panels eliminate cable clutter by providing a centralized hub for connecting network devices. They simplify network management and troubleshooting by enabling easy identification and maintenance of individual cables.

While patch panels share similarities with keystone jacks and wall plates, they differ in their capacity and placement. Keystone jacks and wall plates typically have fewer ports and are mounted on walls, while patch panels feature multiple ports and are installed on server racks.

Patch panels effectively organize network cables, reducing clutter and enhancing the overall appearance of the networking infrastructure.

Patch panels facilitate troubleshooting by providing a centralized location for identifying and isolating cable-related issues.

Patch panels streamline maintenance tasks, making it easier to add, remove, or replace cables without disrupting the entire network.

Types of Patch Panel Connections:

1. Punch-down Type: Cables are directly punched down into the patch panel using a punch-down tool.

2. Keystone Blank Patch Panels: Wires are punched down into standard Keystone jacks, which are then inserted into the patch panel.

3. Coupler Patch Panels: Cables with RJ45 connectors simply plug into the couplers on the patch panel.

Patch panels are available in various types to accommodate different network configurations, including Ethernet, fiber optic, and coaxial.

## PROXY SERVERS

A proxy server acts as an intermediary between a user's computer and the internet, retrieving data on behalf of the user. Typically, users access web pages directly, but a proxy server serves as a middleman, fetching the content and sending it to the user.

Proxy servers provide anonymity by hiding the user's IP address.

Without a proxy, a user's public IP address is visible, allowing others to track visited websites.

Using a proxy shields the user's IP, making only the proxy server's IP visible.

Proxy servers can store web pages in a centralized cache, reducing the need to retrieve data from the internet repeatedly.

This caching mechanism enhances webpage retrieval speed and saves bandwidth.

Companies use proxies to monitor employees' internet activity.

Proxies log websites visited and the duration of visits.

Configurable to block specific websites, ensuring productivity and security.

Proxy servers do not encrypt data transmitted over the internet, leaving it vulnerable to interception by hackers, ISPs, or governments.

Virtual Private Networks (VPNs) offer a solution to the lack of encryption in proxy servers.

In addition to hiding IP addresses, VPNs encrypt data during transmission between the user's computer and the internet.

This encryption ensures the privacy and security of internet activities, preventing unauthorized access.

## PROXY VS REVERSE PROXY

The definition of a proxy is someone or something that has authority to do something for another person or thing.

A proxy is a middleman that sits between a private network and the public internet.

Suppose we have a private network with a bunch of computers. Now all of these computers have access to the internet. But as most of us know, with all these computers having the ability to access the internet, it could also create a massive security concern. Because with all of these computers accessing the internet, they could draw in malicious traffic that could wreak havoc inside this network.

This is where a proxy, or to be more specific, a forward proxy can be beneficial.

When a forward proxy server is used on this network, the proxy server is now the guardian of this network.

When all of these computers want to access the internet, they go to the proxy server instead and then the proxy server will fetch the data out on the internet on their behalf.

Furthermore, proxy hides the identity of clients by masking their IP addresses and using its own IP address. So, when these clients connect to servers out on the internet, those servers only see the IP address of the proxy server and not the clients.

Plus, it also logs user activity. A lot of organizations like to know what websites that their clients are visiting.

Apart from that a proxy can cache or store copies of websites that are frequently used by their clients. So, instead of the proxy server fetching the same websites out on the internet over and over again, those websites can be stored in the proxies’ cache database.

Now, a reverse proxy, just like the name says, is the reverse of a forward proxy.

A reverse proxy is also placed on a network, but instead of regulating traffic going out of a network, a reverse proxy regulates traffic coming into a network.

Suppose we have a private network with servers. Servers are just powerful computers that clients connect to if they want to access certain data such as retrieving a website, or access a database, and so on. These servers will accept incoming connections from clients outside its network from the internet.

When a client on the internet wants to access certain data on these servers, they will directly connect to one of these servers. But by having direct access to a server, this can be a security risk and open the door for hackers to create problems on these servers. This is where a reverse proxy can help.

By using a reverse proxy on this network, it creates a single point of entry that can regulate incoming traffic.

So now when computers from the internet want to access data on these servers, they no longer directly communicate with the servers, they only communicate with the reverse proxy server and then the reverse proxy will fetch the data from the server and then direct it back to the computer.

So, in short, a forward proxy is there to protect clients, while a reverse proxy is there to protect servers.

## VPN

VPN stands for Virtual Private Network.

It establishes a secure connection over an unsecured network like the internet.

Protects internet activity and conceals identity during web surfing.

ISP servers can log and share internet activity.

VPN redirects internet activity through its servers, hiding visited websites from the ISP.

VPN disguises identity by masking the user's IP address.

VPN encrypts and protects data packets during internet use.

Data packets are encapsulated through tunneling, ensuring privacy and security.

Especially useful on public Wi-Fi networks to prevent data interception.

VPN allows access to internet content restricted by geographical location.

Users can choose VPN servers in different countries, changing their IP address and location.

Example: Accessing content restricted to the U.S. from South America.

VPN provides a secure connection for remote workers.

Eliminates the need for leased lines, connecting separate locations through a secure virtual network.

Ensures a dedicated link over the internet for secure file access.

Suitable for anyone seeking enhanced internet safety, security, and anonymity.

Essential for users frequently using public Wi-Fi networks to avoid potential cyber threats.

Compatible with various devices such as desktops, laptops, tablets, and smartphones.

Free VPNs may collect and log user information for advertising purposes.

Paid VPNs are generally more secure, with a no-logging policy for enhanced privacy.

## FIREWALL

A firewall is a security system preventing unauthorized access to a private network by filtering internet data.

Purpose: Creates a barrier between private networks and the internet, protecting against hackers and malicious traffic.

Importance: Crucial for large organizations with numerous devices to prevent disruptions and unauthorized access.

Firewalls can permit or deny access based on IP addresses.

Firewalls can make rules based on domain names, protocols, programs, ports, and keywords.

Types of Firewalls:

Host-Based Firewall: Describes host-based firewalls as software protecting individual computers, either pre-packaged in operating systems or provided by third-party vendors.

Network-Based Firewall: Discusses the combination of hardware and software operating at the network layer, protecting entire networks. Can be standalone, integrated into routers, or deployed in cloud infrastructure.

Maximum Protection Approach: Recommends using both network-based and host-based firewalls for comprehensive security.

Scenario: If harmful data bypasses the network firewall, host-based firewalls on individual devices provide an additional layer of protection.

## DMZ

DMZ stands for a demilitarized zone. DMZ is used to improve the security of an organization's network by segregating devices such as computers and servers on the opposite sides of a firewall. It's sort of like creating two separate networks. The question is why would you want to do this? And how does a DMZ accomplish this?

Let's do an example here. Suppose we have a network that belongs to a company and this company has computers and servers that are behind a firewall. In this company we have servers that need to be accessed by people from the internet so that the company can stay in business.

These servers could be a web server and an email server. Now because these servers are behind the company's firewall, they are inside the company's private network. So that would mean that this company is letting in people from an untrusted network such as the internet, be given access behind the company's firewall and into the company's private network where the servers are.

But this could cause a security concern because as people are accessing these servers’ hackers could use this as an opening to cause havoc on the company's network. Because remember, they already got past the firewall because the servers are behind the firewall. So now hackers can try and access other sensitive data from other devices that are behind the firewall. Such as a database server, where sensitive data is kept or they may even try and plant a virus. This is a security concern.

But what if the company put web and email servers outside the company's internal network and put them on a opposite side of the firewall? Now the servers would still be in the same building but they would be on the other side of the firewall. So now when people access these servers from the internet, they are not going to be accessing them behind the company's internal firewall where the company's sensitive data is kept. These servers are now out in front, facing the internet and fully exposed. This is exactly what a DMZ is.

In conclusion in the real world a demilitarized zone is an area where the military is forbidden and in the computing world It's where firewall protection is forbidden.

## VIRTUALIZATION EXPLAINED

Traditional businesses operate by dedicating one physical machine to one application, often running different operating systems on separate servers. This approach leads to multiple physical servers, each serving a specific purpose.

Virtualization consolidates multiple physical servers, their applications, and operating systems onto a single physical server. This is achieved through the use of virtual machines (VMs) running in a virtual environment.

The software responsible for creating and managing virtualization is called a hypervisor. Two types of hypervisors exist: Type 1, installed on bare metal hardware, and Type 2, running on top of an existing operating system.

An example of a Type 1 hypervisor installation is provided using VMware ESXi. The process involves building server hardware, installing the hypervisor on bare metal, and creating virtual machines.

Type 1 hypervisors (e.g., VMware ESXi, Citrix XenServer, Microsoft Hyper-V) are common in enterprise data centers. Type 2 hypervisors (e.g., Oracle VM Virtualbox, Microsoft Virtual PC, VMware Workstation) are typically used on personal computers for testing and research purposes.

Benefits of Virtualization

Virtualization saves money on hardware, electricity, and floor space.

Physical machine maintenance is reduced, minimizing the need for administrative intervention.

Virtual machines can be easily transferred between physical machines.

Virtualization maximizes computing capability, utilizing a machine's full potential.

Virtual machines, being software files, can be backed up and quickly deployed on other machines in case of failure.

## VIRTUAL MACHINES VS CONTAINERS

In the traditional setup, each server runs one application.

This approach led to inefficiencies and underutilization of server capacity.

Engineers introduced virtual machines to address the inefficiencies.

Virtual machines simulate hardware and software, allowing multiple applications to run on a single server.

Hypervisors like VMware, Citrix, and Microsoft control the allocation and sharing of a machine's hardware.

VMs have their own dedicated operating systems and applications, solving the problem of wasting money on new servers.

Drawbacks of VMs include high disk space consumption, significant use of RAM and CPU, slow startup times, and the need for operating system licenses for each VM.

Containers, like VMs, enable multiple applications to run on a single server but differ in their approach.

Containers only contain the application, bundled with all necessary files, configurations, and dependencies to run on any computing environment.

Docker is a leading software used to create, manage, and run containers.

Containers are lightweight, as they share the underlying operating system on the server and don't require a dedicated operating system for each container.

Container files are smaller, allowing for faster startup times (milliseconds) compared to VMs (minutes).

Containers consume less RAM and CPU power from the server than VMs.

Both VMs and containers are valuable technologies; some organizations use both on the same machine for maximum productivity.

VMs offer flexibility as they can run any operating system, but they are larger, slower, and consume more resources.

Containers are praised for their size, portability, and speed, making them the future of technology.

Containers have a disadvantage in that the container file must be compatible with the server's operating system, and if the server's operating system crashes, all containers on it go down.

## CLOUD COMPUTING

Cloud computing involves storing and running data and applications on the cloud rather than locally.

The cloud, in essence, is a large building filled with servers that provide various services over the internet.

Cloud data centers contain servers for running applications, storing data, data processing, web hosting, etc.

Cloud servers are interconnected and accessible via the internet.

Cloud providers sell computing services, allowing users to outsource their computing workload.

Cloud services range from email hosting to productivity software, web servers, databases, and platforms like YouTube.

Reasons for Using Cloud Computing:

Eliminates the need for purchasing hardware, software, and maintaining a data center.

Cloud providers handle data backup, disaster recovery, and offer redundant sites for uninterrupted service.

Users can pay for the computing resources they need, instantly scaling up or down.

Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, Alibaba, and IBM are major players.

AWS is the largest, holding about a third of the market share.

Netflix outsources its computing needs to AWS, benefiting from reliability, security, and cost savings.

Cloud computing allows Netflix to focus on its core business instead of managing its own data center.

Types of Cloud Computing:

1. Infrastructure as a Service (IaaS)

Cloud provider manages hardware (servers, storage, networking).

Users retain control over software (applications, data, operating system).

2. Platform as a Service (PaaS)

Cloud provider manages hardware, operating system, middleware, runtime.

Users are responsible for applications and data.

3. Software as a Service (SaaS)

All applications hosted by the cloud provider.

No need for software installation or hardware management.

Cloud computing offers flexibility and varying levels of control.

Example of Software as a Service: Google Docs.

Users can choose the cloud service that best suits their needs.

## NAS VS SAN - NETWORK ATTACHED STORAGE VS STORAGE AREA NETWORK

NAS stands for Network Attached Storage.

It is a storage device dedicated to storing data and providing centralized access.

Designed to store and manage data without performing additional functions.

Typically configured with multiple hard drives in a RAID setup for redundancy.

Connects to a network via a network interface card for data access.

Commonly used in homes, small to medium-sized businesses.

Data can be accessed from various devices such as desktops, laptops, and servers.

Single point of failure – if a component fails, access to data is disrupted.

SAN is a Storage Area Network.

A specialized high-speed network dedicated to storing and providing access to large data volumes.

Consists of multiple disk arrays, switches, and servers.

Fault-tolerant architecture with shared data among disk arrays.

Offers high-speed data access as if it were a local hard drive.

Recognized by operating systems as local attached storage rather than a shared network drive.

Highly scalable – additional storage can be added without network interruption.

Interconnected devices using fiber channel, a high-speed standard for SANs.

Fiber channel speeds range from 2 gigabits per second to 128 gigabytes per second.

Some SANs use iSCSI as a cheaper alternative to fiber channel, though with reduced speed.

NAS is a simpler, cost-effective solution for centralized data storage suitable for homes and small to medium-sized businesses.

SAN is a sophisticated, high-speed, and expensive network dedicated to large-scale data storage, favored by large enterprises due to its scalability and fault-tolerant design.

# CHAPTER 7

## ARP (ADDRESS RESOLUTION PROTOCOL) EXPLAINED

ARP, or Address Resolution Protocol, is a crucial networking protocol used to map IP addresses to MAC addresses. This is essential for devices to communicate on a local area network (LAN).

IP addresses locate devices on a network, while MAC addresses uniquely identify each device's network interface card.

When a device, like computer A, wants to communicate with another device (computer B), it needs the MAC address of the target device.

Devices maintain an ARP cache, an internal list associating IP addresses with MAC addresses.

If the ARP cache doesn't have the needed MAC address, the requesting device (computer A) sends a broadcast message on the network, asking for the MAC address associated with a specific IP address.

In Windows, the ARP utility can be used to check the ARP cache (`arp -a`).

Computer A's broadcast message prompts the device with the matching IP address (computer B) to respond with its MAC address.

Once computer A obtains the MAC address, communication between the two devices can occur.

The ARP cache stores IP-to-MAC address associations, making future communications more efficient.

ARP cache entries can be dynamic (created automatically) or static (manually entered).

Dynamic entries are generated when a device sends a broadcast message requesting a MAC address and are periodically flushed to prevent unnecessary entries.

Network administrators can manually enter IP-to-MAC address associations. It Reduces unnecessary ARP broadcast traffic on the network.

## TCP VS UDP

When computers communicate, reliability is crucial to ensure data is received correctly. TCP (Transmission Control Protocol) is a fundamental protocol in TCP/IP networks, guaranteeing data integrity during communication.

TCP (TRANSMISSION CONTROL PROTOCOL)

1. Purpose: Ensures data is received and in order during communication.

2. Connection-Oriented: Requires a three-way handshake to establish a connection before data transmission.

Sender sends a SYN message.

Receiver acknowledges with an acknowledgment message.

Sender confirms the acknowledgment.

3. Guaranteed Delivery: Resends data packets if they are lost during transmission.

4. Use Cases: Critical for applications where data integrity is essential, such as web pages and file downloads.

UDP (USER DATAGRAM PROTOCOL)

1. Purpose: Also for sending and receiving data, but with key differences.

2. Connection-less: Does not establish a session or guarantee data delivery.

3. "Fire-and-Forget" Protocol: Sends data without concern for whether it reaches the destination.

4. Speed: Faster than TCP due to less overhead from not ensuring data delivery.

5. Use Cases: Suitable for applications where occasional data loss is acceptable, emphasizing speed over reliability.

COMPARISON

|  |  |  |
| --- | --- | --- |
|  | TCP | UDP |
| Reliability | Ensures reliable data delivery through a connection-oriented approach. | Sacrifices reliability for speed, making it a "fire-and-forget" protocol. |
| Connection Establishment | Requires a three-way handshake before data transmission. | Does not establish a connection before sending data. |
| Data Delivery | Guarantees delivery by resending lost packets. | Does not guarantee delivery; data loss is possible. |
| Speed | Slower due to connection establishment and guaranteed delivery. | Faster with less overhead, suitable for applications prioritizing speed. |

## HTTP, HTTPS & SSL

HTTP, or Hypertext Transfer Protocol, is the foundation of web communication, allowing us to access web pages through our browsers. However, standard HTTP sends data as plain text, making it susceptible to interception by hackers. Sensitive information like passwords or credit card details transmitted via regular HTTP is easily accessible to potential threats.

To address security concerns, HTTPS, or Secure Hypertext Transfer Protocol, was developed. It encrypts data transmitted through HTTP, ensuring its security during transit. With HTTPS, a website's URL shows an added 'S,' indicating the adoption of secure HTTP. Notably, web browsers display a padlock symbol in the address bar to signal the use of secure communication.

HTTPS employs two primary protocols for encryption: SSL (Secure Sockets Layer) and TLS (Transport Layer Security). SSL, although older, is a security protocol that authenticates websites using digital certificates. It establishes a secure connection between the browser and the server by encrypting data.

TLS, an updated version of SSL, operates similarly by encrypting data and authenticating both server and client. It represents the latest industry standard for secure communication on the web.

Many websites now default to using HTTPS, regardless of whether they handle sensitive data. This shift is partly due to Google's initiative, which flags websites without SSL protection as "not secure" and even penalizes their search rankings. Consequently, major websites have transitioned to using HTTPS to ensure data security and maintain credibility.

## FTP, SFTP, AND TFTP Protocols

FTP (File Transfer Protocol):

Definition: FTP is a standard protocol for transferring files between computers and servers over a network, such as the internet.

Usage: Used for sharing files globally by uploading them to an FTP server, which others can access and download using FTP protocol.

Methods: Files can be accessed through a web browser or FTP client; the example uses FTP server "FTP example.com."

Authentication: FTP servers may require username/password; anonymous login is also possible.

FTP Client: FileZilla is a popular FTP client, providing a graphical user interface for a better user experience.

Drawback: Not secure; data is sent in clear text, making it suitable only for non-sensitive data or on trustworthy networks.

SFTP (Secure File Transfer Protocol):

Definition: SFTP adds a layer of security to FTP by encrypting data using secure shell during transfer.

Security Features: Encrypts all data, authenticates both user and server, uses port 22.

Connection Type: Like FTP, it is connection-oriented and uses TCP for file transfer.

TFTP (Trivial File Transfer Protocol):

Definition: TFTP is a simple file transfer protocol used within a local area network for tasks like transferring configuration files and firmware images.

Usage: Primarily for local network use, not over the internet.

Connection Type: Connectionless; uses UDP instead of TCP.

Reliability: Unreliable transfer protocol.

Security: No security features, but considered acceptable for local network use.

FTP Usage: Common for bulk file transfers and enabling website designers to upload files.

Security Consideration: FTP is insecure; SFTP recommended for sensitive data.

TFTP Specialization: Mainly used within local networks for specific tasks.

Protocol Differences: TCP for FTP and SFTP, UDP for TFTP.

Viewer Experience: FTP clients, such as FileZilla, offer a more user-friendly interface compared to web browsers.

## SMTP - SIMPLE MAIL TRANSFER PROTOCOL

SMTP stands for Simple Mail Transfer Protocol.

Unlike POP and IMAP, which are used for retrieving email, SMTP is a protocol for sending email.

SMTP involves a set of commands that authenticate and direct the transfer of emails.

SMTP serves as the protocol for sending emails, managing the transfer of email from the sender to the recipient.

Acronym: SMTP = 'Sending Mail To People.'

When sending an email, it travels from the sender's computer to their email server using SMTP.

The server, known as the SMTP server, is configured in the email client (e.g., Microsoft Outlook, Gmail).

Example: Gmail's SMTP server address is smtp.gmail.com.

The recipient's email server also uses SMTP to receive the message.

After reaching the recipient's email server, the email stays until the recipient either downloads it using POP or IMAP or views it on the server through webmail.

SMTP uses the TCP protocol, ensuring a connection-oriented and guaranteed delivery process.

If the email address is incorrect or nonexistent, a mail delivery error informs the sender of the failure.

Like POP and IMAP, SMTP is configured in email clients (e.g., Microsoft Outlook, Mozilla Thunderbird, mobile devices).

SMTP server settings, such as smtp.gmail.com for Gmail, are specified in the outgoing server settings of the email client.

## POP3 VS. IMAP

POP3 (Post Office Protocol 3) and IMAP (Internet Message Access Protocol) are two commonly used protocols for retrieving email from a server. While both protocols serve the same purpose, they differ significantly in their functionality and suitability for different user needs.

POP3 is a simpler protocol designed for downloading email from the server to a single device. It only retrieves messages from the inbox folder, leaving all other folders and their contents untouched on the server. Once downloaded, emails are deleted from the server, ensuring that they are stored locally on the device.

Advantages of POP3:

Offline Access: Downloaded emails can be accessed without an internet connection.

Reduced Server Storage: Emails are removed from the server, freeing up storage space.

Disadvantages of POP3:

No Synchronization: Email folders and contents are not synchronized across devices.

Backup Required: Users need to back up their emails to prevent data loss.

Virus Vulnerability: Fully downloaded emails may contain viruses that can infect the device.

IMAP is a more advanced protocol that provides real-time access to email stored on the server. It allows users to view, manage, and organize their email from multiple devices, keeping everything synchronized. Unlike POP3, IMAP does not delete emails from the server after they are accessed.

Advantages of IMAP:

Real-time Access: Email is always accessible, even from multiple devices.

Synchronization: Email folders and contents are synchronized across all devices.

Centralized Storage: Emails are stored on the server, eliminating the need for local backups.

Disadvantages of IMAP:

Offline Access Limited: Offline access requires local caching of emails, which may consume storage space.

Internet Dependency: Requires an internet connection to access email and perform actions.

The choice between POP3 and IMAP depends on individual user preferences and usage patterns.

POP3 is suitable for users who:

Primarily use a single device for email.

Value offline access.

Have limited storage space on their devices.

IMAP is suitable for users who:

Access email from multiple devices.

Require real-time access and synchronization.

Prefer centralized storage on the server.

## DDOS ATTACK

DDoS stands for distributed denial of service.

It is basically a cyber-attack on a specific server or network with the intended purpose of disrupting that network or server's normal operation.

A DDoS attack does this by flooding the targeted network or server with a constant flood of traffic, such as fraudulent requests, which overwhelms the system, causing a disruption or denial of service to legitimate traffic.

So, suppose there is a web server and let's just say that this web server could belong to a company that sells their products over the internet.

There are some customers with their computers that are browsing the company's website, looking at the company's products or services.

Now let's just say that someone just wanted to do an attack on this company's web server. What happens is the attacker is going to use their computer and their program to attack this server and flood it with fraudulent data traffic to try and disrupt its service.

Now this is not a DDoS attack, this is just called a DoS attack which stands for denial of service.

Because a DoS attack is an attack that's just coming from one source.

Now, normally a network or server is able to handle an attack from a single source because it's easier to pinpoint. The server can just simply close the connection where the attack is coming from. So that's not really a problem.

However, the problem is that what if an attack comes from multiple sources simultaneously? And that is what a DDoS is.

A DDoS is an attack from multiple sources all at once.

The computer which is the ringleader, can communicate with other computers around the world and coordinate an attack on this server.

Now instead of an attack coming from a single source, the server now has to deal with an attack from multiple sources and when this happens, it will overwhelm the server. It will eat up the server's system resources, such as the CPU and memory, and it will also eat up network bandwidth.

As a result, these legitimate computers are going to be denied service because the server is too preoccupied in dealing with a DDoS attack.

The web pages is either not going to load or they are going to be very slow in loading.

The question is how does the attacker get other computers to get involved in a DDoS attack? And the simple answer is by using malicious software.

The attacker will develop a malware program and distribute it over the internet and put it on things like websites and email attachments. If computer goes to these infected websites or opens these infected email attachments, the malware will be installed on their computer without the owner even knowing that their computer has been infected.

Now their computer has been recruited in an army of other infected computers to perform a DDoS attack. And this army of infected computers is what's called a botnet.

Botnet is not just limited to a few computers; this botnet could be hundreds or even thousands of computers that are scattered all over the world.

This botnet can be controlled like an army, waiting to receive instructions from the attacker, who is now like a centralized command and control center for the botnet. And then the attacker can send out commands to all these computers and to tell them to attack at a certain date and time. And then once that set time is reached, the attack begins.

Now a DDoS attack can last for hours or even days. It just depends on the attacker’s intent.

Another question is, why do people do DDoS attacks? DDoS attacks can happen for several different reasons. For example, it could be for financial reasons and the attacker is DDoSing a competitor in the marketplace. It could also be for maybe political reasons. Maybe they don't like the targeted organization's beliefs. Or it could also be that maybe the attacker is just doing it for fun!

# RANDOM

basics of ip addressing

* every node in the computer network is identified with the help of ip address.
* logical address.
* can change based on the location of the device.
* assigned by manually or dynamically.
* represented in decimal and it has 4 octets (xxxx).
* to 255.255.255.255 (32 bits).

basics of mac addressing

* mac stands for media access control.
* every node in the lan is identified with the help of mac address.
* ip address = location of a person.
* mac address = name of the person.
* physical address or hardware address.
* unique.
* cannot be changed.
* assigned by the manufacturer.
* represented in hexadecimal.
* example: 70-20-84-00-ed-fc (48 bits).
* separator:hyphen(-), period(.), and colon(:).

basics of port addressing

* reaching our city=reaching our network. (ip address)
* reaching our apartment reaching the host. (mac address)
* reaching the right person reaching the right process. (port address)
* in a node, many processes will be running.
* data which are sent/received must reach the right process.
* port=communication endpoint.
* every process in a node is uniquely identified using port numbers.
* fixed port numbers and dynamic port numbers (0-65535)
* example: fixed port numbers: 25,80 etc. & assigned dynamic port numbers: 62414.

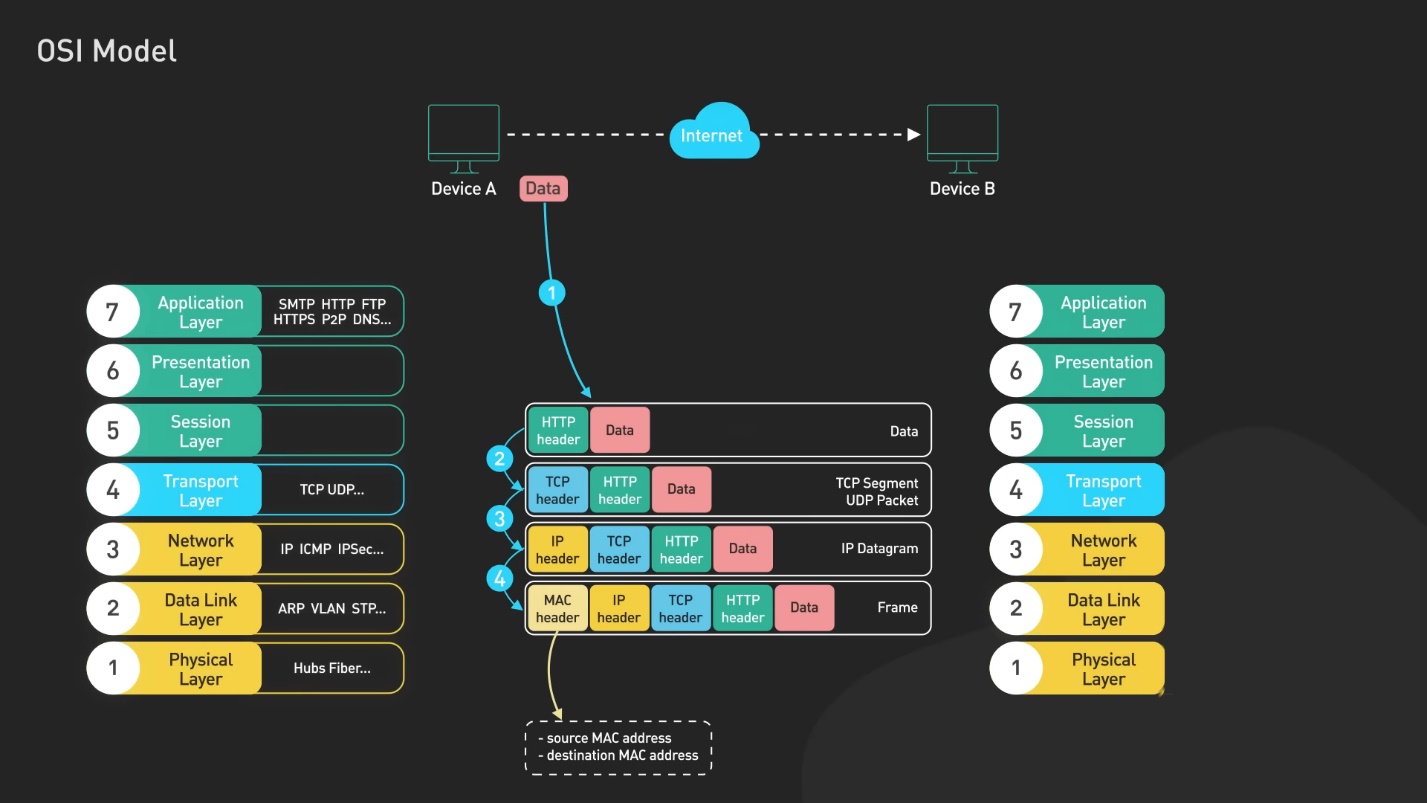
layering in computer networks

* layering means decomposing the problem into more manageable components (layers)
* protocols
* it is a set of rules that governs data communication.
* the protocols in each layer governs the activities of the data communication.
* layered architectures

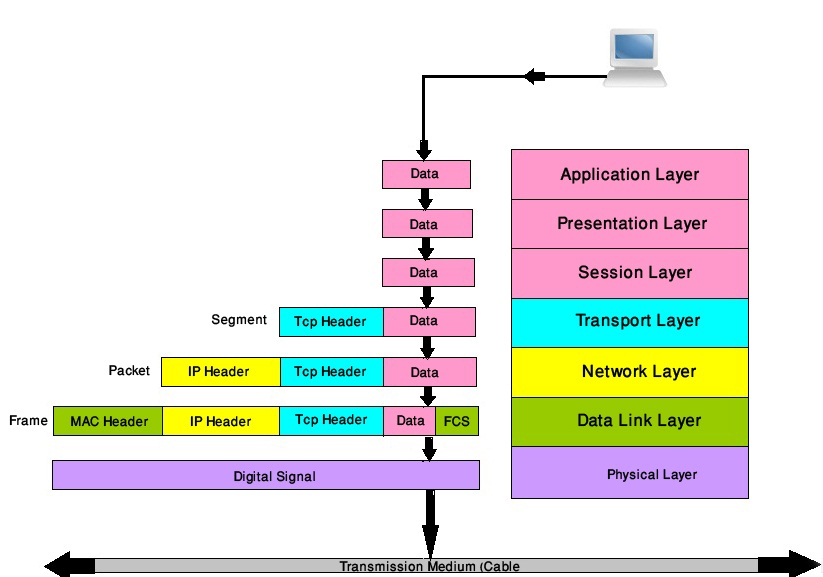
1. the osi referece model

* osi stands for open system interconnection.
* it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.
* developed by the international standards for organizations (iso).
* the osi model is not a protocol.
* it is only a guideline and hence it is referred as osi reference model
* the purpose of the osi model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software.
* the osi model was never fully implemented.
* it is important to know that all seven layers of osi model works simultaneously and not one after another.
* each layer is nothing but a collection of protocols.

**the following two images will help understand the osi model completely**!



\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



1. the tcp/ip model.

tcp/ip = transmission control protocol/internet protocol.

the tcp/ip protocol suite was developed prior to the osi model.

therefore, the layers in the tcp/ip protocol suite do not exactly match those in the osi model.

tcp/ip is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality

must watch - <https://youtu.be/ydtc6sbyffe?si=r01p-3jha-tgvkiu>

ieee

ieee stands for the institute of electrical and electronics engineers.

ieee-sa stands for the ieee standards association. it is a division of the ieee that is responsible for developing and publishing technical standards.

imagine a city with no traffic laws. everyone is driving on the wrong side of the road, and there are no stop signs or red lights. this would be chaotic.

ieee-sa is like the city council that develops traffic laws.

ieee-sa develop standards that ensure that different devices and systems can work together safely and efficiently.

ieee-sa standards are used in a wide range of industries, including: telecommunications, computer networking, consumer electronics, healthcare, transportation, energy, manufacturing and more.